CYBER SECURITY SOLUTIONS FOR CRITICAL INFRASTRUCTURE AND INDUSTRIAL CONTROL SYSTEMS

NON-INVASIVE PROTECTION ACROSS OPERATIONAL AND INFORMATION TECHNOLOGY ASSETS

OVERVIEW

The growing threat of advanced cyber attacks on critical infrastructure and industrial control systems presents a unique challenge for organizations. State based agents, terrorists and organized crime increasingly target industrial systems, resulting in physical disruption to business operations and intellectual property theft. Companies of all sizes — from small power generation plants to global pharmaceutical manufacturers — must balance budget constraints with the need to secure their industrial network environments.

A customized blend of technology, intelligence and expert consulting services can enable industrial and manufacturing organizations to identify risks and proactively mitigate threats. FireEye® and its partners provide a non-invasive, holistic security solution for your entire information technology (IT) and operational technology (OT) enterprise.

Systemic challenges

Industrial control systems include technologies such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) at the core of day to day operations in manufacturing, chemical processing, oil and gas production and other industries. Applications include railroad switches, SCADA monitors and programmable logic controllers (PLCs). Infrastructure organizations critical to national economy and security, from banking data centers to electrical power grids and railway transportation, use many similar technologies. Many of these systems, once segregated or "air gapped," are now becoming increasingly connected to IT networks, leaving them more vulnerable to cyber attack.

IT network security is focused on three priorities: ensuring that data is confidential, assuring its integrity and maintaining its availability for the user. In contrast, OT networks have historically prioritized system availability over security; they often operate with brittle legacy systems that are misconfigured or outdated or cannot be secured through patches or by accepting agents. Organizations need partners that can help them manage these challenges across their network.

FireEye®

Cyber threats

Cyber attacks against critical infrastructure and industrial systems have risen rapidly since 2010. In 2015 the Department of Homeland Security Industrial Control Systems — Computer Emergency Response Team (ICS-CERT) reported a 20 percent increase in cyber attacks against industries managing critical infrastructure and ICS over the past year, with the most targeted areas including manufacturing, energy, water and transportation.[1] Outdated networking technologies leave such organizations open to traditional threats like commodity spam and malware.

Recent high-profile attacks indicate that threat actors are using more sophisticated techniques, such as multi-flow, multi-vector attacks that exploit vulnerabilities in IT networks to move into OT systems. The 2010 attack on Iranian centrifuges that relied on complex malware known as Stuxnet and physically destroyed PLCs was introduced through a USB stick drive. Malware introduced via spear phishing and social engineering was used to cause severe physical damage to a German steel mill in 2014. Once inside, the attacker used captured credentials and IT connectivity to the plant's OT network to deregulate critical systems and cause physical damage.[2] In the recent Black Energy attack on a Ukrainian power grid, increasingly networked OT environments opened the door for commodity malware to become a major threat.

Organizations that suffer ICS attacks face a host of potential business impacts including data corruption, equipment damage, regulatory fines and business disruption.[3] Theft of intellectual property, corporate strategy and R&D information is a serious problem for victim organizations, particularly those with global operations. At the same time, senior level management often overlooks cyber risk in corporate planning.

Firewalls, whitelisting and network segmentation can help organizations reduce risk, but they are not sufficient. Attackers will exploit security gaps in IT networks and move laterally into OT systems to pilfer data or sabotage critical systems.

Personnel challenges

Cloud-based business models and a changing regulatory environment have expanded the risk profile of many organizations. This is particularly salient for managers of OT, IT or IoT in organizations with developing security programs that struggle to match business requirements with an evolving threat landscape. A 2015 Tripwire survey of 400 executives and IT professionals across the oil, gas, utility and energy sectors found that fewer than half believed their organization could immediately detect a cyber attack, although 94 percent believed they were a target. Furthermore, 83 percent believed that such attacks could do "serious physical damage".[4]

Although there has been an increased focus on cyber security in recent years, advanced persistent threats against critical infrastructure such as the energy sector continue to go undetected for an average of six months.[5]

Part of the reason for this is alert overload. Standard cyber security deployments generate hundreds of thousands of alerts per week, but most organizations only have the resources to investigate about six percent.[6, 7] With only 19 percent reliability, organizations waste millions of dollars a year chasing false positives or performing investigations with inadequate intelligence and insufficient expertise.[8] As attacks against critical infrastructure occur through multiple stage and different vectors, organizations need higher fidelity and context from their security solution.

Common sense first steps

The NIST Framework for Improving Critical Infrastructure Cyber Security provides guidance to help you reduce your risk profile. These include the identification of your most important systems and assets and the implementation of mitigating controls to protect them, such as continuously monitoring network traffic across OT and IT environments to detect anomalous activity, developing plans to respond quickly to these events and developing a post-breach recovery plan.[9] In addition to this guidance, FireEye recommends segmenting networks, regularly patching servers and computer systems, installing firewalls and advanced threat detection and implementing application whitelisting. But this is just a starting point.

---

1 Jim Finkle (January 20, 2016). U.S. Sees 20% Jump in Cyberattacks on Critical Manufacturers.
2 Robert M. Lee, Michael J. Assante and Tim Conway (December 30, 2014). German Steel Mill Cyber Attack.
3 Paul A. Ferillo, Randi Singer and Dan Scali (March 28, 2016). Stay Out of the Dark!—Dealing With and Responding to Cyberattacks on Critical Infrastructure.
4 Tripwire (June 25, 2015). Survey: 86 Percent of Energy Security Professionals Believe They Can Detect a Breach on Critical Systems in Less Than One Week.
5 FireEye (February 2015). M-Trends 2015: A View from the Front Lines.
6 FireEye (July 2014). The SIEM Who Cried Wolf: Focusing Your Cybersecurity Efforts on the Alerts that Matter.
7 Ponemon Institute (January 2015). The Cost of Malware Containment.
8 Ibid.
9 National Institute of Standards and Technology (February 12, 2014). Framework for Improving Critical Infrastructure Security.

Integrated FireEye solution

The FireEye solution for critical infrastructure and industrial control systems is non-invasive, conforms to industry standards and federal regulations and protects your entire network environment. There are many moving parts in a comprehensive FireEye solution. However, every component can be individually installed to work smoothly within your existing security environment.

The FireEye solution generally begins with the Mandiant® ICS HealthCheck, which consists of interviews with staff, reviews of your architectural diagrams, contextual assessment of known threats and the creation of a custom risk rating for your organization. Next, experts conduct a complete manual check of your system configurations and thoroughly analyze your network traffic with proprietary, industry-leading packet capture technology.

FireEye technology with Belden integrations detects and prevents lateral movement of advanced attacks from IT systems into OT systems using signature-less, virtual machine based behavioral analysis. The cloud-based FireEye Threat Analytics Platform (TAP) leverages intelligence on adversaries and victims and from millions of sensors across the globe and applies it to logs and events from both your IT and OT environments to detect, respond and hunt for hidden threats. Integration between TAP and the Belden portfolio of products, including the Tofino Xenon Industrial Security Appliance, brings the advanced threat analytics capability of TAP to OT network traffic. Using Tofino firewall logs, TAP can identify potential threats based on ICS protocol anomalies as well as behavioral patterns that may indicate malicious activity. On the IT side, Tripwire Enterprise extends the visibility of FireEye network security products by monitoring IT system and file change data, correlating data with FireEye iSIGHT Critical Infrastructure (FireEye iSIGHT Intelligence for ICS and critical infrastructure) and sending anomalous traffic to TAP and the broader FireEye network security platform.

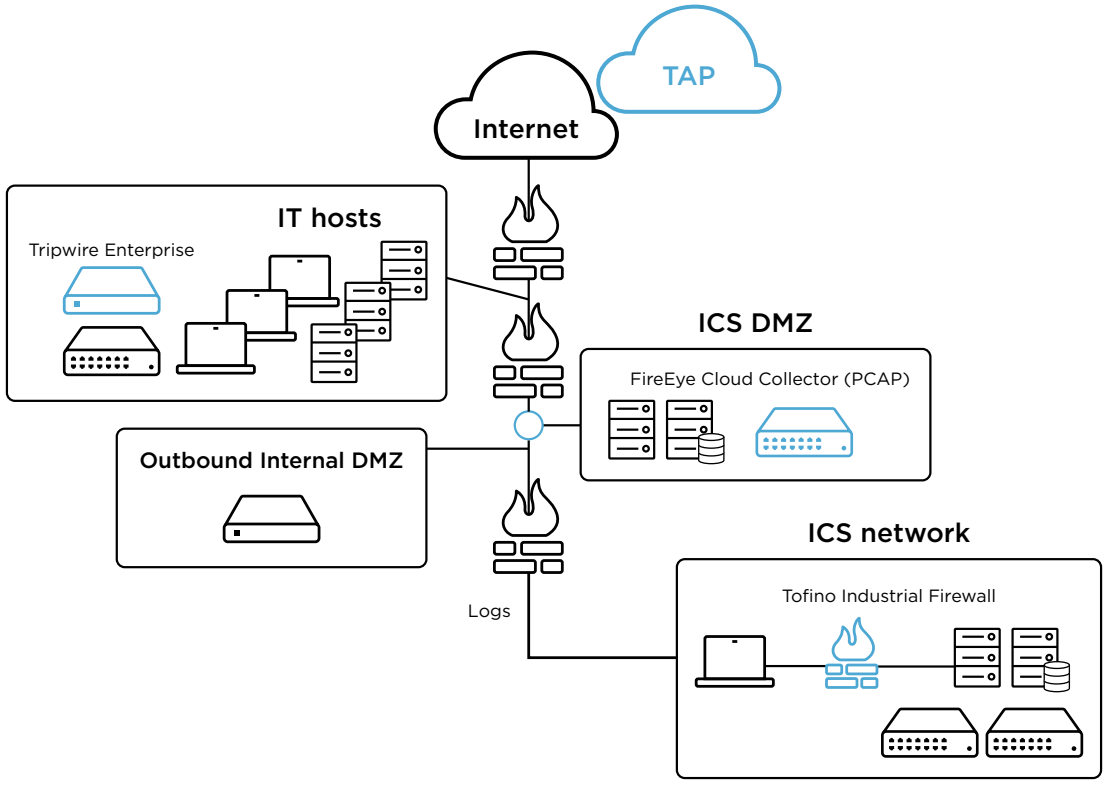

FIGURE 1. FIREEYE SOLUTION WITH BELDEN INTEGRATIONS FOR SECURING ICS AND CRITICAL INFRASTRUCTURE.

FireEye iSIGHT intelligence provides your organization with intelligence on ICS threats, including cyber physical systems, IoT and automation, giving your team insight into the intent and capabilities of threat actors targeting your organization. This subscription service tells you exactly who they are, what they're after and why, so you can make informed business decisions and better manage risk.

To help your organization comprehensively assess its security posture, Mandiant Red Team Operations uses realistic attack scenarios and methodologies to carry out a simulated intrusion on your network. Mandiant Penetration Testing services offer a customizable assessment of security controls for your critical systems and applications.

TABLE 1. HOW TO CHOOSE A STARTING POINT WITH FIREEYE.

YOUR CURRENT RISK	YOUR IMMEDIATE NEED	YOUR FIRST STEP
Unpatched OT systems, poorly configured firewalls and internet connected networks	Identify vulnerabilities in your entire network and conduct a full packet capture analysis of data across your IT and ICS network without deploying agents in your OT environment.	Mandiant ICS Health Check
Incident response delays due to paperwork and resource management and allocation	Retain a dedicated team of experts at no cost that can start working immediately when you suspect or uncover a attack.	Mandiant Incident Response Retainer
Lack of evidence on the efficacy of your security program and directions for meaningful improvement	Provide real world attack scenarios or specifically tailored testing to assess the strength of your security	Mandiant Red Team and Penetration Testing
Inadequate intelligence prevents firms inhibits you from implementing strong defenses	Gather real-world intelligence on the tactics, techniques, procedures and motivations of attackers likely to target your organization.	FireEye Intelligence Center and iSIGHT Threatscape
Inability to detect signs of advanced attack without interrupting critical control processes	Deploy a single cloud application that uses high fidelity signature-less detection technology to alert you to anomalous behavior across your IT network and enable your team to actively hunt for threats in your networks.	FireEye Threat Analytics Platform (TAP) with Belden integrations (Tofino and Tripwire) for IT and OT coverage

Security results for industry and infrastructure

FireEye offers a minimally invasive solution for helping global organizations identify vulnerabilities and threats, reduce the risk of advanced attacks to their business and keep security costs under control. Our consulting services provide customers with tailored recommendations and testing services to build a security program that meets their unique needs. Leading, signature-less, behavior-based technology combined with partner OT integrations allow clients to detect, prevent, analyze and respond to the next generation of threats that moves laterally from IT to OT networks. These solutions include dedicated email, endpoint, network and forensics defenses to expand the detection, response and hunting capabilities of TAP. Fully deployed FireEye critical infrastructure and ICS network security delivers a comprehensive threat management security solution for your IT and OT environments.

For more information about our other IT security products and partner offerings, please visit **https://www.fireeye.com/products.html** and **http://info.belden.com/ics-security**

ABOUT FIREEYE, INC.

FireEye® is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 825 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com