Security for the

Energy Industry

CONTROL OPERATIONS AND ACCESS WHILE SECURING ESSENTIAL DATA

Energy companies may be the biggest target for cyber criminals because they are perceived to be highly vulnerable and have the financial wealth to fill attackers' pockets. With multiple parties in the supply chain – some moving from one remote location to another – securely accessing data from anywhere in the world creates ongoing challenges for the dedicated and outsourced IT staff.

"Oil giant Chevron fends off as many as 500 hack attacks a week" - InfoSecurity, May/June 2009 edition

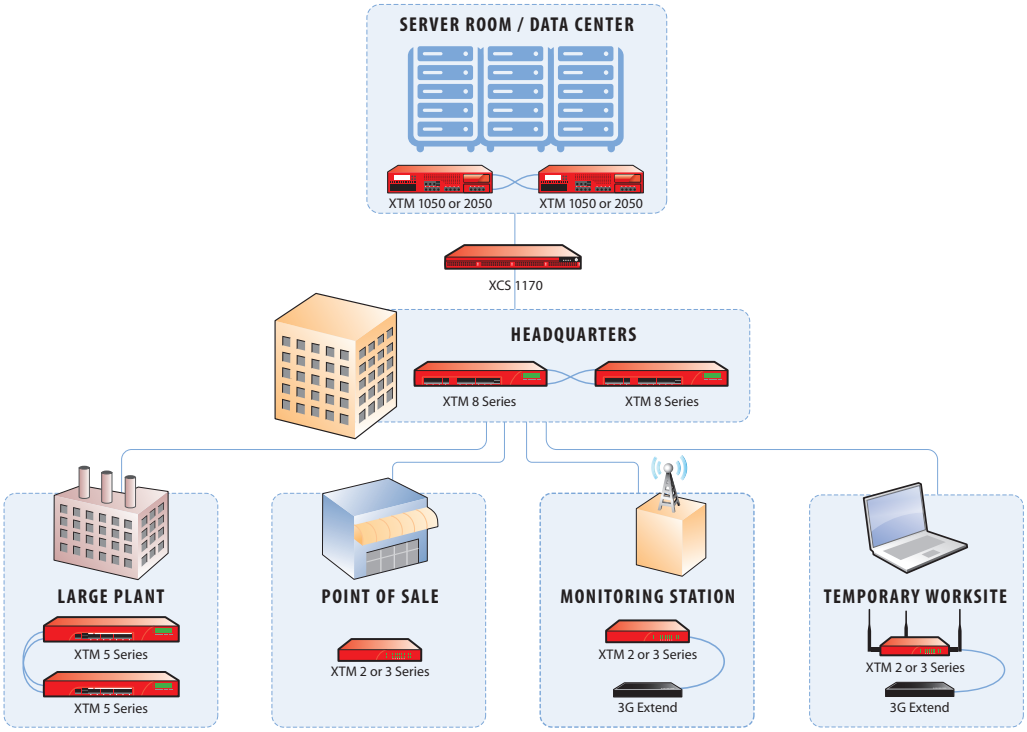
Threats can come from within, too. The cost of a disgruntled employee hacking into your network to gain employee data, copy customer account information, or disable physical systems can be catastrophic for a company and its customers, partners, contractors, and suppliers.

CHALLENGES ENERGY COMPANIES FACE INCLUDE:

- **Operational complexity** – Protecting SCADA (Supervisory Control and Data Acquisition) infrastructure, managing remote and transient workers, and ensuring WLAN security while carefully monitoring the full supply chain.
- **Lack of real-time monitoring and reporting** – Accessing real-time information about possible network vulnerabilities to make intelligent operational decisions.
- **Protecting the infrastructure from threats within and outside the system** – Ensuring users are protected from network threats such as viruses, and that critical systems are protected from both users and outside attacks.
- **Employee, contractor, partner, and supplier productivity** – Eliminating the majority of spam and spim, blocking dangerous and inappropriate web surfing, and protecting against blended threats to reduce downtime and financial loss.

INDUSTRY CHECKLIST

- **DEPLOY LAYERED SECURITY** for the broadest threat coverage
- **SCAN NETWORK TRAFFIC** for threats and malware targeting SCADA infrastructure
- **SECURE CONNECTIVITY** between headquarters, field sites, and other network end points
- **INCREASE PRODUCTIVITY** by eliminating spam and controlling web surfing
- **USE REAL-TIME VIEWS OF SECURITY ACTIVITY** to stay on top of what's happening in your network at all times
- **MEET COMPLIANCE STANDARDS** by implementing a solution that is robust, secure, and flexible



WatchGuard offers a family of interoperable, centrally managed devices that easily integrate into a multitude of networks sharing data.

WHY ENERGY COMPANIES CHOOSE WATCHGUARD

"I looked at Fortinet, Juniper, and SonicWall's current offerings. I looked at cost and ease of the interface. I looked at performance, not only for raw throughput but also for VPN performance. I looked at the available options for antivirus, and intrusion prevention and detection – I wanted a firewall that would respond to outside threats and begin blocking automatically on its own... I looked at all those things, and the WatchGuard devices came out on top time and again. It really became a no-brainer." – SCADA Analyst/Security Administrator

EXTENSIBLE THREAT MANAGEMENT FOR ENERGY

Extensible threat management (XTM) security solutions from WatchGuard aggregate multiple security measures into a single, easily configurable solution. Powerful firewall/VPN technology combines with application control, virus blocking, spam blocking, spyware protection, and URL filtering to stop threats. WatchGuard XTM's Intrusion Prevention Service (IPS) includes specific protections for SCADA systems as well as broad-based intrusion prevention for a multitude of different attack and vulnerability types. WatchGuard XTM solutions also include enhanced support for business technologies such as Voice over IP (VoIP), and are the only XTM products on the market that offer inbound and outbound HTTPS inspection to increase web security coverage.

MOVING DATA SECURITY

In the Energy industry, there is constant transfer of data from external facilities to main offices and data centers where historic data exists. Data is further processed and analyzed for making critical decisions and optimizing operations. Role based access control (RBAC) ensures higher security by allowing users to obtain only the information they are assigned at the time. Faster decision-making with accurate information results in improved operations.

MEETING COMPLIANCE REQUIREMENTS

In addition to the challenge of protecting SCADA infrastructure, regulatory challenges abound. Many energy companies face compliance requirements including PCI DSS (Payment Card Industry Data Security Standard) if they are accepting credit or debit cards in exchange for goods or services with vendors and/or customers, and HIPAA (Health Insurance Portability and Accountability Act) if they provide benefits to customers who are disabled. To meet compliance standards, it is important to design a network with appropriate physical and logical boundaries to segregate the compliant operating environment.

WatchGuard uses a zoned network architecture to segregate protected information so that it cannot be accessed directly via the Internet. Network zones can be configured to create a DMZ for all public-facing servers and a Trusted zone where the protected information resides. In addition, all firewall management communications are done via a secure encryption-based protocol.

INTUITIVE TOOLS, REAL-TIME MONITORING, RICH REPORTING

Network administrators have granular control, using an intuitive management console to centrally manage all security capabilities. Scriptable CLI supports interoperability in large networks and allows easy integration into existing infrastructure for direct, quick connections. Interactive real-time monitoring and reporting give an unprecedented view into security activity, so administrators can take immediate preventive or corrective action.

INTEGRATE SECURITY ALL DOWN THE LINE

Keep numerous offices and sites across multiple continents communicating with secure VPN connections. Employees, contractors, partners, and suppliers can safely work from anywhere, anytime using SSL VPNs, Mobile User VPNs or Branch Office VPNs. Remotely monitor sites and safely transmit video streams over a 3G cellular connection, through a VPN tunnel if you so choose. VPNs can be connected from most major platforms, including popular smartphones and tablets such as Apple's iOS products.

There are a number of different data sources that may be active at any given time of day from remote facilities to tank farms, POS systems, and support centers. Highly reputable, affordable, easily upgradable and extensible WatchGuard network security solutions fit your environment and protect your network from headquarters to the remote edges.

FIND OUT MORE

CASE STUDIES

- End-to-End Security for Energy Giant
- Oil and Gas Business Solutions Company Has a Direct Pipeline to Their Customers
- Intuitive Tools Allow Energy Company to Easily Manage Network Security In-House
- More case studies are available at www.watchguard.com/casestudies

WHITE PAPERS

- Practical Advantages of Fireware® XTM for Hands-On IT Administrators
- Finding Value in a Turbulent Economy with PCI DSS
- More network security white papers are available at www.watchguard.com/whitepapers

PRODUCT COMPARISONS

- www.watchguard.com/compare

To learn more about WatchGuard Network Security Solutions for the Energy Industry, contact your reseller, visit www.watchguard.com, or call +1.206.613.0895.

For more information about WatchGuard Retail Security Solutions, contact your reseller, visit www.watchguard.com, or call the number below.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com