A comprehensive enterprise security solution for corporate networks and SCADA systems
The Power to

Protect an Industry
Essential protection for the unique needs of electric utilities

As electric power generation and distribution systems are opened up to greater network connectivity and remote control, they become more versatile, more cost-effective—and more vulnerable to attacks on the computers that control them.

Comprehensive information security programs become the critical means by which electric utilities can effectively manage risk. Utilities should therefore examine and execute those programs from both operational and strategic perspectives. In both day-to-day operations and high-threat situations, an effective information security program will support business continuity goals while ensuring that real-time, mission-critical activities remain uninterrupted.

With partial adherence to the new NERC cybersecurity standards required in March 2004—and complete adherence by January 2005—now is the time for electric utilities to examine their approach to managing cyber risks. Utility executives should develop a comprehensive approach to securing critical assets, networks, and information systems while implementing robust defenses against hackers, viruses, and other online threats.

As the world leader in Internet security technology, Symantec offers a broad range of security products and services that create the foundation for Symantec for Electric Power, a comprehensive enterprise security solution designed, assembled, and enhanced to meet the unique needs of electric utilities. Based on proven technologies and practices, Symantec for Electric Power helps power companies ensure business continuity, adhere to industry cybersecurity standards, and avoid the costly disruptions associated with information security breaches.
An industry at the crossroads

Whether you’re planning the modernization of your overall grid architecture, an upgrade to your billing system, or maintenance of your SCADA system, consider the following information security challenges:

- **Increasing—and increasingly disruptive—attacks.** The need for cybersecurity measures such as those mandated by NERC has become dramatically evident in recent years. The Slammer, Blaster, and Welchia worms caused widespread disruptions to enterprise networks. In some cases, electric utilities were directly affected.

- **Increased public scrutiny.** The blackout of August 14, 2003, has prompted increased scrutiny by government agencies and Congress of the modernization of the nation’s electric power systems infrastructure. Also, the new NERC standard requires all electric market and grid participants to report cybersecurity incidents. Such attention to the vulnerabilities of our national power systems is yet another catalyst for more comprehensive and consistent information security procedures and practices.

- **Regulatory complexity.** Electric utilities must already comply with a wide range of regulations—and face the prospect of new FERC-imposed security regulations that are expected as time goes on.

NERC Urgent Action Standard 1200 includes the following components:

- Cyber Security Policy
- Critical Cyber Assets
- Electronic Security Perimeter
- Electronic Access Controls
- Physical Security Perimeter
- Physical Access Controls
- Personnel
- Monitoring Physical Access
- Monitoring Electronic Access
- Information Protection
- Training
- Systems Management
- Test Procedures
- Electronic Incident Response Actions
- Physical Incident Response Actions
- Recovery Plans


www.nerc.com
Increased Internet access. Regulations now demand that utilities be connected to the Internet, thus providing access points for hackers to penetrate. In addition, utilities are migrating to open standards within SCADA networks, opening corporate networks to facilitate remote access, and implementing more efficient methods of managing energy resources. While such changes offer many benefits, they also increase the danger of unauthorized access to both the SCADA and business networks.

Cost effectiveness. For privately held electric utilities, all of the above goals must be accomplished in a competitive environment characterized by tight budgets and ever increasing public pressure to keep rates low. But outages cost even more—in lost revenues, diminished stock prices, angry customers, and lengthy investigations. Uptime is a power company’s greatest ongoing concern, so it must be preserved as aggressively as possible.

NERC recommendations for SCADA security

- Deploy firewalls to protect SCADA system networks from the Internet and other company networks.
- Implement firewall rules that deny all network traffic that isn’t specifically required for the operation of the critical system and supported operations.
- Restrict traffic on open ports to those addresses from which such traffic is expected.
- Do not permit VPN tunneling through the SCADA network security perimeter.
- Restrict remote access to SCADA networks.

Source: NERC, 2003
Symantec™ for Electric Power

As electric utilities bring more and more operational components online, it’s crucial to develop and deploy a comprehensive, enterprise-wide security system. Symantec for Electric Power combines Symantec’s industry-leading security products and services with specific expertise gained from years of working with dozens of electric utilities to secure both corporate IT networks and SCADA infrastructures.

In implementing Symantec for Electric Power for your company, we will work with you to:

- Examine and improve your adherence to industry cybersecurity standards.
- Understand your risks and secure key assets.
- Provide early warning on threats while proactively preparing for, detecting, and responding to security incidents.
- Effectively protect both your security perimeter and your internal networks.

Symantec offers a wide range of solutions for enterprise security. The following products and services are the ones most commonly used when developing a customized security solution for electric utilities. Our Assessment Services, Managed Security Services, protection technologies, and early warning services are designed to work together to strengthen your infrastructure against outages induced by cyberattacks. Symantec products are based on the Symantec™ Enterprise Security Architecture, allowing for simplified integration with other popular third-party security technologies in your existing IT security infrastructure.

**SCADA and information systems assessments**

Symantec’s Security Services experts have unparalleled knowledge of the security challenges with SCADA systems, as well as access to templates developed by Symantec expressly for assessing the security of SCADA networks. These experts will evaluate the security of your SCADA network safely, making sure to avoid disruption to system operations.

If you choose, the assessment can go beyond SCADA to provide a comprehensive evaluation of the network at large. Such an assessment encompasses network discovery, vulnerability detection, system penetration, and applications testing. Symantec can also perform technical control reviews. At the end of the assessment, Symantec provides system-level recommendations for network design and operational procedures.
Symantec DeepSight™

Early warning is key to maintaining business continuity. Receiving early, detailed alerts of potential attacks allows your company to efficiently prioritize tasks and deploy internal resources to keep the power flowing.

The Symantec DeepSight Threat Management System tracks security on a global basis, providing early warning of active attacks. With personalized notification triggers, expert analyses, and industry-specific reporting capabilities, it enables enterprises to prioritize IT resources in order to better protect critical information assets against a potential attack.

The DeepSight system continuously correlates intrusion detection system and firewall attack data from more than 20,000 sensors in over 180 countries—plus other human intelligence resources—to keep track of the latest attack techniques. The experts at Symantec analyze the information to identify active attacks and deliver advanced warning based on your specific network configuration. Patches, countermeasures, workarounds, and additional references are also provided, reducing the time spent searching through Web sites and emails.

Symantec DeepSight Alert Services provide personalized alerts about vulnerabilities and malicious code to bridge the gap between awareness and action. Symantec analysts monitor potential threats across more than 14,000 distinct product versions and information from more than 140 different sources. A detailed analysis of each threat is provided, describing its severity and potential impact, its technical makeup, the systems that might be affected, available patches or workarounds, and comprehensive mitigation strategies. Alerts are directed to the specific personnel responsible for addressing and remediating the problem.

Symantec Enterprise Security Manager™

Symantec Enterprise Security Manager provides comprehensive, policy-based security assessment and management. Using a template based on the NERC cybersecurity standard, it provides a solid foundation for electric utilities to begin implementing the NERC standard and measuring their ability to adhere to it.

“In a recent, nationally televised Public Broadcasting Service (PBS) Frontline special, entitled ‘Hackers,’ one interviewee claimed that the power grid ‘could be brought down in the click of a button.’ Whether this is true or not is less important than the fact that hackers, saboteurs and terrorists may believe it to be true. This could cause them to turn their attention to attacks on the grid.”

Gartner, Inc., Prepare for Cyberattacks on the Power Grid, October 2002
From a single location, Symantec Enterprise Security Manager controls the enterprise-wide discovery of policy deviations and vulnerabilities in services that hold mission-critical applications and data. Using its intelligent tools, your administrators can quickly and cost-effectively create baselines, measure performance against those baselines to identify systems that are not in compliance, and then correct faulty settings to bring systems back into compliance.

Symantec Enterprise Security Manager provides management reports detailing policy compliance and security vulnerabilities both inside the enterprise and from the Internet. This detailed reporting gives administrators a comprehensive view of their policy management status and the ability to drill down to analyze specific compliance issues.

Symantec™ Managed Security Services

Symantec Managed Security Services offer a cost-effective way to optimize security resources. Symantec currently manages the security infrastructures of several leading electric utilities in the United States. By outsourcing some or all of your IT security, your company will enjoy the benefits of centralized management and monitoring of protection technologies along with early warnings, incident response, and decision support.

Symantec Managed Security Services deliver industry-leading security monitoring, management, and response. These 24x7 services are delivered through a unique combination of skilled personnel, best-practices processes, and state-of-the-art technologies. They are designed to enhance your organization’s information security posture through continuous monitoring and management of security devices, expert analysis of log data, and immediate response to potential security threats as they are detected. The flexible, vendor-neutral offerings are designed to meet a variety of business needs.

“Power companies depend on SCADA to control their operations and should, therefore, provide security in proportion to the threat. Security measures for SCADA systems should include intrusion detection and strong authentication measures, as well as recovery plans for the operation centers and SCADA systems.”

Symantec ManHunt™

An intrusion detection system (IDS) is a vital element of modern network security, and has therefore been recommended by the President’s Critical Infrastructure Protection Board as a component of electric utilities’ overall security strategies.

Symantec ManHunt provides high-speed network intrusion detection, real-time analysis and correlation, and proactive prevention and response to defend against internal and external intrusions and denial-of-service attacks. Because ManHunt can also collect events from other vendors’ IDS products, it provides a single, integrated view of intrusions across your entire network.

Specific benefits of Symantec ManHunt for electric utilities include:

• Zero-day attack prevention leads to stronger protection against attack-induced outages.
• Event correlation and response leads to faster response times, which can prevent or minimize outages.
• Reduced false positives result in better accuracy and fewer distractions for your IT staff.

Symantec™ Gateway Security

Defining and protecting the security perimeter is one of the most important initial steps in the execution of a fully functional operational security program. Effective perimeter defense must include implementing comprehensive security to establish “zones of trust” within the network.

Symantec Gateway Security is a full-inspection firewall appliance that integrates seven different security technologies for maximum effectiveness. The appliance provides strong security at the gateway between the Internet and your corporate network or between network segments.

As the industry’s most comprehensive firewall appliance, Symantec Gateway Security offers full-inspection firewall technology, protocol anomaly–based intrusion prevention and intrusion detection engines, award-winning virus protection, URL-based content filtering, anti-spam technology, and IPSec-compliant virtual private networking technology with hardware-assisted high-speed encryption.

recommendations

Symantec recommendations for protecting enterprise information assets

• Turn off and remove unneeded services.
• Keep patch levels up to date, especially on computers that host public services (such as HTTP, FTP, mail, and DNS) and are accessible through the firewall.
• Enforce a password policy.
• Configure email servers to block or remove email that contains file attachments (such as .vbs, .bat, .exe, .pif and .scr files) that are commonly used to spread viruses.
• Isolate infected computers quickly to prevent further compromising your organization. Then perform a forensic analysis and restore the computers using trusted media.
• Train employees not to open attachments unless they are expecting them. Also, instruct them not to execute software that is downloaded from the Internet unless it has been scanned for viruses.
• Ensure that emergency response procedures are in place.

Source: Symantec Internet Threat Report, October 2003
The time to act is now

NERC, the federal government, shareholders of publicly owned electric utilities, and the general public have made their position clear: Electric utility companies must take steps quickly to protect electric generation and delivery systems—and their associated business networks—against viruses, hackers, and other online threats.

As the world leader in Internet security, Symantec has the products and services your company needs for robust cyberprotection—including ones that have been tailored especially for the electric power industry. We can design a customized solution of products and services that will work together to provide comprehensive IT security and complement your existing investment in security protection technologies.

Contact your Symantec representative or visit http://ses.symantec.com/power for further information on how Symantec products and services can help your organization plan and implement an effective cybersecurity system.
Symantec, the world leader in Internet security technology.
ABOUT SYMANTEC

Syman
tec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to enterprises, individuals, and service providers. The company is a leading provider of client, gateway, and server security solutions for virus protection, firewall and virtual private network, vulnerability management, intrusion protection, Internet content and email filtering, remote management technologies, and security services to enterprises and service providers around the world. Symantec’s Norton brand of consumer security products is a leader in worldwide retail sales and industry awards.