



## ArcSight Protection Suite for NERC CIP Compliance

# Providing Complete Protection for Electric Utilities

### Highlights:

- Demonstrate compliance with NERC CIP audit requirements
- Detect threats against critical cyber assets in real-time
- Ensure the reliability of bulk electric supply and underlying infrastructure

ArcSight offers the most comprehensive, scalable, and cost-effective solution for protection of critical cyber assets and compliance with the NERC CIP 002–009 standards.

### NERC CIP (Critical Infrastructure Protection) 002-009 Standards

The North American Electric Reliability Corporation (NERC) was formed to promote the reliability and adequacy of bulk power transmission in the electric utility systems of North America. With increasing connectivity across utility infrastructure, much of which was deployed before the advent of the Internet, the North American electrical grid is increasingly a target of cyber-crime designed to disrupt critical services including power supply. NERC Critical Infrastructure Protection (CIP) regulations were put into place to ensure the reliability of the power grid and

protect critical electric utility operations and assets. The NERC CIP regulations include eight mandatory reliability standards that require implementing safeguards or controls across critical utility infrastructure and monitoring their effectiveness.

To comply with the NERC CIP standards, companies must both establish and monitor an electronic security perimeter. In order to meet the requirements of this perimeter a host of technologies must be deployed. SIEM and Log Management are needed to meet many of the requirements as depicted in the table below.



NERC CIP Cyber-Security Requirement	Primary Technologies
Log Collection and Analysis	Log Management and SIEM
Access Management	Directories, Authentication, IAM, SIEM
Compliance Reporting	Log Management and SIEM
Intrusion Detection/Prevention	Firewall, IDS/IPS, SIEM
Anti-Malware	Anti-Virus, SIEM
Privileged User Activity Analysis	CMDB, Log Management and SIEM
Incident Reporting and Response	Help Desk, SIEM, Wireless meter mesh networks
Physical Security Controls	Physical Security, SIEM
Network Configuration Control	Network Change and Compliance Management, SIEM
Monitoring	Log Management and SIEM

## ArcSight Protection Suite for NERC CIP Compliance

The ArcSight Protection Suite for NERC CIP Compliance is the market-leading solution for automation of NERC CIP compliance monitoring through collection, storage, reporting, and real-time correlation of events across all utility infrastructure. It provides a central point of analysis for daily business operations by tracking activity on critical cyber assets.

### Benefits:

- Reduce the cost of NERC CIP audits through automation
- Protect operating margins and customer satisfaction by reducing the risk of outages
- Mitigate the risk of non-compliance fines
- Secure sensitive data including customer information, personnel data and network information

- Leverage best practices in monitoring critical infrastructure and reduce the need for internal compliance expertise
- Easily extend your investment to broader use cases and regulatory initiatives

The ArcSight Protection Suite for NERC CIP Compliance is modular and can be deployed collectively or in phases. The core layers of the solution include:

### Event Collection

ArcSight Connectors uniquely enable a minimally intrusive and agent-less approach to log collection across hundreds of commercial products with the ability to easily extend collection to legacy sources. This is particularly valuable in SCADA and / or DCS environments because of the widespread deployment of proprietary applications on aging infrastructure and their associated 24/7 uptime requirements. ArcSight Connectors normalize logs across sources into a common format, which enables simpler and faster analysis. Audit quality controls including secure, reliable transmission and bandwidth metering are also standard capabilities of ArcSight Connectors.

### Log Management

ArcSight Logger is designed to efficiently store and analyze large volumes of enterprise log data. A single appliance

### ArcSight Capabilities by NERC CIP Standard:

<b>CIP-002-1</b>	<b>Critical Cyber Assets</b>	ArcSight tracks and monitors Critical Assets and the Critical Cyber Assets
<b>CIP-003-1</b>	<b>Security Management Controls</b>	ArcSight monitors Security Management Controls required to protect the Critical Cyber Assets
<b>CIP-004-1</b>	<b>Personnel and Training</b>	ArcSight monitors users with access to Critical Cyber Assets
<b>CIP-005-1</b>	<b>Electronic Security Perimeters</b>	ArcSight monitors the logical security perimeter where Critical Cyber Assets reside
<b>CIP-006-1</b>	<b>Physical Security</b>	ArcSight monitors the Physical Security Perimeters within which Critical Cyber Assets reside
<b>CIP-007-1</b>	<b>Systems Security Management</b>	ArcSight monitors controls associated with system test procedures, account and password management, security patch management, system vulnerability, system logging, and configuration changes on Critical Cyber Assets
<b>CIP-008-1</b>	<b>Incident Reporting and Response Planning</b>	ArcSight automates reporting, investigation, and response when incidents relating to Critical Cyber Assets are identified
<b>CIP-009-1</b>	<b>Recovery Plans for Critical Cyber Assets</b>	ArcSight monitors backup and recovery procedures of Critical Cyber Assets

can effectively store up to 35 TB of log information in support of NERC CIP retention requirements. It leverages the common event format of ArcSight Connectors to deliver high-speed forensics search and reporting, as well as alerting via email, SNMP, or a web console. This helps satisfy CIP-007-1 and CIP-008-1 with the benefit of faster response and less time spent in incidents researching alerts.

### Real-time Correlation

ArcSight ESM delivers scalable real-time correlation of logs across all systems, applications, and users for continuous detection of threats to the reliability and security of utility infrastructure. Through a combination of trend analysis, statistical analysis, pattern discovery and other techniques, ESM uniquely delivers an adaptive system that can detect both known and unknown threat vectors. A comprehensive and flexible asset and user model within ArcSight ESM gives it the intelligence to inject factors such as known asset vulnerabilities, criticality, user roles, and user privileges into its correlation logic. ArcSight ESM also uniquely offers multi-tiered tracking and escalation of threats along with inbuilt case management and workflow. Finally, as threats are detected, ESM supports a range of automated or approval-based remediation options.

### User Activity Monitoring

For threat detection, the ability to track activity back to users is critical, but logs often lack user context. Additionally a given user may have numerous identities

across applications and that makes user-based analysis even more challenging. Much of the North American electric grid infrastructure predates the internet era and the underlying infrastructure was built with reliability rather than security in mind. As such, access controls are often lacking and user monitoring becomes even more important. The high levels of remote access by contractors and vendors to support 24/7 operations only compounds this challenge. ArcSight IdentityView is a specialized application that can associate users with network activity through a combination of session awareness and identity correlation. The solution is based on integration with leading identity management systems, which enables ArcSight to synchronize user and role information and leverage that context in its real-time correlation engine.

### Compliance Insight Packages

The ArcSight Compliance Insight Package for NERC enables top down visibility into NERC CIP compliance, continuous protection of critical cyber assets, and automation of NERC CIP audits. The content is derived from widely accepted standards including NIST 800-53 and ISO 27002-2005. This purpose built content package allows utilities to kick start their NERC compliance initiative and also reduces the need for extensive in-house compliance expertise. Large utilities subject to other regulations such as Sarbanes-Oxley, PCI, HIPAA, etc. can add similar focused content packages to the ArcSight platform to streamline cross regulatory compliance efforts.

### About ArcSight:

ArcSight, an HP company, is a leading global provider of cybersecurity and compliance solutions that protect organizations from enterprise threats and risks. Based on the market-leading SIEM offering, the ArcSight Enterprise Threat and Risk Management (ETRM) platform enables businesses and government agencies to proactively safeguard digital assets, comply with corporate and regulatory policy and control the internal and external risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage. For more information, visit [www.arcsight.com](http://www.arcsight.com).



### ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA  
[www.arcsight.com](http://www.arcsight.com) [info@arcsight.com](mailto:info@arcsight.com)

Corporate Headquarters: 1-888-415-ARST  
EMEA Headquarters: +44 (0)844 745 2068  
Asia Pac Headquarters: +65 6248 4795

© 2010 ArcSight, Inc. All rights reserved.  
ArcSight and the ArcSight logo are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners.  
ARST-PB008-041409-02