

# MANAGED CYBERSECURITY SERVICE PROVIDERS FOR ELECTRIC UTILITIES

---

## PREPARED FOR:

THE AMERICAN PUBLIC POWER ASSOCIATION AND  
THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

BY: PRESCOUTER



October 2017

## Acknowledgment

This material is based upon work supported by the Department of Energy, Office of Electricity Delivery and Energy Reliability under Award Numbers DE-OE0000807 and DE-OE0000811.

---

## Disclaimers

### **NRECA and APPA Disclaimer:**

This report is not an endorsement of the companies, products, or services referenced herein. NRECA, APPA and the report authors assume no liability for how readers may use this report or any damages resulting from its use. There is no warranty or representation that the use of this report does not infringe on privately held rights or that this report is complete, up-to-date or accurate. Readers are encouraged to perform due diligence in applying this report to their specific needs.

### **Department of Energy Disclaimer:**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

# Table of Contents

<b>Acknowledgment</b> .....	<b>i</b>
<b>Disclaimers</b> .....	<b>i</b>
<b>PreScouter's Statement of Work</b> .....	<b>iv</b>
The Business Challenge .....	<b>iv</b>
Areas of Interest .....	<b>iv</b>
<b>Report Organization</b> .....	<b>v</b>
Description of Categories and Icon Legend .....	<b>v</b>
<b>Section 1 Executive Summary</b> .....	<b>1</b>
Organization.....	<b>1</b>
Proposed Next Steps .....	<b>1</b>
<b>Section 2 Summary Tables</b> .....	<b>3</b>
On-site Systems Integration Consulting.....	<b>3</b>
Systems Management of the Client's Network .....	<b>4</b>
Managed Security Monitoring.....	<b>5</b>
Incident Management Forensics Analysis Services.....	<b>7</b>
Penetration Testing and Vulnerability Assessments .....	<b>9</b>
<b>Section 3 Company Descriptions</b> .....	<b>11</b>
AlienVault.....	<b>11</b>
Alpine Security .....	<b>12</b>
Brier & Thorn .....	<b>13</b>
Carbon Black, Inc. ....	<b>14</b>
Center for Internet Security (CIS) .....	<b>15</b>
Cisco Systems, Inc. ....	<b>16</b>
Datashield.....	<b>17</b>
Delta Risk LLC .....	<b>18</b>
Digital Guardian .....	<b>19</b>
Digital Hands .....	<b>20</b>
DNV GL.....	<b>21</b>
Duff & Phelps .....	<b>22</b>
EiQ Networks, Inc. ....	<b>23</b>
EventTracker.....	<b>24</b>
FireEye .....	<b>25</b>
Fortinet Security Services.....	<b>26</b>
Hitachi Systems Security .....	<b>27</b>
LogRhythm.....	<b>28</b>
Lumension Security Inc .....	<b>29</b>
Masergy .....	<b>30</b>
Morphick .....	<b>31</b>

Mosaic451 .....	32
N-Dimension Solutions, Inc. ....	33
Netwatcher .....	34
Nexum, Inc. ....	35
NTT Security .....	36
Nuspire Networks.....	37
Palo Alto Networks.....	38
Proficio.....	39
Rapid7.....	40
RAVENii .....	41
Redhawk.....	42
RedSeal, Inc. ....	43
Rendition Infosec .....	44
root9B.....	45
SageNet.....	46
SecureWorks .....	47
SecurIT360 .....	48
Security On-Demand .....	49
Sedara .....	50
Sera-Brynn.....	51
Solvere One .....	52
SpearTip.....	53
Symantec .....	54
Tagrem Security.....	55
Trustwave .....	56
Wipro, Ltd .....	57

# PreScouter's Statement of Work

## The Business Challenge

The American Public Power Association (Public Power) and the National Rural Electric Cooperative Association (NRECA) represent thousands of not-for-profit, community- and consumer-owned electric utilities. Their member utilities are responsible for delivering reliable, affordable electricity to a majority of the United States. These utilities are relatively small and may be resource-limited in terms of IT staffing. Public Power and NRECA member utilities are often located in geographic regions that provide limited access to trained cybersecurity personnel. The goal of this report is to aid members that may be looking to outsource their cybersecurity work by providing a catalogue of potential cybersecurity service providers working in this growing field. Readers are encouraged to perform due diligence in applying this report to their specific needs.

## Areas of Interest

This report identifies managed security service providers (MSSPs) that offer commercial-off-the-shelf (COTS) solutions. The report's target audience is utilities with few, if any, IT staff and/or access to cybersecurity expertise. (However, the content provided within may be useful for utilities of all sizes and staffing levels.) These utilities may rely on third parties to provide Information Technology (IT) services and cybersecurity. In some cases, the person responsible for cybersecurity may have a primary role in an administrative field, not a technical field. This may be a staff member in finance/billing, office management, community outreach, etc. This report identifies MSSPs who can fill the gap that existing staff resources cannot meet in terms of cybersecurity expertise. Each entry focuses on one commercial solution/MSSP capable of satisfying some or all of the following criteria:

- MSSPs that offer **bundled services**. More specifically the MSSP provides at least one of the following four service domains as part of their bundle of offered services:
  - **End-point security** solution that includes malicious code management (preferably white listing to reduce administrative overhead, host-based firewalls with

centralized management, intrusion detection/prevention, loss prevention, etc.

- **Privilege Identity Management** that includes the ability to manage shared accounts and administrator accounts.
  - **Patch Management** solution that includes discovery of new patches and ability to group devices and deliver patches.
  - **Vulnerability assessment** tools that allow assessing network and system threats.
- MSSPs that have **experience providing services to the electricity sector**. This does not have to be their only service market, but it should be included in their potential service market.
  - MSSPs that focus on **Ethernet enabled devices**, not serially-connected devices. While primary systems that need to be secured fall within traditional IT systems (desktops, servers, etc.), this report focuses on MSSPs that can also provide cybersecurity tools/techniques to secure Ethernet enabled ICS devices (e.g. systems commonly referred to as relays, programmable logic controllers, reclosers, remote terminal units, protocol converters, etc.) and MSSPs with service offerings for security monitoring, secure configuration management, and vulnerability assessments for the ICS devices.
  - MSSPs that emphasize their ability to **offer services to small businesses**. The emphasis is on MSSPs that focus on, or have experience servicing, small systems with less than 100 assets.
  - Where available, each entry also highlights MSSPs that provide services in any of the following domains:
    - Single file encryption software
    - Security Information and Event Management
    - Mobile device encryption
    - Bring your own device (BYOD) — provisioning for company and personal devices
    - Subscriptions to threat information intelligence feeds

\*The information provided by PreScouter for this report was collected from publicly available websites, not from direct contact with the MSSPs.

# Report Organization

## Description of Categories and Icon Legend

### ON-SITE SYSTEMS INTEGRATION CONSULTING



This is customized assistance to assess business risks, and then identify and integrate appropriate technologies and business processes to address prioritized cyber risks. A system integrator's core function is to bring together component subsystems into one system and enable those subsystems to function seamlessly together. In the context of this effort, the systems integrator consultant's core service will help secure product integration of both security subsystems and subsystems that are not primarily security focused.

### SYSTEMS MANAGEMENT OF THE CLIENT'S NETWORK



This service involves installing, upgrading, and managing the network hardware and software infrastructure such as firewalls, routers and switches, Virtual Private Networks (VPN) for remote access, intrusion prevention and detection technologies, and business applications such as electronic mail, billing and finance services, and web services. These providers may also provide services for configuration management, monitoring, and firewall access control. Regular reports would be provided to the client regarding network utilization, systems' health monitoring, and records that demonstrate actions taken for security patching and security monitoring. It is possible that managed security monitoring will be bundled into a systems management service.

### MANAGED SECURITY MONITORING



This is the day-to-day monitoring and interpretation of important system events throughout the network — including anomalous communication, such as malicious code, denial of service (DoS), anomalies, and trend analysis. It is one of the suggested first steps in an incident response process. Intrusion detection management, either at the network level or at the individual host level, involves providing intrusion alerts to a customer, keeping up-to-date with new defenses against intrusions, and regularly reporting on intrusion attempts and activity. Content filtering services may be provided such as email filtering and other data traffic filtering. It is quite possible that these services will be bundled in a systems management service.

### INCIDENT MANAGEMENT FORENSICS ANALYSIS SERVICES



These services would be used after a cybersecurity incident to rapidly respond to the incident, assess the loss, implement measures to try to: stop or reduce continued losses; reduce the vulnerabilities used by the attacker; restore affected systems and services; and implement changes that aim to reduce the likelihood of another incident. These services may also be included in either a managed security or system management service.

### PENETRATION TESTING AND VULNERABILITY ASSESSMENTS



This includes one-time or periodic network penetration tests to simulate an attacker's ability to compromise a network by exploiting existing vulnerabilities. The penetration test can be performed from an external attacker's perspective, with limited knowledge of the target, or from an insider threat perspective, leveraging known configurations and vulnerabilities. Vulnerability assessments use automated or manual scanning of the hardware and software to find weaknesses in the implementations that could be exploited by an attacker.

# Executive Summary

## Organization

### INTRODUCTION:

PreScouter identified and presented companies that provide cybersecurity products and services that might be relevant to members of NRECA and APPA based upon provided criteria explained in the Statement of Work.

### SEGMENTS ADDRESSED IN THIS REPORT:

The report has been organized alphabetically. Icons, as well as the summary table segmentation, indicate the categories of providers to which each company belongs. The categories are as follows:

- On-site Systems Integration Consulting
- Systems Management of the Client's Network
- Managed Security Monitoring
- Incident Management Forensics Analysis Services
- Penetration Testing and Vulnerability Assessments

See Report Organization on [page v](#) for a detailed description of these categories.

### INSIGHTS IN THIS REPORT:

1. A large number of cybersecurity providers are available that service the utility/ electricity sectors and have specific offerings for small business that match the needs identified by NRECA and APPA.

2. The largest number of companies identified belong to the categories of Managed Security Monitoring and Penetration Testing & Vulnerability Assessments.
3. Although cybersecurity services are globally available, this research revealed numerous providers focused on the North American market.
4. No single company was found that possessed all the focus areas, and that offered all of the critical and non-critical services required.

## Proposed Next Steps

Moving forward, organizations wishing to use this report to select a cybersecurity provider can take the following steps:

1. Determine and prioritize the relevant cybersecurity needs for your organization.
2. Use this report, in addition to other resources available to your utility to identify appropriate companies for your particular cybersecurity needs:
  - Use the summary table to quickly understand which of the companies match the criteria most relevant to your organization.
  - Review company descriptions to better understand the profile and offerings for each provider, and to obtain contact information to get in touch with the provider.

\*This report is not intended to provide a comprehensive or complete list of MSSPs. Additional MSSPs will be added over time.

- Discuss offerings with all providers that seem relevant and determine if the level of security provided is above, below, or level with your organization's requirements.
3. Understand costs of outsourcing cybersecurity to these companies by asking for detailed quotes, including installation fees as well as recurring costs.
  4. Select one or multiple providers, including, but not limited to, using the information in this report, to meet your utility's specific needs.



# Summary Tables

## On-site Systems Integration Consulting

Company	Page	SERVICE OFFERINGS (Y/N)									FOCUS AREAS (Y/N)			
		Endpoint Security	Privileged Data Management	Patch Management	Vulnerability Assessments	Single File Encryption Software	Security Information and Event Management	Mobile Device Encryption	Bring Your Own Device Provisioning	Subscriptions to Threat Information Intelligence Feeds	Managed Security Service Provider	NERC CIP Compliance	Electricity Sector Experience	Small Business Focus
		C2M2 Domain												
		ACM, TVM	ACM, IAM	TVM	TVM	ACM	SA, IR	ACM	ACM, IAM	TVM, ISC	EDM	EDM	N/A	N/A
Digital Hands	20	●	●		●		●		●	●	●			●
EventTracker	24						●			●	●	●	●	
Hitachi Systems Security	27	●	●	●	●		●			●	●		●	●
Lumension	29	●	●	●	●	●	●			●	●	●	●	●
Masergy	30	●			●		●		●	●		●	●	
Mosaic451	32	●	●	●	●		●				●	●	●	●
N-Dimension	33				●		●		●	●	●	●	●	●
NTT Security	36	●	●	●	●		●			●	●	●	●	●
Nuspire Networks	37	●		●							●			
Palo Alto Networks	38	●					●			●			●	
Proficio	39	●			●		●			●	●	●	●	
Rapid7	40	●			●		●			●	●	●	●	●
Rendition Infosec	44	●			●		●			●	●			
root9B	45			●	●		●			●	●			
Security On-Demand	49	●	●	●	●		●		●	●	●	●	●	●
Symantec	54	●	●	●	●		●		●	●	●		●	

## Systems Management of the Client's Network

Company	Page	SERVICE OFFERINGS (Y/N)									FOCUS AREAS (Y/N)			
		Endpoint Security	Privileged Data Management	Patch Management	Vulnerability Assessments	Single File Encryption Software	Security Information and Event Management	Mobile Device Encryption	Bring Your Own Device Provisioning	Subscriptions to Threat Information Intelligence Feeds	Managed Security Service Provider	NERC CIP Compliance	Electricity Sector Experience	Small Business Focus
		C2M2 Domain												
		ACM, TVM	ACM, IAM	TVM	TVM	ACM	SA, IR	ACM	ACM, IAM	TVM, ISC	EDM	EDM	N/A	N/A
Brier & Thorn	13	●	●	●	●		●			●	●		●	
Center for Internet Security (CIS)	15				●		●			●	●			
Cisco Systems	16	●	●	●			●	●	●	●	●		●	●
Digital Hands	20	●	●		●		●		●	●	●			●
Fortinet	26	●	●	●	●			●		●	●			●
Mosaic451	32	●	●	●	●		●				●	●	●	●
N-Dimension	33				●		●		●	●	●	●	●	●
Nexum	35	●	●	●	●		●			●	●			●
NTT Security	36	●	●	●	●		●			●	●	●	●	●
Proficio	39	●			●		●			●	●	●	●	
Rapid7	40	●			●		●			●	●	●	●	●
RAVENii	41	●		●	●	●	●	●	●	●	●		●	
RedSeal	43	●			●			●			●	●	●	
Security On-Demand	49	●	●	●	●		●		●	●	●	●	●	●
Symantec	54	●	●	●	●		●		●	●	●		●	

## Managed Security Monitoring

Company	Page	SERVICE OFFERINGS (Y/N)									FOCUS AREAS (Y/N)			
		Endpoint Security	Privileged Data Management	Patch Management	Vulnerability Assessments	Single File Encryption Software	Security Information and Event Management	Mobile Device Encryption	Bring Your Own Device Provisioning	Subscriptions to Threat Information Intelligence Feeds	Managed Security Service Provider	NERC CIP Compliance	Electricity Sector Experience	Small Business Focus
		C2M2 Domain												
		ACM, TVM	ACM, IAM	TVM	TVM	ACM	SA, IR	ACM	ACM, IAM	TVM, ISC	EDM	EDM	N/A	N/A
Alpine Security	12	●			●		●			●	●			●
Brier & Thorn	13	●	●	●	●		●			●	●		●	
Carbon Black	14										●			
Cisco	16	●	●	●			●	●	●	●	●		●	●
Datashield	17	●			●		●				●	●	●	
Delta Risk	18	●			●		●	●		●	●	●		
Digital Guardian	19	●	●			●		●		●	●		●	
Digital Hands	20	●	●		●		●		●	●	●			●
EiQ Networks	23	●		●	●		●			●	●	●		●
EventTracker	24						●			●	●	●	●	
Fortinet	26	●	●	●	●			●		●	●			●
Hitachi Systems Security	27	●	●	●	●		●			●	●		●	●
LogRhythm	28	●			●		●			●	●	●	●	
Lumension Security	29	●	●	●	●	●	●			●	●	●	●	●
Masergy	30	●			●		●		●	●	●	●	●	●
Morphick	31	●			●		●			●	●			
Mosaic451	32	●	●	●	●		●				●	●	●	●
N-Dimension	33				●		●		●	●	●	●	●	●
Netwatcher	34	●			●		●		●		●			●
Nexum	35	●	●	●	●		●			●	●			●

Continued

## Managed Security Monitoring (Cont.)

Company	Page	SERVICE OFFERINGS (Y/N)									FOCUS AREAS (Y/N)			
		Endpoint Security	Privileged Data Management	Patch Management	Vulnerability Assessments	Single File Encryption Software	Security Information and Event Management	Mobile Device Encryption	Bring Your Own Device Provisioning	Subscriptions to Threat Information Intelligence Feeds	Managed Security Service Provider	NERC CIP Compliance	Electricity Sector Experience	Small Business Focus
		C2M2 Domain												
		ACM, TVM	ACM, IAM	TVM	TVM	ACM	SA, IR	ACM	ACM, IAM	TVM, ISC	EDM	EDM	N/A	N/A
NTT security	36	●	●	●	●		●			●	●	●	●	●
Nuspire Networks	37	●		●							●			
Proficio	39	●			●		●			●	●	●	●	
Rapid7	40	●			●		●			●	●	●	●	●
RAVENii	41	●		●	●	●	●	●	●	●	●		●	
Redhawk	42			●	●		●				●	●	●	●
Rendition Infosec	44	●			●		●			●	●			
root9B	45			●	●		●			●	●			
SageNet	46	●	●	●	●		●				●		●	
SecureWorks	47	●			●		●				●		●	
SecurIT360	48	●			●		●		●	●			●	●
Security On-Demand	49	●	●	●	●		●		●	●	●	●	●	●
Sedara	50	●		●	●		●				●	●		●
Sera-Brynn	51				●		●			●	●			
Solvere One	52				●		●			●	●		●	
SpearTip	53	●			●		●			●	●			●
Symantec	54	●	●	●	●		●		●	●	●		●	
Tagrem	55	●	●		●		●				●		●	●
Trustwave	56	●			●	●	●	●	●	●	●			●
Wipro	57	●	●		●		●				●			

## Incident Management Forensics Analysis Services

Company	Page	SERVICE OFFERINGS (Y/N)									FOCUS AREAS (Y/N)			
		Endpoint Security	Privileged Data Management	Patch Management	Vulnerability Assessments	Single File Encryption Software	Security Information and Event Management	Mobile Device Encryption	Bring Your Own Device Provisioning	Subscriptions to Threat Information Intelligence Feeds	Managed Security Service Provider	NERC CIP Compliance	Electricity Sector Experience	Small Business Focus
		C2M2 Domain												
		ACM, TVM	ACM, IAM	TVM	TVM	ACM	SA, IR	ACM	ACM, IAM	TVM, ISC	EDM	EDM	N/A	N/A
Alpine Security	12	●			●		●			●	●			●
Brier & Thorn	13	●	●	●	●		●			●	●		●	
Center for Internet Security (CIS)	15				●		●			●	●			
Delta Risk	18	●			●		●	●		●	●	●		
Digital Guardian	19	●	●			●		●		●	●		●	
DNV GL	21	●		●	●		●			●	●	●		●
Duff & Phelps	22				●									
EiQ Networks	23	●		●	●		●			●		●	●	
FireEye	25	●			●		●			●	●		●	
Fortinet	26	●	●	●	●			●		●	●			●
LogRhythm	28	●			●		●			●		●	●	
Lumension	29	●	●	●	●	●	●			●	●	●	●	●
Morphick	31	●			●		●			●	●			
Mosaic451	32	●	●	●	●		●				●	●	●	●
Nexum	35	●	●	●	●		●			●	●			●
NTT Security	36	●	●	●	●		●			●	●	●	●	●
Nuspire Networks	37	●		●							●			
Proficio	39	●			●		●			●	●	●	●	
Rapid7	40	●			●		●			●	●	●	●	●
Rendition Infosec	44	●			●		●			●	●			
SecureWorks	47	●			●		●		●	●	●		●	

Continued

## Incident Management Forensics Analysis Services (Cont.)

Company	Page	SERVICE OFFERINGS (Y/N)									FOCUS AREAS (Y/N)			
		Endpoint Security	Privileged Data Management	Patch Management	Vulnerability Assessments	Single File Encryption Software	Security Information and Event Management	Mobile Device Encryption	Bring Your Own Device Provisioning	Subscriptions to Threat Information Intelligence Feeds	Managed Security Service Provider	NERC CIP Compliance	Electricity Sector Experience	Small Business Focus
		C2M2 Domain												
		ACM, TVM	ACM, IAM	TVM	TVM	ACM	SA, IR	ACM	ACM, IAM	TVM, ISC	EDM	EDM	N/A	N/A
SecurIT360	48	●			●		●						●	●
Security On-Demand	49	●	●	●	●		●		●	●	●	●	●	●
Sedara	50	●		●	●		●				●	●		●
Solvere One	52				●		●			●	●		●	
SpearTip	53	●			●		●			●	●			●
Symantec	54	●	●	●	●		●		●	●	●		●	

## Penetration Testing and Vulnerability Assessments

Company	Page	SERVICE OFFERINGS (Y/N)									FOCUS AREAS (Y/N)			
		Endpoint Security	Privileged Data Management	Patch Management	Vulnerability Assessments	Single File Encryption Software	Security Information and Event Management	Mobile Device Encryption	Bring Your Own Device Provisioning	Subscriptions to Threat Information Intelligence Feeds	Managed Security Service Provider	NERC CIP Compliance	Electricity Sector Experience	Small Business Focus
		C2M2 Domain												
		ACM, TVM	ACM, IAM	TVM	TVM	ACM	SA, IR	ACM	ACM, IAM	TVM, ISC	EDM	EDM	N/A	N/A
AlienVault	11				●		●			●		●	●	●
Alpine Security	12	●			●		●			●	●			●
Brier & Thorn	13	●	●	●	●		●			●	●		●	
Cisco	16	●	●	●			●	●	●	●	●		●	●
Delta Risk	18	●			●		●	●		●	●	●		
Digital Guardian	19	●	●			●		●		●	●		●	
Digital Hands	20	●	●		●		●		●	●	●			●
Duff & Phelps	22				●									
FireEye	25	●			●		●			●	●		●	
Fortinet	26	●	●	●	●			●		●	●			●
Hitachi Systems Security	27	●	●	●	●		●			●	●		●	●
Lumension	29	●	●	●	●	●	●			●	●	●	●	●
Masergy	30	●			●		●		●	●	●	●	●	●
Morphick	31	●			●		●			●	●			
Mosaic451	32	●	●	●	●		●				●	●	●	●
N-Dimension	33				●		●		●	●	●	●	●	●
Nexum	35	●	●	●	●		●			●	●			●
NTT Security	36	●	●	●	●		●			●	●	●	●	●
Nuspire Networks	37	●		●							●			

Continued

## Penetration Testing and Vulnerability Assessments (Cont.)

Company	Page	SERVICE OFFERINGS (Y/N)									FOCUS AREAS (Y/N)			
		Endpoint Security	Privileged Data Management	Patch Management	Vulnerability Assessments	Single File Encryption Software	Security Information and Event Management	Mobile Device Encryption	Bring Your Own Device Provisioning	Subscriptions to Threat Information Intelligence Feeds	Managed Security Service Provider	NERC CIP Compliance	Electricity Sector Experience	Small Business Focus
		C2M2 Domain												
		ACM, TVM	ACM, IAM	TVM	TVM	ACM	SA, IR	ACM	ACM, IAM	TVM, ISC	EDM	EDM	N/A	N/A
Proficio	39	●			●		●			●	●	●	●	
Rapid7	40	●			●		●			●	●	●	●	●
RAVENii	41	●		●	●	●	●	●	●	●	●		●	
Redhawk	42			●	●		●				●	●	●	●
RedSeal	43	●			●			●			●	●	●	
Rendition Infosec	44	●			●		●			●	●			
root9B	45			●	●		●			●	●			
SageNet	46	●	●	●	●		●				●		●	
SecureWorks	47	●			●		●		●	●	●		●	
SecurIT360	48	●			●		●						●	●
Security On-Demand	49	●	●	●	●		●		●	●	●	●	●	●
Sedara	50	●		●	●		●				●	●		●
Sera-Brynn	51				●		●			●	●			
Solvere One	52				●		●			●	●		●	
SpearTip	53	●			●		●			●	●			●
Symantec	54	●	●	●	●		●		●	●	●		●	
Tagrem	55	●	●		●		●				●		●	●
Trustwave	56	●			●	●	●	●	●	●	●			●
Wipro	57	●	●		●		●				●			



# Company Descriptions

## Alien Vault



1875 S. Grant Street, Suite 200, San Mateo, CA 94402

(650) 713-3333

<https://www.alienvault.com/contact>

### DESCRIPTION OF COMPANY:

AlienVault is a platform provider which emphasizes work with mid-market businesses and organizations, and the company has experience in the energy and utility industries, including working with electric companies as well as ICS/SCADA environments.

### ADDITIONAL DETAILS:

- Founded in 2007.
- Headquartered in San Mateo, CA.
- 200–500 employees.
- More than 3,000 commercial customers worldwide.
- Serving mid-sized companies to large government agencies.
- Has electricity sector experience.
- Has NERC CIP v5 compliance expertise.
- Has ICS/SCADA systems expertise.

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Platform is able to integrate other endpoint security products.
- Vulnerability assessments services are offered.
- Unified Security Management (USM) software simplifies ICS/SCADA security and facilitates NERC CIP v5 compliance.
- Security information and event management through USM.
- Solution provides up-to-date information on intrusion protection, vulnerabilities, etc. through the company's Open Threat Exchange (OTX).
- Can assist clients to find AlienVault certified MSSPs.
- Platform is specifically targeted for IT teams with limited budget and resources for mid-size organizations.


- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

[WWW.ALIENVAULT.COM](https://www.alienvault.com)

# Alpine Security



 7 Eagle Center, O'Fallon, IL 62269

 (844) 925-7463

 [info@alpinesecurity.com](mailto:info@alpinesecurity.com)

## DESCRIPTION OF COMPANY:

Alpine Security is an MSSP with strong focus on education and training.

## ADDITIONAL DETAILS:

- Founded in 2014.
- 51–200 employees.
- Has ICS/SCADA systems expertise.
- Serves small to medium businesses.
- A part from managed services, Alpine has a strong training program on cybersecurity suites for clients.
- Business focused on operation in North America.

- Endpoint Security
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Alpine Security provides Endpoint Security coupled with Intrusion Prevention & Detection services.
- Alpine Security provides data loss protection services.
- SIEM services is offered through Alpine Security + “Bit9 + Carbon Black Connect” Alliance Program and consists of network security and analytics, Firewall Administration and Monitoring, Authentication and Access Control, Intrusion Prevention & Detection, and Threat Intelligence.
- Other important services include Wireless Access Control and Authentication and Access Control.
- For the Enterprise Security Analysis, Alpine performs holistic audits, checks documentation, checks operation security, and covers controls for industry-based audits (PCI DSS, HIPAA, ISO, etc.) that can be leveraged for NERC CIP Compliance.


[WWW.ALPINESECURITY.COM/SERVICES/MANAGED-SECURITY-SERVICES](http://WWW.ALPINESECURITY.COM/SERVICES/MANAGED-SECURITY-SERVICES)

## Brier & Thorn



 1855 1st Avenue, Suite 103, San Diego, CA 92101

 (858) 381-4977

 sandiego@brierandthorn.com

### DESCRIPTION OF COMPANY:

Brier & Thorn works with the 'middle market' and across industries. In particular, Brier & Thorn is as much a security consultancy firm as it is an MSSP, and it can discuss and develop solutions using third party OTS software tailored to the requirements of a given business.

### ADDITIONAL DETAILS:

- Headquartered in San Diego, CA.
- Global company with offices in Mexico, London, and Stuttgart.
- Has experience in the energy sector.
- Has experience with energy companies securing modern ICS and SCADA systems.
- Focused on businesses with 50+ employees.

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Provides endpoint security and monitoring, but builds on systems already used by clients (not an integrator).
- Provides vulnerability assessments in the form of continual monitoring of the network, quarterly vulnerability scanning, and yearly penetration testing. Expertise in Internet of Things (IoT) penetration testing.
- Brier & Thorn has experience in the energy industry sector and experience with ethernet connected devices and utility specific devices.
- Brier & Thorn performs case studies in the energy industry.

- Endpoint Protection
- Patch Management
- Privileged Data Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

[WWW.BRIERANDTHORN.COM/EN/ENERGY.HTML](http://WWW.BRIERANDTHORN.COM/EN/ENERGY.HTML)

# Carbon Black, Inc.



1100 Winter St., Waltham, MA 02451  
(617) 393-7400  
info@eiqnetworks.com

### DESCRIPTION OF COMPANY:

Carbon Black, Inc. (formerly Bit9, Inc) is a security company that develops endpoint security software.

### ADDITIONAL DETAILS:

- Founded in 2002.
- Headquartered in Waltham, MA.
- 500+ employees.
- Has offices in Texas, Singapore, the UK, Tokyo, and Australia.
- Has approximately 2,000 worldwide customers, including 25 of the Fortune 100.

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Enables prioritized patch management with IBM BigFix and endpoint security.
- File integrity monitoring is provided.
- Only approved wireless access points are available on the network.
- SIEM 24x7 Security log management.
- Application control.
- Machine learning antivirus protection.

- Endpoint Security
- Patch Management
- Security Information and Event Management
- Vulnerability Assessments

[WWW.CARBONBLACK.COM](http://WWW.CARBONBLACK.COM)

## Center for Internet Security (CIS)



31 Tech Valley Drive, Suite 2, East Greenbush, NY 12061

(518) 266-3460

contact@cisecurity.org



### DESCRIPTION OF COMPANY:

The Multi-State Information Sharing & Analysis Center (MS-ISAC®) has been designated by Department of Homeland Security (DHS) as a key resource for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments. Through its 24/7 Security Operations Center, the MS-ISAC serves as a central resource for situational awareness and incident response for SLTT governments.

### ADDITIONAL DETAILS:

- Nonprofit entity founded in 2000.
- Headquartered in East Greenbush, NY.
- 51-200 employees.
- Has offices in Arlington, VA.

- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Multi-State Information Sharing & Analysis Center (MS-ISAC) as a part of Managed Security Services (MSS) provides monitoring and/or management of security devices that include Security Event Analysis and 24/7 Notifications, Firewalls, IDS (Intrusion Detection System)/IPS (Intrusion Prevention System), Web Proxy, and Endpoint.
- Vulnerability assessment is fee based and includes Network Assessment, Web Application Assessment — including manual analysis of reported vulnerabilities, prioritization of vulnerability remediation — customized reporting & vulnerability remediation support, and Payment Card Industry (PCI) compliance scanning.
- SIEM is offered using the Albert service for members and include Network & Computer Forensic Analysis, Log & Malware Analysis, Access to the Malicious Code Analysis Platform (MCAP), and Remediation Consulting.
- The CIS Security Operations Center (SOC) receives information from a variety of different sources; the information is analyzed to determine the need for the creation of advisories or bulletins. These needs include: threats, vulnerabilities, exploits, attacks, and compromises. Notifications and immediate remediation steps are provided.

[WWW.CISECURITY.ORG/CYBERSECURITY-TOOLS](http://WWW.CISECURITY.ORG/CYBERSECURITY-TOOLS)

## Cisco Systems, Inc.



 170 West Tasman Dr., San Jose, CA 95134

 (866) 428-9596

 <https://engage2demand.cisco.com/LP=567?ecid=136>

### DESCRIPTION OF COMPANY:

Cisco is a corporation with many products and services available. In particular, Cisco has specific security offerings for small businesses.

### ADDITIONAL DETAILS:

- Founded in 1984.
- Headquartered in San Jose, CA.
- Almost 72,000 employees.
- Works with businesses of all sizes.
- Has experience working with utilities.
- Has experience with all industries.
- Small business focus from the small business team.

- Bring Your Own Device Provisioning for Company and Personal Services
- Endpoint Security
- Mobile Device Encryption
- Patch Management
- Privileged Data Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds

### DESCRIPTION OF SERVICES/ PRODUCTS PROVIDED:

- Provides endpoint security, malware detection software, and threat management which responds in real time for all devices.
- Data management, Cisco Defense Orchestrator allows cloud-based management of accounts.
- Patch management included in management services offered by Cisco.
- Mobile device encryption and Bring Your Own Device (BYOD) provisioning for company and personal services is provided by a secure mobility client, allowing employees to work anywhere on any device.
- Cloud-based email security offered as a service.
- Offers network management and data storage as other services.
- Also provides hardware if the network requires it.

[WWW.CISCO.COM](http://WWW.CISCO.COM)

# Datashield



 455 E 200 S, Suite 100, Salt Lake City, UT 84111  
 (866) 428-4567  
 [info@datashieldprotect.com](mailto:info@datashieldprotect.com)

## DESCRIPTION OF COMPANY:

Datashield is an MSSP that offers a wide variety of cybersecurity services.

## ADDITIONAL DETAILS:

- Founded in 2009.
- Headquartered in Salt Lake City, UT.
- 51–200 employees.
- Has offices in Scottsdale, AZ.
- Services customers in Energy, Finance, Government, Retail, Defense, Gaming, Manufacturing.
- Has experience working with utilities.
- Has electricity sector experience.
- Has NERC CIP compliance expertise.

- Endpoint Security
- Security Information and Event Management
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Major services/products offered: Managed Detection and Response, Security Analytics (SA) — Security Information and Event Management (SIEM), Incident Response — Hunting — Cyber Threat Intelligence, and Compliance.
- Endpoint security and monitoring is provided through the proprietary tool DATASHIELD PROTECT™.
- Vulnerability assessments are implemented through ShieldVision software from Datashield. It allows for Rapid Automated Querying, Real Time Alerting, and historical querying, all working in tandem with new-threat intelligence. Both manual and automated vulnerability identification are provided, along with scanning capability for comprehensive network monitoring.
- Datashield provides for NERC CIP compliant Log Monitoring, Log Management, Vulnerability Management and Security Device Management. The services are a part of DATASHIELD Managed Security Services and Security Consulting Services.

[WWW.DATASHIELDPROTECT.COM](http://WWW.DATASHIELDPROTECT.COM)

## Delta Risk LLC



106 S. St. Mary's Street, Suite 601, San Antonio, TX 78205

(210) 293-0707

info@delta-risk.net

### DESCRIPTION OF COMPANY:

Delta Risk is a managed security service provider helping clients build advanced cyber defense and risk management capabilities.

### ADDITIONAL DETAILS:

- Founded in 2007.
- Headquartered in San Antonio, TX.
- 50–200 employees.
- Has offices in Arlington, VA and King of Prussia, PA.
- Works with businesses of all sizes and industries.
- Has electricity sector experience.
- Has NERC CIP compliance expertise.
- Has ICS/SCADA expertise.

- Endpoint Protection
- Mobile Device Encryption
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Endpoint security offered through company's ActiveEye<sup>SM</sup> and ActiveResponse<sup>SM</sup> service.
- Security advisory service provided to help client develop security programs or assess existing security efforts, determine vulnerability, and provide training to clients.
- Security information and event management solution offered.
- Keep clients informed on threat information and intelligence through newsletter and regular webinars.
- NERC CIP compliance through the company's ActiveEye<sup>SM</sup> and ActiveInsight<sup>SM</sup> services.
- Managed detection and response service provides 24/7 detection and response.
- Penetration testing service offered including: internal and external network, wireless network, mobile application, physical device, as well as social engineering penetration.
- Cloud application security.


[WWW.DELTA-RISK.COM](http://WWW.DELTA-RISK.COM)



# Digital Guardian



 860 Winter Street, Suite 3, Waltham, MA 02451

 (781) 788-8180

 [info@digitalguardian.com](mailto:info@digitalguardian.com)

## DESCRIPTION OF COMPANY:

Digital Guardian is a digital product provider offering managed security programs for threat protection, data loss prevention, and data protection.

## ADDITIONAL DETAILS:

- Founded in 2003.
- Headquartered in Waltham, MA.
- 200–500 employees.
- Has offices in Reston, VA, Santa Clara, CA, and Lehi, UT.
- Has energy sector experience.

- Endpoint Security
- Mobile Device Encryption
- Privileged Data Management
- Single-File Encryption Software
- Subscriptions to Threat Information Intelligence Feeds

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:


- Endpoint security offered using company's Application Control platform that uses a context-aware approach to control high-risk apps without restricting users.
- Privileged data management through company platform's content and context-aware control to ensure security of privileged users.
- Digital Guardian also offers automated, policy-based usage control and encryption for devices, removable devices, as well as email for security. The platform can automatically identify and encrypt sensitive data for devices.
- Threat information and intelligence provided through webinars and knowledge base.
- Managed threat protection service is provided to offer protection against zero-day attacks, polymorphic malware, ransomware, and other attacks.
- Offers cybersecurity team that's available 24/7.
- Provides proactive threat hunting and incident response.
- Managed security service that centers around data protection.

[HTTPS://DIGITALGUARDIAN.COM](https://digitalguardian.com)

## Digital Hands



 400 N. Ashley Drive, Suite 900, Tampa, FL 33602

 (877) 229-8020

 <https://www.digitalhands.com/about/contact>

### DESCRIPTION OF COMPANY:

Digital Hands is a U.S.-based Managed Services Provider (MSP). It has core competencies providing Managed Cybersecurity Services, Managed Network Infrastructure Services, and End-user Services (Service Desk/Help Desk). It serves both public and private organizations through IT Cybersecurity and Network support.

### ADDITIONAL DETAILS:

- Founded in 2001.
- 51–200 employees.
- Managed Security Service Provider for small- to large-scale businesses and production site.

- Bring Your Own Device Provisioning for Company And Personal Devices
- Endpoint Security
- Privileged Data Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Provides endpoint security and control using various security suites. For example: Aruba, Barracuda, McAfee, Microsoft, RSA, Palo Alto, Cisco Check Point Software Technologies, Symantec.
- Digital Hands provides data management using secure servers and cloud-based options. Automatically secures critical data in cases of active threat/breach. Digital Hands uses security solutions from various providers, such as McAfee, RSA (EMC).
- Vulnerability assessments offered through Unified Threat Management Services (UTM) by Digital Hands comprises features such as Web Application Firewall, Intrusion Detection, Intrusion Prevention, Antivirus Protection, Anti-Spam Protection, Data Loss Prevention, and Content Filtering.
- Digital Hands does offer E-mail encryption services.
- SIEM & Event Log Management is offered to track network activity, analyzing for suspicious or unauthorized events.
- Provides for BYOD Management, which allows workers to use their own personal devices, such as laptops, smartphones, and tablets, to perform their functions on the go.

[WWW.DIGITALHANDS.COM/SERVICES/MSSP](https://www.digitalhands.com/services/mssp)

DNV GL



One International Boulevard Crossroads Corporate Center,  
Suite 406, Mahwah NJ 07495

(201) 512-8900

<https://www.dnvgl.com/contact/group.html>



#### DESCRIPTION OF COMPANY:

DNV GL is an international certification body and classification society with main expertise in technical assessment, advisory, and risk management. DNV GL is an accredited certifier of electricity generation and distribution components. It was created in 2013, but the original version of the organization was founded in 1864.

#### ADDITIONAL DETAILS:

- Headquartered in Baerum, Akershus, Norway.
- Has offices in over 15 states in the United States.
- Has ICS/SCADA systems expertise.
- Has NERC CIP compliance expertise.
- Customers include small businesses, enterprise, and mid-size organizations.
- According to a 2015 company report DNV GL has 80,000+ customers, 350 offices in over 100 countries, and annual revenue of 2.4B NOK.
- Annually, DNV GL invests heavily in R&D which amounts to 5% of its total revenue.
- DNV GL operates the world's largest high power and voltage test laboratory.

#### DESCRIPTION OF SERVICES/ PRODUCTS PROVIDED:

- Control system architecture reviews, risk assessment methodology, and security architecture design are a few of the services available.
- DNV GL provides cybersecurity support to utilities throughout the project lifecycle for SCADA/EMS/DMS and DCS/PLC implementations.
- Security guidelines for remote access to control systems.
- Control system architecture reviews, Risk assessment methodology, Security architecture design.
- Incident response exercise development and facilitation.
- Network penetration and application security testing.
- Security infrastructure hardening.
- cybersecurity health test (whitebox testing), including security testing of energy IT, smart grid and smart meter components and detailed report back of findings and possible mitigation measures.

- Endpoint Security
- Mobile Device Encryption
- Patch Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

[WWW.DNVGL.COM/SERVICES/CYBER-SECURITY-FOR-ELECTRICITY-UTILITIES-17937](https://www.dnvgl.com/services/cyber-security-for-electricity-utilities-17937)

# Duff & Phelps



 55 East 52nd Street, 31st Floor, New York, NY 10055

 (212) 871-6366

 <http://insights.duffandphelps.com/contact-us>

## DESCRIPTION OF COMPANY:

Duff & Phelps analyze security posture and develop plans to prepare for, respond to, and recover from a security compromise. Clients include publicly traded and privately held companies, law firms, government entities and investment organizations such as private equity firms and hedge funds.

## ADDITIONAL DETAILS:

- Founded in 1932.
- Has more than 2,000 professionals located in more than 70 offices in 20 countries around the world.
- Develops cybersecurity and compliance frameworks that are aligned with SEC OCIE Risk Alert or other applicable regulatory agency.
- Has experience with the energy and mining sector.

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Vulnerability assessments performed as part of the services.
- Penetration testing and vulnerability scanning.
- Create a Written Information Security Policy (WISP).
- Development of an Incident Response Plan (IRP).
- Conduct third-party vendor due diligence.
- Sensitive and critical data identification and classification.
- End-user cybersecurity training.
- Phishing tests.
- Ongoing Cybersecurity Advisory Services “Virtual Chief Information Security Officer” (vCISO).


- Vulnerability Assessments

[WWW.DUFFANDPHELPS.COM](http://WWW.DUFFANDPHELPS.COM)

## EiQ Networks, Inc.



 60 State Street, Boston, MA 02109

 (617) 337-4880

 [info@eiqnetworks.com](mailto:info@eiqnetworks.com)

### DESCRIPTION OF COMPANY:

EiQ Networks' origins are in analysis of log files across web servers, file servers, firewalls, and other network devices, before moving to the SIEM market.

### ADDITIONAL DETAILS:

- Founded in 2001.
- Headquartered in Boston, MA.
- Has energy sector experience.
- SOC2 Type 1 Certified Service Provider.
- Has NERC CIP compliance expertise.

- Endpoint Security
- Patch Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/ PRODUCTS PROVIDED:

- EiQ's SOCVue Security Monitoring service helps organizations address NERC CIP by providing 24/7/365 security monitoring and reporting on system events and critical security controls, as required by CIP-007-5 R4.
- Typical vulnerability assessments include: Discovering IT assets, Classifying, Scanning, Remediating, and Verifying.
- Only approved wireless access points are available on the network.
- 24/7 Security log.
- Forensic analysis.
- Log Management.

[WWW.EIQNETWORKS.COM](http://WWW.EIQNETWORKS.COM)

# EventTracker (formerly Netsurion)



514 NE 13th Street, Fort Lauderdale, FL 33304

(866) 559-2170

sales@eventtracker.com

## DESCRIPTION OF COMPANY:

EventTracker (formerly Netsurion) offers a choice of Firewalls and IDS, Managed network security, data security, Wi-Fi access points, PCI compliance, broadband monitoring, SIEM and Threat monitoring.

## ADDITIONAL DETAILS:

- Founded in Houston, Texas in 1989.
- In 2016, Netsurion merged with EventTracker.
- EventTracker is now headquartered in Ft. Lauderdale, Florida.
- The company has about 51–200 employees.
- Has offices in St. Louis, Missouri, Columbia, Maryland, and Houston, Texas.

- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds

## DESCRIPTION OF SERVICES/ PRODUCTS PROVIDED:

- EventTracker provides endpoint security solutions using a newly launched (Jan. 2017) managed SIEM solution, SIEM-at-the-Edge. With a simple sensor deployed to critical servers and point-of-sale (POS) systems, the software would alert and take corrective actions for any anomalies or suspicious activities.
- The company does offer services with data management and big data analysis of various log files. One of the related services is called File integrity monitoring (FIM).
- Vulnerability assessments are offered through EventTracker's Vulnerability Assessments Service (ETVAS), which allows clients to schedule vulnerability scans to meet client requirements, such as weekly, monthly or quarterly scans.
- EventTracker provides enterprise-grade equipment combined with security architecture that provides a managed network solution. This security is coupled with SIEM that can pinpoint a threat in real-time and alert customers immediately, and take defined remedial actions. To this end, EventTracker monitors all the endpoints, detecting a wide range of suspect events across the network and devices.

[WWW.EVENTTRACKER.COM](http://WWW.EVENTTRACKER.COM)

# FireEye



1440 McCarthy Blvd., Milpitas, CA 95035

(408) 321-6300

info@fireeye.com

## DESCRIPTION OF COMPANY:

FireEye is a security technology and consultation provider covering all aspects of an institute's security needs.

## ADDITIONAL DETAILS:

- Founded in 2004.
- Headquartered in Milpitas, CA.
- 1,000–5,000 employees.
- Has offices in Alexandria and Reston, VA, Draper, UT, and New York, NY.
- More than 4,400 customers in more than 45 countries.
- Works with both small and medium businesses and Forbes' Global 2000 companies.
- Has experience serving regional utility companies, as well as utility districts.
- Has ICS/SCADA systems expertise.

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- FireEye has the capacity for endpoint security. It uses an adaptive platform that utilizes advance analytics beyond signature-based defense to provide visibility of known or unknown threats.
- Vulnerability assessments services are offered. FireEye provides assessment on security programs, identifies a compromise, helps setup response plan, as well as comprehensive health checks for SCADA and ICS environments.
- Up-to-date information on intrusion protection, vulnerabilities, and others.
- Additional services provided: email and network threat management, threat analytics and forensics, incident response service/retainer.


- Endpoint Protection
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments


[WWW.FIREEYE.COM](http://WWW.FIREEYE.COM)

# Fortinet Security Services



 899 Kifer Road, Sunnyvale, CA 94086

 (408) 235-7700

 <https://www.fortinet.com/corporate/about-us/contact-us.html>

## DESCRIPTION OF COMPANY:

The company develops and markets cybersecurity software, appliances, and services such as firewalls, anti-virus, intrusion prevention and endpoint security, among others.

## ADDITIONAL DETAILS:

- Founded in 2000.
- Headquartered in Sunnyvale, California, with offices around the globe.
- Has more than 4,000 employees.
- Customers include small businesses, mid-size organizations, and large enterprises.
- Company has more than 300,000 customers.
- Has SCADA systems expertise.

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Vulnerability scans.
- Mobile security service.
- Database security control.
- Application control and IPS.
- Web application security service.
- Botnet IP and registration.
- Application and user-identity awareness.
- Content security with integrated intrusion prevention.
- Antivirus.
- Web filtering.
- SSL encryption/decryption.
- Advanced threat detection and remediation.

- Endpoint Protection
- Mobile Device Encryption
- Patch Management
- Privileged Data Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments


[WWW.FORTINET.COM/FORTIGUARD/THREAT-INTELLIGENCE/FORTIGUARD-SUBSCRIPTION-SERVICES.HTML](http://WWW.FORTINET.COM/FORTIGUARD/THREAT-INTELLIGENCE/FORTIGUARD-SUBSCRIPTION-SERVICES.HTML)



# Hitachi Systems Security



 6431 Longhorn Dr., Irving, TX 75063

 (450) 430-8166

 <https://www.hitachi-systems-security.com/contact-us>

## DESCRIPTION OF COMPANY:

Hitachi Security Systems (formerly Above Security) is an MSSP which emphasizes work with small/medium businesses and has experience in the energy and utility industries, including working with plant equipment and PCSs.

## ADDITIONAL DETAILS:

- Founded in 1999.
- Works with both small/medium businesses and fortune 500 companies.
- Has electricity sector experience.
- Four security operations offices in Canada, Mexico, and Switzerland. Also serves companies in over 45 countries around the world.

- Endpoint Protection
- Patch Management
- Privileged Data Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Above Security aka Hitachi Security Systems uses a flexible system which manages third party solutions and can be tailored to the requirements of the small/medium business.
- Patch management is available if it is included in third party software managed by Hitachi Security Systems for end-point security. Log management system patches are delivered by Hitachi Security Systems.
- Vulnerability assessments services are offered. Hitachi Security Systems will identify the key information assets of the system, determine vulnerabilities, and provide recommendations and comprehensive reports to strengthen security.
- Security Information and Event Management is handled by the ArkAngel platform. Logs are stored by Hitachi Security Systems and analyzed to assess potential threats and improve security. On-demand access is provided and the security of log retention devices is constantly monitored. Hitachi Security Systems offers options for Ethernet-enabled devices and has experience working with PCS and SCADA systems.

[WWW.HITACHI-SYSTEMS-SECURITY.COM](http://WWW.HITACHI-SYSTEMS-SECURITY.COM)

# LogRhythm



 4780 Pearl East Circle, Boulder, CO 80301

 (303) 413-8745

 [info@logrhythm.com](mailto:info@logrhythm.com)

## DESCRIPTION OF COMPANY:

LogRhythm specializes in Threat Lifecycle Management, which empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyberthreats.

## ADDITIONAL DETAILS:

- Founded in 2003.
- Headquartered in Boulder, CO.
- 500–1000 employees.
- Customers include Energy and Utilities, Banking and Finance, Healthcare, Defense, Retail.
- Has NERC CIP compliance expertise.
- Has ICS/SCADA systems expertise.
- Has experience working with utilities.

- Endpoint Security
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:


- LogRhythm uses customized Endpoint Behavior Analysis and a Threat Detection tool with big data analytics combined into the system to detect endpoint anomalies and eliminate compromised hosts.
- As a part of its Retina CS services LogRhythm provides for Vulnerability Assessments and remediation, accurate asset discovery policy drive scans and misconfiguration identification.
- Advanced Agent Technology from LogRhythm includes the so-called active encryption and File Integrity Monitoring (FIM).
- SIEM services are provided through its Next-Gen SIEM tool.
- LogRhythm incorporates threat intelligence from STIX/TAXII-compliant providers, commercial and open source feeds, and internal honeypots, using an integrated threat intelligence ecosystem. The platform uses this data to reduce false-positives, detect hidden threats, and prioritize marked concerns.
- Generate irrefutable network-based evidence for threat analysis, policy enforcement, and legal action.

[HTTPS://LOGRHYTHM.COM](https://logrhythm.com)

# Lumension Security Inc



 8660 East Hartford Drive, Scottsdale, AZ 85255

 (602) 566-5900

 sales@lumension.com

## DESCRIPTION OF COMPANY:

Lumension is a security software solution provider that offers endpoint management, data protection, managed security service, and proactive risk management, to improve audit readiness for NERC CIP.

## ADDITIONAL DETAILS:

- Founded in 1991.
- 200–500 employees.
- Has offices in Austin, TX.
- Serves more than 3,000 clients globally.
- Works with businesses and industries of all sizes.
- Has electricity sector experience.
- Has NERC CIP compliance expertise.

- Endpoint Security
- Patch Management
- Privileged Data Management
- Security Information and Event Management
- Single-File Encryption Software
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Endpoint security, privileged data management offered using the company's Lumension Scan, Devise Control, Application Control, AntiVirus, and Security Configuration Management software.
- Security advisory service provided to help client model incoming threat and develop security programs or assess existing program.
- Encryption software for whole disk encryption.
- SIEM through company platform.
- Stay on top of latest security trends through company's webcasts.
- NERC CIP compliance (CIP-002-1, 003-1, 005-1 to 009-1) provided through company's various software platforms including Patch and Remediation, Application Control, and the Scan software.
- Lumension's MSSP maintains all security related hardware and software, perform assessment and threat remediation, and provide ongoing security monitoring.
- Onsite deployment service as well as security training.
- Security plan design.

[WWW.LUMENSION.COM](http://WWW.LUMENSION.COM)

## Masergy



 2740 North Dallas Parkway, Suite 260, Plano, TX 75093

 (866) 588-5885

 [info@masergy.com](mailto:info@masergy.com)

### DESCRIPTION OF COMPANY:

Masergy owns and operates its own software platform for managed security, hybrid network working, and cloud communication.

### ADDITIONAL DETAILS:

- Founded in 2000.
- 201–500 employees.
- Has experience working with utilities.
- Has electricity sector experience.
- Has NERC CIP compliance expertise.

- Bring Your Own Device Provisioning for Company and Personal Devices (only for communications through Masergy's app)
- Endpoint Security
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:


- Endpoint security and monitoring is provided through the APTM (Advanced Persistent Threat Management) module which is a part of the Unified Enterprise Security suite of the Masergy's managed security solutions.
- Integrated vulnerability assessments/scanning, which automatically correlates results with IDS/IPS.
- SIEM includes integrated real-time monitoring, log management/ archival, analysis and reporting, learning normal network behaviors and correlate all sub-system data to identify abnormal behaviors.
- BYOD is allowed for communications using Masergy's app.
- Provides custom routers to manage security risks in case connected with personal devices.
- Provides Network Access Policy Monitoring — Defines and enforces corporate network security policy with continuous monitoring and advanced behavioral network analysis and correlation.
- Expert services for compliance and penetration testing.

[WWW.MASERGY.COM](http://WWW.MASERGY.COM)

# Morphick



 4555 Lake Forest, Suite 150, Cincinnati, OH 45242

 (844) 506-6774

 <http://www.morphick.com/contact>

## Description of company:

Morphick is a computer security company that employs customized and adaptive systems to provide security for its clients.

### ADDITIONAL DETAILS

- Founded in 2013.
- 50–200 employees.
- Offers services to all businesses and customizes its offerings to each business.

- Endpoint Security (with endgame security)
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## Description of services/ products provided:

- Primary offerings are threat detection and response, and endpoint threat detection and response.
- Endpoint security: Morphick partners with Endgame and delivers both threat detection and response systems, along with Endgame's endpoint threat detection and response.
- Vulnerability assessments: a-la-carte security defense assessment (examines the security of the system), and compromise assessment (determines if there exists a current security breach).
- Creation of custom threat detection routines to target specific problems if they arise.
- Focus on repelling repeat or persistent attackers by dynamically changing the security posture of the business without affecting its running.
- Proactive threat hunting — Morphick doesn't just respond to threats, its analysts actively monitor the network to detect known and unknown threats.
- One of a small number of firms to be awarded the NSA's Cyber Incident Response Assistance (CIRA) certification.

[WWW.MORPHICK.COM](http://WWW.MORPHICK.COM)

## Mosaic451



3838 North Central Ave., Suite 2050, Phoenix, AZ 85012



(888) 364-0803



<https://www.mosaic451.com/company/about-us/contact>

### Description of company:

Mosaic451 is an information security company with a focus on Security Operations Center (SOC) and Network Operation Center (NOC) services.

#### ADDITIONAL DETAILS

- Founded in 2012.
- Headquartered in Phoenix, AZ.
- Has 95 employees.
- Has offices in Las Vegas, NV, Portland OR, and Boston, MA.
- Has energy sector experience.
- Provides information security services for companies at a national level including those in Power, Gas Extraction, Financial Services Sector, Transport, Government, and K-12 Education.
- Has NERC CIP compliance expertise.
- Has SCADA systems expertise.

### Description of services/ products provided:

- Mosaic451 provides security software management, including patch management.
- Mosaic451 provides vulnerability management services
- Log Management.
- The company proposes a hybrid model with on-site dedicated SOC and remote monitoring.
- Key controls and compliance reporting for regulations such as PCI, HIPAA, SOX, FISMA, and CIP.
- Offers SCADA compliance solutions.

[WWW.MOSAIC451.COM](http://WWW.MOSAIC451.COM)

- Endpoint Protection
- Patch Management
- Security Information and Event Management
- Vulnerability Assessments

## N-Dimension Solutions, Inc.



15305 Dallas Parkway, Suite 300, Addison, TX 75001

(905) 707-8884

sales@n-dimension.com



### Description of company:

N-Dimension solutions delivers comprehensive managed security services specifically tailored to protect critical energy infrastructure from cyber threats and vulnerabilities, improving system reliability and safe guarding assets.

#### ADDITIONAL DETAILS

- Founded in 2001 with < 50 employees.
- Creates solutions specially designed for the utility sector and has worked with a large number of utility companies.
- Has ICS/SCADA systems expertise.
- Has energy sector experience.
- Has NERC CIP compliance expertise.

- Bring Your Own Device Provisioning for Company and Personal Services
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### Description of services/ products provided:

- N-Dimension's solution provides on-going assessment of endpoints (including servers, ICSs, desktops, laptops, smartphones and more) connected to a network, providing an up-to-date view of vulnerabilities in the system. Daily reports provide recommendations and prioritization of vulnerabilities. It also provides cybersecurity experts a chance to review reports and answer questions as they arise.
- Provides monitoring and vulnerability assessments for ICS, DCS, SCADA, etc. It also provides this service for users personal devices (laptops, smartphones, etc.) if they must be connected to the network.
- N-Dimension provides a comprehensive monitoring solution which manages event information, provides alerts, and recommendations for further action.
- Maintains up-to-date intelligence on the latest threats for effective monitoring and assessment.
- N-Dimension is capable of making recommendations of which partners and services may be required for the given client.


[WWW.N-DIMENSION.COM](http://WWW.N-DIMENSION.COM)



# NetWatcher



 1861 Wiehle Ave, Suite 250, Reston, VA 20190

 (202) 630-7849

 <https://netwatcher.com/contact>

## Description of company:

NetWatcher is a medium and small business focused MSSP with technology built for the mid-market.

### ADDITIONAL DETAILS

- Founded in 2014.
- 11-50 employees.

- Bring Your Own Device Provisioning for Company And Personal Services
- Endpoint Security
- Patch Management
- Security Information and Event Management

## Description of services/ products provided:

- Affordable managed security solutions including detection and monitoring of security events.
- Endpoint security, for VPNs, log forwarding and behavioral monitoring, also works if mobile users connect via unsecured Wi-Fi.
- Patch management, software is kept up to date and maintained by NetWatcher.
- NetWatcher offers detailed reporting on the security of the network, including potential vulnerabilities and security incidents.
- NetWatcher's software allows users to connect remotely and remain secure and monitored.
- NetWatcher also provides monitoring of file integrity and logs to ensure data is secure.
- Endpoint health and hygiene scores allow quick assessment of the state of the network.
- NetWatcher provides support and guidance on how to best deal with security issues.


[HTTPS://NETWATCHER.COM](https://netwatcher.com)




## Nexum, Inc.



 190 S. LaSalle St., Suite 1450, Chicago, IL 60603

 (312) 726-6900

 <https://www.nexuminc.com/company/contact>

### DESCRIPTION OF COMPANY:

Nexum is dedicated to computer security with offerings that target small and medium businesses and with particular experience in military applications.

### ADDITIONAL DETAILS:

- Founded in 2002.
- Headquartered in Chicago, IL.
- 51-200 employees.
- Has particular offerings for small and medium businesses.

- Endpoint Security
- Privileged Data Management
- Patch Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Separates offerings into identification, protection, and detection services, and has offerings aimed at small businesses for all of these.
- Endpoint security which organizes, monitors, and administrates networks.
- Privileged data management provides custom configurations after consultation. Nexum has experience developing and implementing these systems for military application where security is a high priority.
- Patch management services to deliver patches and software updates, and keeps the system and configurations up to date as part of its management services.
- Vulnerability assessments as a separate service.
- SIEM as part of the management service. Nexum collects, collates, retains, and analyzes logs in real time to determine the security of the network.
- Has a large number of clients in primarily public services and military.
- Offers on-site support, if requested.

[WWW.NEXUMINC.COM](http://WWW.NEXUMINC.COM)

# NTT Security



9420 Underwood Avenue, Omaha, NE 68114

(402) 361-3000

us-info@nttsecurity.com

## DESCRIPTION OF COMPANY:

An MSSP aimed at mid- to large-size businesses (50+ employees) which explicitly offers security solutions for the utility industry, including PCS, DCS and SCADA systems.

## ADDITIONAL DETAILS:

- Has NERC CIP compliance expertise.
- Has experience in the electric utility sector, including experience working with many devices, including PCS, DCS and SCADA systems.
- Specializes in security solutions for medium-size businesses (50+ employees).
- NTT-Security is a worldwide organization with four offices in the USA, 10 Security Operations Centers and 7 R&D centers, 1,500+ employees across the globe, more than 10,000 clients worldwide, and more than 6.2 billion attacks detected and defended against per year.

- Endpoint Security
- Patch Management
- Privileged Data Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:


- Provides monitoring services for over 205 device types.
- Tailored services for client-specific needs.
- NTT-Security provides targeted threat intelligence, network access control, log monitoring and management, vulnerability management, security device management and mobile solutions management.
- NTT-Security will manage a large number of third-party vendors' access control solution, firewalls and malware protection solutions, endpoint security, VPNs, web applications, network devices, operating systems, and unified threat management solutions. NTT-Security works with the business to design a security system which is right for them.
- NTT-Security offers a patch management solution as part of its managed security devices suite of services.
- Allows a selection of multiple vulnerability scanning services including internal and external vulnerability scanning, change enforcement control and penetration testing.
- As a managed service, NTT-Security scans on behalf of the client, but the client retains on-demand control. NTT-Security also helps clients choose the best platform for vulnerability lifecycle management.

[WWW.NTTSECURITY.COM](http://WWW.NTTSECURITY.COM)

# Nuspire Networks



 3155 Dallavo Ct, Commerce Charter Twp, MI 48390

 (877) 435-1640

 [info.na@nuspire.com](mailto:info.na@nuspire.com)

## DESCRIPTION OF COMPANY:

MSSP which emphasizes work with small/medium businesses and has experience in the energy and utility industries, including working with plant equipment and PCs.

## ADDITIONAL DETAILS:

- Founded in 1999.
- Headquartered in Walled Lake, MI.
- 50–200 employees.
- Works with small and medium businesses to global enterprises.

- Employee Bring Your Own Device (BYOD) support possible
- Endpoint Protection
- Patch Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Nuspire has the capacity for endpoint security. Combine expertise of security analytics team with the company's nuEndpoint technology to deliver security as a service from the cloud.
- Patch management through comprehensive gateway solutions.
- Security Information and Event Management is handled by the NuSecure nuSIEM platform. Cloud based service ensures logs and intelligence reports are processed and analyzed in real time, providing faster reaction to security events and alerts.
- Up-to-date information on Intrusion protection, vulnerabilities, etc.
- Fully staffed 24/7/365 Security Operations Center provide expertise for threat analytics as well as quick alert response and threat remediation.
- In house security engineering and R&D team constantly investigate and understand customer's network assets, research security threats, and develop solutions.
- Rogue wireless access point detection add extra layer of security to organization offering BYOD policies, by providing necessary hardware to actively scan for unauthorized access points.

[WWW.NUSPIRE.COM/MSS/MANAGED-SECURITY-SERVICES-OVERVIEW](http://WWW.NUSPIRE.COM/MSS/MANAGED-SECURITY-SERVICES-OVERVIEW)

# Palo Alto Networks



 4401 Great America Parkway, Santa Clara, CA 95054

 (866) 320-4788

 [info@paloaltonetworks.com](mailto:info@paloaltonetworks.com)

## DESCRIPTION OF COMPANY:

Product provider focusing on integrated and automated security platform that includes advanced firewall, network monitoring, endpoint protection, and cloud service threat control.

## ADDITIONAL DETAILS:

- Founded in 2005.
- 1,000–5,000 employees.
- More than 35,500 customers in 140 countries worldwide.
- Works with customers that range from small and medium businesses to global enterprises.
- Experience with utility customers.
- Has ICS/SCADA systems expertise.
- Has NERC CIP compliance expertise.

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Capacity for endpoint security. Palo Alto Networks' Traps system combine malware and exploit prevention to pre-emptively block both known and unknown threats.
- Offers options for Ethernet-enabled devices and security platform products for ICS/SCADA security.
- Security Information and Event Management is centrally managed in the endpoint security manager software.
- Up-to-date information on Intrusion protection, vulnerabilities, etc.
- Network-based security, stream-based malware protection, URL, file and data filtering, and policy based access management are also provided.

- Endpoint Protection
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds

[WWW.PALOALTONETWORKS.COM/SOLUTIONS/INDUSTRIES/ENTERPRISE/ELECTRIC-UTILITIES](http://WWW.PALOALTONETWORKS.COM/SOLUTIONS/INDUSTRIES/ENTERPRISE/ELECTRIC-UTILITIES)

# Proficio



 3264 Grey Hawk Court, Carlsbad, CA 92010

 (450) 430-8166

 <https://www.proficio.com/contact>

## DESCRIPTION OF COMPANY:

An MSSP that provides security services and has experience in the energy sector, including working with ICS/SCADA systems.

## ADDITIONAL DETAILS:

- Founded in 2010.
- Headquartered in Carlsbad, CA.
- 50–200 employees.
- Has offices in Singapore and Spain.
- Works with mid- to large-sized enterprises.
- Has experience working with utilities.
- Has electricity sector experience.
- Has NERC CIP compliance expertise.
- Has ICS/SCADA systems expertise.

- Endpoint Protection
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Award-winning MSSP offering a full range of cybersecurity services including managed detection and response (MDR).
- Endpoint security through the ProSOC platform. The company provides 24/7 security event monitoring, threat correlation analysis, incident response, and forensic investigation service.
- Identity/privileged access management is offered through a partner (Thycotic).
- Vulnerability assessments services are offered. Proficio provides risk assessments, penetration testing, and code review, among other services that help organizations gain better understanding of their assets and threats.
- Up-to-date information on Intrusion protection, vulnerabilities, etc.
- Advanced SIEM analysis.
- Offers options for Ethernet-enabled devices and has experience working with ICS and SCADA systems.
- The cloud-based security operation center (SOC) provides detection, protection and automated incident response.
- Help increase visibility and proactively investigate and hunt for known and unknown threats.
- 24/7 managed security services.
- Scalable deployment.

[HTTPS://PROFICIO.COM](https://www.proficio.com)

# Rapid7



100 Summer Street, 13th Floor, Boston, MA 02110

(617) 247-1717

info@rapid7.com

## DESCRIPTION OF COMPANY:

Rapid7 is a security data and analytics solution provider that also offers MSSP services using in-house products and solutions and provides wide range of services.

## ADDITIONAL DETAILS:

- Founded in 2000.
- 500–1,000 employees.
- More than 6,000 clients in 110 countries worldwide.
- Works with businesses and industries of all sizes.
- Has electricity sector experience.
- Has NERC CIP compliance expertise.
- Has ICS/SCADA systems expertise.

- Endpoint Protection
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Endpoint security offered using company's Nexpose vulnerability management solution to visualize endpoint risk and remediate the threat. The company also offers other products with web application security testing capabilities.
- Security advisory service provided to help clients model incoming threats and develop security programs or assess existing programs.
- Security information and event management solution offered through InsightIDR product.
- Active community sharing threat intelligence and latest threats.
- NERC CIP compliance through the company's Nexpose and Metasploit product for penetration testing, vulnerability scans, and automatic asset discovery. Security Advisory Service also offered to assess and help achieve compliance.
- Managed detection and response service provide 24/7 detection and response service that act immediately when breaches happens, allowing quick response time.
- Compromised credentials detection with company's InsightIDR solution, as well as user behavior analysis.
- Penetration testing services are offered for all possible situations including: internal and external networks, wireless networks, mobile applications, physical devices, and social engineering penetration.

[HTTPS://RAPID7.COM/SOLUTIONS/INDUSTRY/ENERGY](https://rapid7.com/solutions/industry/energy)

## RAVENii



 17501 W. 98th St. Pillar, #18-33, Lenexa, KA, 66219

 (844) 317-0944

 [inquiries@RAVENii.com](mailto:inquiries@RAVENii.com)

### DESCRIPTION OF COMPANY:

RAVENii provides continuous threat and vulnerability management, firewall management, managed endpoint protection, and incident response. RAVENii provides a comprehensive endpoint security solution which includes CylancePROTECT anti-virus protection.

### ADDITIONAL DETAILS:

- Founded in 2014.
- 10-50 employees.
- RAVENii advertises its MSSP as a three-tier system.
  1. The first tier includes licensing, maintenance, and administrative upkeep, but the customer operates the solution.
  2. Tier two builds upon this by also providing the day-to-day management and operation of the solution.
  3. Tier three adds incident management and triage activity for critical security incidents.
- Has experience working with utilities.
- Has energy sector experience.

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- RAVENii provides security assessment services, which can be run continuously, and active assessments that can run regularly. RAVENii also provides compliance assessments and vulnerability management in the form of a debrief — a reporting portal and analysis, remediation plans and the ability to deploy updates.
- Specializes in securing Internet of Things (IoT) devices.
- Encryption is available as part of the bundle of services.
- Daily vulnerability assessments, security/application/system/custom log file monitoring are services available.
- Device tracking and reclamation.
- Complete security information and event management and log management for installed security devices.
- Provision for personal and company devices to access the network and be included in vulnerability assessments.
- Remote assistance and backups for single files to entire systems.

- Bring Your Own Device Provisioning for Company And Personal Services
- Endpoint Security
- Patch Management
- Security Information and Event Management
- Single-File Encryption Software
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

[WWW.RAVENII.COM](http://WWW.RAVENII.COM)



# Redhawk



62958 Layton Ave., Suite One, Bend, OR 97701

(541) 382-4360

sales@redhawksecurity.com

## DESCRIPTION OF COMPANY:

Redhawk Network Security provides a multi-faceted view into the company's security environment.

## ADDITIONAL DETAILS:

- Founded in 2000.
- Headquartered in Bend, Oregon.
- 11-50 employees.
- Has an office in Austin, TX.
- Services Utilities, Healthcare, Government Services (NIST, CJIS, FISMA), Indian Gaming Sites, and Financial Institutions.
- Has NERC CIP compliance expertise.

- Patch Management
- Security Information and Event Management
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- MSSP and consulting services. Redhawk's network security services comprises of PCI, HIPAA and NERC CIP compliances, Security Assessments, Managed Security, Penetration Testing, Vulnerability Management, Risk Management and many other features.
- Redhawk provides maintenance administration, upgrades, patches and incident response, thereby, covering the patch management aspect.
- Vulnerability Management is a key part of the of the services by Redhawk. The managed process finds known vulnerabilities in networks and applications.
- SIEM services comprises of Redhawk's SecureSensor™ Solution that ensures maintenance, configuration, incident response, vulnerability scanning and security testing. Testing helps assure that systems are updated and changes do not create new vulnerabilities. Scan observations include risk analysis with assigned risk levels and technical recommendations for remediation. Monitoring, alert and event management are available 24/7/365. The services also include archiving of files — policies, procedures, and managed service reports.

[WWW.REDHAWKSECURITY.COM/MANAGED-SERVICES](http://WWW.REDHAWKSECURITY.COM/MANAGED-SERVICES)



## RedSeal, Inc.



940 Stewart Drive, Sunnyvale, CA, 94085

(408) 641-2200

info@redseal.net

### DESCRIPTION OF COMPANY:

RedSeal provides a cyber-security analytics platform. The platform provides companies with a Digital Resilience Score which acts as a simple metric for how effectively RedSeal's current security measures are working to protect its network.

### ADDITIONAL DETAILS:

- Has more than 100 employees.
- Has experience working with utilities.
- Has energy sector experience.
- Has NERC CIP v5 compliance expertise.
- Has SCADA systems expertise.
- Customers include: Adobe Systems, Capital One, PG&E, Cisco Systems, U.S. Department of Defense, and the U.S. Army.

### DESCRIPTION OF SERVICES/ PRODUCTS PROVIDED:

- Provides endpoint security and monitoring.
- Builds map of an organization's technology and connectivity to provide a view of the security posture and identify vulnerabilities.
- RedSeal provides a simple metric and identifications of vulnerabilities.
- RedSeal works with utilities customers to secure corporate networks and those that control critical equipment, Supervisor Control, and Data Acquisition (SCADA) networks.
- Mobile and personal device security is likely to be provided as RedSeal displays its Digital Resilience Score on assorted mobile devices.


- On-Demand Analysis of Security Posture
- Vulnerability Assessments

[WWW.REDSEAL.NET](http://WWW.REDSEAL.NET)

# Rendition Infosec



 451 Sugarcreek Dr., Grovetown, GA 30813

 (888) 409-5811

 [inquiry@renditioninfosec.com](mailto:inquiry@renditioninfosec.com)

## DESCRIPTION OF COMPANY:

Rendition Infosec is a full-service security consulting firm that provides a wide variety of services ranging from managed security service, endpoint and network monitoring to incident response and threat information and intelligence sharing.

## ADDITIONAL DETAILS:


- Founded in 2014.
- 10-50 employees.
- Has experience working with utilities.

- Endpoint Security
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- The company can perform endpoint security and network monitoring, as well as intrusion detection through a combination of its custom monitored web application firewall (WAF) and partner SIEM platform.
- Vulnerability assessments and audit services are provided. The company's Advanced Persistent Threat Adaptive Penetration Testing (APT2) model helps businesses address real world threats and risks. Vulnerability and penetration testing are also available for institutions with wireless networks.
- Security information and event management platforms are available (through partnership with AlienVault).
- Monthly webcast of intelligence and threat highlights are offered to clients for the latest scoop on the security landscape.
- Incident response retainer, forensic analysis, botnet analysis, and cyber threat intelligence helps clients better understand the threats and assist in threat remediation.
- Staff mentoring helps develop client's security staff and keeps them up to date on latest security trends and new practices.
- Periodic phishing assessments to prevent phishing attacks.

[WWW.RENDITIONINFOSEC.COM](http://WWW.RENDITIONINFOSEC.COM)

**root9B** 102 North Cascade Ave., Suite 220, Colorado Springs, CO 80903 (719) 505-6717 info@root9b.com**DESCRIPTION OF COMPANY:**

root9B protects a wide range of commercial industries for the federal and local governments.

**ADDITIONAL DETAILS:**

- Founded in 2011.
- Has about 200 employees.
- Customers include both commercial and public entities of all sizes.

- Patch Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

**DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:**

- Vulnerability assessments: root9B provides a comprehensive analysis of the system's vulnerabilities using custom software which identifies the critical links attackers will exploit.
- Extensive analysis of security events to prevent future vulnerabilities.
- Cutting edge knowledge of the security environment, deployed as soon as the information becomes available.
- Manned Information Security solution actively hunts attackers in the network and deploys countermeasures to neutralize them.
- root9B's Adversary Pursuit Center allows remote anomaly analysis, incident response, malware analysis and credential security.
- root9B's offerings are more training focused than a traditional MSSP.
- Offers beginner to advanced security training.
- root9B produces a short term, medium term, and long term plan together with the client to satisfy their security needs.

[WWW.ROOT9B.COM](http://WWW.ROOT9B.COM)

# SageNet



10205 E. 61st Street, Tulsa, OK 74133

(918) 270-7000

info@sagenet.com

## DESCRIPTION OF COMPANY:

SageNet designs, implements and manages networks. SageNet manages communications at more than 160,000 locations around the nation.

## ADDITIONAL DETAILS:

- SageNet was founded in 1998, following a merger with Spacenet, founded in 1981.
- SageNet Acquired Turnberry Solutions' Cybersecurity Division in 2015.
- Targets customers in the retail, healthcare, financial, energy, and public utilities sectors.
- Experience working with state lotteries and government agencies.

- Endpoint Security
- Patch Management
- Privileged Data Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Cryptzone provides a software perimeter using VPN and a jump server.
- Develop authentication methods including hardware tokens, software tokens or other multifactor methods to protect on prem, cloud based or 3rd party hosted systems and information.
- Deployment of patches and countermeasures is considered under vulnerability Management Services.
- SageNet performs Pen Tests involving Reconnaissance, Vulnerability Identification, Attack Planning, Vulnerability Exploitation, Clean Up and Reporting.
- Next Generation Firewalls (NGFW).
- 24x7 Security log.
- SIEM runs on Amazon Web Services.
- Firewall Management.
- IPS/IDS Protection.
- Data Loss Protection.
- Content Filtering.

[WWW.SAGENET.COM/MARKETS/CYBERSECURITY-SOLUTIONS/MANAGED-SECURITY-SERVICES](http://WWW.SAGENET.COM/MARKETS/CYBERSECURITY-SOLUTIONS/MANAGED-SECURITY-SERVICES)

## SecureWorks



1 Concourse Pkwy NE, #500, Atlanta, GA 30328

(877) 838-7947

[www.secureworks.com/contact/talk-with-an-expert](http://www.secureworks.com/contact/talk-with-an-expert)

### DESCRIPTION OF COMPANY:

SecureWorks is an MSSP with a focus in SaaS-based early-warning systems and has experience in the energy and utility industries, including working with power plant thread detection and vulnerability patching.

### ADDITIONAL DETAILS:

- Founded in 1999.
- Has more than 10,000 employees.
- More than 4,300 clients in 59 countries worldwide.
- Works with businesses and industries of all sizes.
- Has electricity sector experience.

- Bring Your Own Device (BYOD) Provisioning
- Endpoint Protection
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Endpoint security service offered. Uses both typical preventative endpoint protection products — such as data encryption, device and application control, VPN anti-malware/phishing, and vulnerability shielding — as well as advance malware detection tools that actively identify malware through behavioral characteristics analysis.
- Vulnerability assessments services are offered. SecureWorks offers various levels of assessment solutions including deploying on-site technicians to establish a security baseline, identify issues, and validate patching and hardening program.
- Up-to-date information on Intrusion protection, vulnerabilities.
- Incident Response team helps develop incident response plan, Incident Response Management Retainer guarantees assistance to mitigate and help recovery from a security breach.

[WWW.SECUREWORKS.COM](http://WWW.SECUREWORKS.COM)

# SecurIT360



 530 Beacon Pkwy W, Suite 901, Birmingham, AL 35209

 (205) 202-4233

 [contact@securit360.com](mailto:contact@securit360.com)

## DESCRIPTION OF COMPANY:

SecurIT360 provides consultation, security audits, and training, as well as endpoint monitoring and incident response service.

## ADDITIONAL DETAILS:

- Founded in 2009.
- 10–50 employees.
- Works with businesses and industries of all sizes
- Has experience working with utilities.

- Endpoint Security
- Security Information and Event Management
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Endpoint security service offered. Endpoint logs are monitored with the company's Logit360 solution that provides features such as remote monitoring, alerting, event correlation, etc.
- Vulnerability assessments and auditing service offered to assess the security readiness of the client. Service is tailored to client's specific need, from as small as auditing security configuration of firewalls to full blown auditing of organization's security plan, infrastructure, and so forth.
- Security information event management through Logit360 solution.
- Penetration testing offered for both internal and external networks, as well as physical and social engineering penetrations.
- Incident Response team ready to deploy at moment's notice to help clients in case of a breach.
- Incident analysis provides expertise and assistance to assess a breach, estimate the damage, and formulate remediation actions.
- Training offered either online or in person to help bring client's staff up to speed to the latest security landscape.

[WWW.SECURIT360.COM/SERVICES](http://WWW.SECURIT360.COM/SERVICES)

## Security On-Demand



12121 Scripps Summit Drive, Suite 320  
San Diego, CA 92131

(858) 693-5655

info@securityondemand.com

### DESCRIPTION OF COMPANY:

Security On-Demand is a comprehensive MSSP with a focus on small/medium businesses. It provides security from the endpoint to the cloud, rapidly detecting threats, and has experience with utility companies.

### ADDITIONAL DETAILS:

- Founded in 2001.
- Has security operations centers in San Diego, California, and Arlington, Virginia.
- Has experience working with utilities.
- Has experience working with local government.
- Extensive experience with medium/small businesses.
- Has electricity sector experience.
- Has NERC CIP compliance expertise.

- Bring Your Own Device Provisioning for Company and Personal Services
- Endpoint Security
- Patch Management
- Privileged Data Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:


- Managed intrusion prevention service, including protection for unpatched systems.
- Threat and log analysis.
- Malware threat protection service; scans files on the network, in email, uploads suspicious files on demand and protects against advanced threats. The company inspects the system across all operating environments and gives full threat lifecycle information.
- Managed firewall service with the ability to add web content filtering, anti-malware, web-based application protection and more.
- Patch management and delivery for security devices through the Managed Firewall Service.
- Vulnerability assessments tool which includes vulnerability management and reporting, and scans and reports for compliance mandates, also provides Vulnerability assessments and monitoring for both company and personal devices.
- Managed intrusion prevention provides security event alerts, investigation, and response. Ensures compliance is maintained and can protect unpatched systems.
- Managed Network Access Control Service ensures each endpoint is only able to access its authorized resources and information. Also enforces organization policy, including patch requirements for connected devices.

[WWW.SECURITYONDEMAND.COM](http://WWW.SECURITYONDEMAND.COM)

## Sedara



 77 Goodell St., #420, Buffalo, NY 14203

 (844) 473-3272

 [Info@sedarasecurity.com](mailto:Info@sedarasecurity.com)

### DESCRIPTION OF COMPANY:

Sedara is an MSSP with strong partnerships with AlienVault and Bit9 + Carbon Black. By such partnerships, Sedara can add capabilities to its existing cybersecurity abilities.

### ADDITIONAL DETAILS:

- Services small to large businesses.
- Has NERC CIP compliance expertise.

- Endpoint Security
- Security Information and Event Management
- Single-File Encryption Software
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/ PRODUCTS PROVIDED:

- Endpoint security is offered through its partnership with Bit9 + Carbon Black. The security will provide for application whitelisting and detailed application audit trails. In addition, it will only allow for approved applications to be run on company systems. If an intrusion, virus or malware outbreak occurs, Sedara can perform incident response on those systems in seconds.
- Sedara leverages AlienVault's Unified Security Management™ (USM) solution to provide a flexible SIEM platform. The program allows for real-time correlation and identification of unwanted behaviors using event, threat, and risk information together.
- As a part of NERC CIP and HIPAA compliance adherence, Sedara offers comprehensive vulnerability assessments. Its Intrusion Detection System (IDS) monitors the activities, to look for internal and external violations, and sends alerts for suspicious behavior.
- Above capabilities are often coupled with integrated Intrusion Detection System, log and asset management to provide for a complete solution. In addition, the services are customizable to one's needs.


[WWW.SEDARASECURITY.COM](http://WWW.SEDARASECURITY.COM)



## Sera-Brynn



 5806 Harbour View Blvd., #204, Suffolk, VA, 23435

 (757) 243-1257

 [info@sera-brynn.com](mailto:info@sera-brynn.com)

### DESCRIPTION OF COMPANY:

Sera-Brynn is a cybersecurity audit and advisory firm. The company works with legal, insurance, accounting, and law enforcement industries to provide the best protection possible.

### ADDITIONAL DETAILS:

- Founded in 2011.
- Has approximately 50 employees.
- Works with midsize companies, governmental organizations and non-profits.
- Expertise in compliance testing and auditing.

- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Consultancy firm for businesses that require occasional or project-specific security and compliance assistance.
- Vulnerability assessments: Sera-Brynn provides a full Cyber Risk assessment, which discovers the vulnerabilities and risks of the system, compliance requirements and the steps forward in securing the system.
- Security information and event management: Cyber-forensics included as part of the incident response service offering.
- A comprehensive incident response service is available, assessing, containing, analyzing and cleaning up the damage, while working with law enforcement and legal representatives if needed.
- Consulting services provided as required security services, saving money and time, while providing the expertise when it's needed.
- Extensive penetration testing is available and the results are presented in a business-centric way.
- Extensive vulnerability testing services.

[HTTPS://SERA-BRYNN.COM](https://sera-brynn.com)

## Solvere One



601 Pennsylvania Ave., NW, #900, Washington, DC 20004



(202) 905-2722



info@solvere.com

### DESCRIPTION OF COMPANY:

Solvere One is an IT consulting and outsourcing company specialized in security and policy compliance, offering services including vulnerability assessments, CIO and CTO support, as well as managed security as a service.

### ADDITIONAL DETAILS:

- Founded in 2008.
- 50–200 employees.
- Serving and providing on-demand IT and consulting to over 300 offices worldwide.
- Works with businesses of all sizes and industries.
- Experience in the electricity sector.

- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/ PRODUCTS PROVIDED:

- Vulnerability assessments services are offered to analyze client's network environment. This includes constant scanning and monitoring vulnerabilities.
- SIEM through log management, SIEM event correlation, netflow analysis, and other service availability monitoring are available through a unified management console.
- Managed detection and response service provides 24/7 detection and response service that act immediately when breach happens; this allows for quick response time.
- Penetration testing service to assess network security risk, review network design, and policy.
- Incident response and forensics to analyze threat.
- Leverage Windows Rights Management System to provide encryption and content security.

[WWW.SOLVEREONE.COM](http://WWW.SOLVEREONE.COM)

## SpearTip



1714 Deer Tracks Trail, Suite 150, St. Louis, MO 63131  
 (800) 236-6550  
<http://www.speartip.com/company/contact-us/#content>

### DESCRIPTION OF COMPANY:

SpearTip is an MSSP with strong roots in Cyber Counterintelligence. The company specializes in analyzing cyber threats including espionage and terrorism to deliver custom solutions. SpearTip's Cyber Counterintelligence Team conducts penetration testing, malware analysis, digital forensics, human intelligence collection (HUMINT), pre-attack intelligence analysis, open source data review, elicitation techniques, and technical surveillance countermeasures (TSCM). These areas of expertise include specialized enterprise risk management service mapped to COBIT, NIST, ISO, and/or other industry standards.

### ADDITIONAL DETAILS:

- SpearTip serves small businesses including retail shops.
- The company's usual clients include financial and healthcare firms.

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- SpearTip provides endpoint security using Network-based advanced malware detection and malware analysis, and peer-to-peer data leak monitoring.
- Subscriptions to threat information intelligence feeds.
- Its host-based advanced malware detection and malware analysis uses active memory analysis with key features such as reverse engineering and zero-day identification.
- SpearTip also uses DarkNet research to identify the human operator behind an attack.
- The assessment services include penetration testing, web-application testing, and other tools for proactive compliance management.

- Endpoint Security
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

[WWW.SPEARTIP.COM/MANAGED-SERVICE-PROVIDER](http://WWW.SPEARTIP.COM/MANAGED-SERVICE-PROVIDER)

# Symantec



 350 Ellis Street, Mountain View, CA 94043

 (650) 527-8000

 <http://partnerlocator.symantec.com>

## DESCRIPTION OF COMPANY:

Symantec offers a variety of services and products targeting a wide array of industries and all service sizes.

## ADDITIONAL DETAILS:

- Founded in 1982.
- 10,000+ employees (>1,000 in MSSP cybersecurity teams).
- Offers a wide range of security products from OTS software to full MSSP services.
- Offers services to businesses of all sizes and targets many industries, including, industrial & utilities.
- Has particular offerings for the devices used in industrial processes, i.e. PLCs and more.

- Endpoint Security
- Patch Management
- Privileged Data Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Endpoint security is a main feature of the MSSP offering. Engineers assess the business and implement a solution based on the field.
- Symantec offers a number of services, including account and data management.
- Vulnerability assessments are available as a separate service.
- Log retention and analysis provides improved detection and system assessment.
- Assists with compliance reporting when requested.
- ICS asset detection, anomaly detection, and automated learning.
- Internet of Things (IoT) security, including industrial equipment (PLCs, etc.).
- A dedicated team of engineers is assigned to a business, and stays with it, allowing monitoring and updates by people who know the system.
- Bring your own device provisioning for company and personal services

[WWW.SYMANTEC.COM/SERVICES/CYBER-SECURITY-SERVICES/MANAGED-SECURITY-SERVICES](http://WWW.SYMANTEC.COM/SERVICES/CYBER-SECURITY-SERVICES/MANAGED-SECURITY-SERVICES)

## Tagrem Security



 9820 Willow Creek Road, Suite 390, San Diego, CA 92131

 (800) 867-1375

 info@tagrem.com

### DESCRIPTION OF COMPANY:

Tagrem is a global eCommerce agency providing enterprise software, technology and digital marketing solutions to large- and medium-size organizations in the United States and around the world.

### ADDITIONAL DETAILS:

- Founded in 1999.
- Currently a small company with less than 50 employees in IT.
- Founded in San Diego, California and now has offices in San Diego, Toronto, Pune, India and Ho Chi Minh City, Vietnam.
- Focuses on small to medium companies.
- Has energy sector experience.

### DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:

- Vulnerability Scanning.
- Log Management.
- Security Assessments.
- SCADA Compliance Solutions.
- Anomaly Detection Tools.
- Application Whitelisting
- Security Awareness Training.
- PCI Solutions.
- KiOSK Protection and Compliance.


[HTTPS://TAGREMSECURITY.COM](https://tagremsecurity.com)

- Endpoint Protection
- Privileged Data Management
- Security Information and Event Management
- Vulnerability Assessments

# Trustwave



 70 W. Madison St., Suite 600, Chicago, IL 60602

 (312) 873-7500

 [infosales@trustwave.com](mailto:infosales@trustwave.com)

## DESCRIPTION OF COMPANY:

Trustwave is an MSSP that specializes in cybercrime, data protection, and managing security risk integrated technologies. Trustwave uses a team of security experts, ethical hackers, and researchers to help businesses manage their information security and compliance programs.

## ADDITIONAL DETAILS:

- Founded in 1995.
- Has more than 1,500 employees.
- Services a range of industries, including small businesses.
- Prior experience includes education sector, payment services, restaurants, healthcare, hotels, and financial services.

- Bring Your Own Device (BYOD) Management
- Endpoint Protection
- Encryption Management
- Security Information and Event Management
- Subscriptions to Threat Information Intelligence Feeds
- Vulnerability Assessments

## DESCRIPTION OF SERVICES/PRODUCTS PROVIDED:


- Trustwave provides endpoint security using the cloud to implement its Trustwave Endpoint Protection Suite (EPS) irrespective of the device used.
- Managed Encryption: integrated full-disk encryption for laptops, encryption for USB drives and other removable media, and encryption for email attachments — all as a managed service.
- Trustwave also provides for managed Intrusion Detection and Prevention Systems.
- Trustwave Vulnerability Management services deliver proactive scanning, testing and remediation of application, database and network vulnerabilities.
- In addition to BYOD management, Trustwave offers managed Two-Factor Authentication for secure logins.
- Trustwave helps meet the compliance requirements by identifying risks and defining corresponding management systems.

[WWW.TRUSTWAVE.COM](http://WWW.TRUSTWAVE.COM)

## Wipro, Ltd



 601 13th Street, 11th Floor South, Washington, DC 20005

 (202) 534-1794

 <http://www.wipro.com/contact>

### DESCRIPTION OF COMPANY:

Wipro, Ltd is a global information technology, consulting and outsourcing company with 170,000+ workforce that serves clients in 175+ cities across 6 continents. Wipro has experience with many industries, including utilities.

### ADDITIONAL DETAILS:

- Founded in 1945.
- Made it onto Forbes' Global 2000.
- 20+ offices throughout the US, with clients such as NV Energy, Michigan State, Xactly, and Medicare Services. Wipro claims to support 50+ utility clients around the world.
- Specific industry capabilities with leading product vendors such as SAP, Oracle, IBM, ABB, and ESRI.

- Endpoint Protection
- Privileged Data Management
- Security Information and Event Management
- Vulnerability Assessments

### DESCRIPTION OF SERVICES/ PRODUCTS PROVIDED:

- Wipro offers the ServiceNXT Managed Security Service.
- Sustained assessment of vulnerabilities: periodic scans on infrastructure/applications, establishing risk-based profile to remediate vulnerabilities, and consultative support during remediation process.
- Managed Authentication Services: infrastructure support, token provisioning, distribution and inventory management, and end user support.
- Compliance based reporting — SOX, PCI DSS, HIPAA, GLBA, FISMA.
- Integrated Alert and Advisory services.
- Early detection and prevention of emerging threats.
- Services delivered using industry standards (ITIL, ISO) and best practice processes.
- Global, 24x7 support available to manage change, incident, performance, and service requests; Security Event Monitoring and Incident Response; Identity and Access Management.

[WWW.WIPRO.COM](http://WWW.WIPRO.COM)