



Today's sophisticated networks in the energy sector are a combination of traditional information technology (IT) systems and industrial control systems (ICS) such as supervisory control and data acquisition (SCADA) systems. These organizations have historically depended on the physical isolation of ICS to provide security for their systems running proprietary control protocols, and using specialized hardware and software. These networks had little resemblance to traditional IT installations. "Now, widely available, low-cost Internet protocol (IP) devices are replacing many proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents."¹

"We wanted a complete upgrade to increase overall bandwidth and security while continuing to ensure network uptime between 99.8 and 99.9 percent for our trading and 24/7 power management operations."

"The ability to insert TippingPoint IPS devices seamlessly into the network core is a major advantage."

"The TippingPoint IPS is simple to deploy, extraordinarily powerful and so effective, Vattenfall now has a policy to use it throughout our enterprise."

Kaj Lindqvist

Nordic-Area Network Manager
Vattenfall

What Security Challenges Do Energy Organizations Face Today?

Increasingly Open and Interconnected IT and ICS Networks

The supply chain structure in energy industries is increasingly open, creating complex business and IT ecosystems. Some organizations have dedicated security personnel and best practices in place to manage these partner and remote access ecosystems, but many do not, exposing them to a variety of threats.

Energy organizations, including electricity generation, transmission, and distribution; natural gas production and distribution; petroleum products refining; transportation systems monitoring and control; water supply; wastewater treatment; and chemical processing companies are also connecting the corporate network to process automation control systems in order to enable: data collection from anywhere in the network, Web-based applications to view data more easily, remote monitoring, and ERP planning

systems to monitor process operations (and obtain information in real-time). ICS teams are adopting IT solutions to promote improved corporate connectivity and remote access capabilities. They are designed and implemented using industry standard computers, operating systems and network protocols, and are beginning to resemble IT networks. This integration supports new IT capabilities, but also significantly reduces isolation for ICS from the outside world, creating a greater need to secure these systems.

Exposure to Targeted Attacks

According to the 2007 Computer Security Institute (CSI) Annual Computer Crime and Security Survey, "Almost one-fifth (18 percent) of respondents said they'd suffered a "targeted attack,"...aimed exclusively at their organization...or a small subset of organizations."² For energy companies understanding these targeted attack vectors is essential to building effective security strategies for both IT and ICS networks.

Inadequate Traditional Protection

Traditional IT network security tools (Firewalls, Intrusion Detection Systems (IDS), Anti-Virus, etc.) do not provide adequate security in the face of new targeted threats and more sophisticated versions of old threats (worms, viruses, etc.). Technologies such as IDS, which rely on reactive, high-touch models, lack the automated enforcement required to adequately protect today's networks. Many customers realize the need for in-line enforcement, but are afraid of the impact it might have on the performance of IT and ICS systems.

In addition, ICS systems have historically been susceptible to only local threats because their components were in physically secured areas and

TipingPoint_Energy_Solution_Brief

IPS-Secured_Networks

completely separated from other networks. But now, interconnectivity with IT systems is exposing these systems to targeted attacks, and these control systems usually have little to no security capabilities designed into their components, nor do they have the capacity to add such security controls.

TipingPoint Customer Base

- 4,000+ worldwide customers
- 15,000+ in-line IPS deployments
- 300+ Fortune 1000 customers

Production_Interruption_and_Human/Environmental_Safety_Concerns

Attacks on energy IT and ICS networks can have a huge impact inside and outside the organization, especially as compared to other types of industries. Successful attacks on general IT systems can mean the loss of confidential data and loss of worker productivity, but successful attacks on ICS networks can cause significant production interruptions, loss of in process materials, physical harm to humans inside and outside the facility, harm to the environment, and even harm to the local economy.

Regulatory_Requirements_and_Internal_Security_Mandates

Due to the significant potential losses from successful IT and ICS attacks, Internal Security Policies have become more stringent along with audit compliance requirements – driven by security, privacy, regulatory and legal concerns (including ISO/IEC 27001 and 27002; AS7799; ISA-SP99; NIST SP 800-12, 14, 26; API 1164; API RP 70; AGA 12; NERC Cyber Security Standards; etc.)

Availability_and_Performance_Sensitivities

Outages are simply not tolerated on energy IT and ICS systems because of the huge costs associated with loss of production. In fact, maintenance outages typically are planned weeks, if not months in advance, meaning security solutions have to work without downtime and/or regular maintenance. In addition, many energy ICS systems are extremely sensitive to traffic delay and jitter so security solutions on the ICS network can't impact these performance characteristics of the network.

Patching_ICS_Networks_and_Devices

Change management or applying security patches to operating systems and applications in a control systems environment is non-trivial. Updates require rigorous testing by both the vendor and end user meaning implementation can take weeks or

months to accomplish, and in other cases the ICS may utilize older versions of operating systems that are no longer supported by the vendor, resulting in patches not being available at all.

ICS_Device_Resource_Constraints_Limit_Security_Upgrade_Options

“ICS and their real time operating systems are often dedicated, resource constrained systems that do not include typical IT security capabilities. In fact, there may not be computing resources available to retrofit these devices with current security capabilities and in some instances, third party security solutions are not allowed to be added to devices due to ICS vendor license and service agreements.”³

How_TipingPoint_Protects_Energy_IT_and_ICS_Networks

Improve_Network_Reliability_and_Security

In the face of more targeted attacks, more sophisticated traditional attacks, and the inability of traditional solutions to meet security and performance requirements for IT and ICS networks, the TipingPoint IPS provides network reliability and security with:

1. Automated protection for Web servers and applications;
2. In-line security for sensitive corporate data, and intellectual property;
3. Protection against the latest blended threats with thorough and timely network security filters; and
4. SCADA protection for integrated / interconnected IT and ICS networks

In addition, the TipingPoint Network Access Control solution reduces network vulnerabilities by ensuring only authorized users and devices that meet internal security policies have access to the network.

Minimize_IT_Staffing_Demands

Customers minimize staffing demands with automated in-line protection – eliminating time consuming event follow-up and manual remediation associated with IDS-based solutions.

TippingPoint_Energy_Solution_Brief

IPS-Secured_Networks

Improve_Efficiency_of_Patching_Programs

The TippingPoint IPS solution allows customers to reduce cost and complexity by eliminating emergency patches for IT and ICS applications, operating systems and network devices with IPS filters that provide a virtual patch from zero-day events.

- > Virtual Patching – covers software vulnerabilities and zero-day threats allowing you to protect assets before patches are deployed

Maintain_or_Improve_Network_Performance

Customers can maintain or even improve network performance with line-rate speeds and rate limiting capabilities built into the TippingPoint IPS.

Improve_Security_Compliance

In the face of more stringent security policies and regulatory demands, the TippingPoint IPS provides automated enforcement of network security policies and reporting to show internal and external auditors how the network is protected from the latest threats. In addition to meeting compliance requirements, TippingPoint provides the best security enforcement available for IT and even ICS networks.

- > Meet internal mandates and regulatory requirements with an easy to use central management system
 - Generate reports for internal requirements and audits

What_is_the_TippingPoint_Solution?

The TippingPoint Intrusion Prevention System is purpose-built for in-line network protection and is specifically designed to deliver network security enforcement with:

- > High availability
- > Multi-gigabit throughput including 10Gbps solutions with the TippingPoint Core Controller
- > Switch-like latency and support for millions of sessions
- > Filter accuracy (no false positives)

- > Broad filter coverage
 - Vulnerability, exploit and anomaly-based filters
 - SCADA filters
- > Timeliness of filter coverage
- > Low-touch central management system (manage with current staff)

Filter accuracy, coverage, and timeliness are made possible by the world-renowned DV Labs security research team.

The TippingPoint IPS also provides multiple enforcement functions:

- > Blocks malicious traffic flows
- > Quarantines non-compliant hosts
- > Rate limits non-critical traffic
- > Alerts staff of key events
- > Redirects designated traffic
- > Allows clean traffic to pass unimpeded

The function of the product is based on a simple concept: bad traffic goes in; only good traffic comes out. This provides real-time automatic protection for applications, operating systems, clients, servers, VoIP infrastructure, routers, switches, SCADA protocols and other assets.

The TippingPoint solution protects networks at the WAN perimeter and inside the network; providing protection of critical Web infrastructure in the DMZ and key assets in the data center. TippingPoint provides security isolation in the core, for key network zones at the aggregation and access layers, and between IT and ICS zones. By enabling strong protection between network zones, organizations can mitigate the propagation of threats within the network.

The TippingPoint Network Access Control (NAC) solution helps organizations manage user access and endpoint security which is a critical component to ensuring the overall security and availability of its IT infrastructure. TippingPoint provides an easy to

TippingPoint_Energy_Solution_Brief

IPS-Secured_Networks

manage, comprehensive NAC solution that provides a means to confirm user and endpoint identity and verify device health prior to granting access to the network and its resources. TippingPoint NAC provides multiple methods of enforcement including 802.1X, DHCP and in-line blocking, allowing customers to centrally manage a combination of the appropriate enforcement types given their network topology and access control priorities.

How_TippingPoint_Can_Help

Over 4,000 TippingPoint customers are already securing their networks with TippingPoint and passing security audits with flying colors. Learn how our energy customers are protecting their IT and ICS networks with TippingPoint by visiting www.tippingpoint.com, or call TippingPoint directly to speak to a representative about our IPS evaluation program at +1 888 878-3477.

1. Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology (NIST) Special Publication 800-82 Second Public Draft, U.S. Department of Commerce
2. Richardson, Robert. "2007 CSI Computer Crime and Security Survey." October 2007 Computer Security Institute. http://www.gocsi.com/forms/csi_survey.jhtml
3. Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology (NIST) Special Publication 800-82 Second Public Draft, U.S. Department of Commerce

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS

European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450

Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999