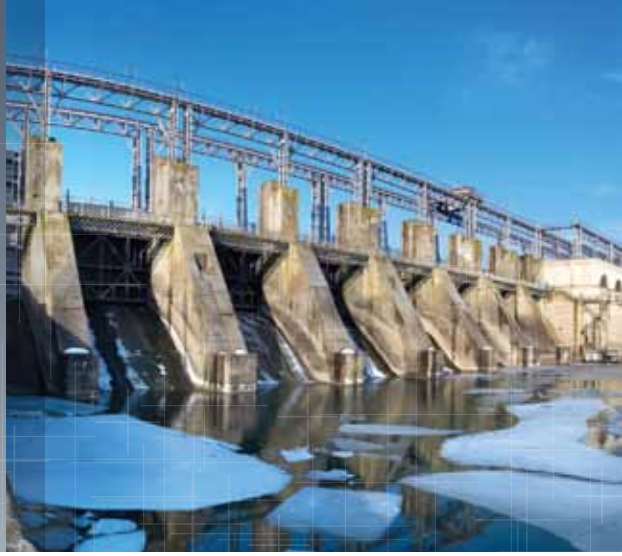
McAfee®
An Intel Company

PROTECT CRITICAL INFRASTRUCTURE

Solution Guide

In October 2011 researchers McCorkle and Rios researched industrial control systems and found 665 issues, such as remote code execution, local privilege escalation, and web exploits. They stated that the bugs were straight out of the 1990s. Later in January 2012, similar issues were disclosed across a broad range of industrial control systems, inferring that the majority of control systems remain at risk.



Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

Even lower level controls, such as programmable logic controllers or PLCs, have been discovered with unnecessary services and code, making them potentially susceptible to compromise. Some examples include: FTP, SNMP, HTTP, telnet, sample programs, and vendor debugging code.

Secure IT, SCADA, and Industrial Control Systems

Challenges

Organizations faced with securing critical infrastructure have a complicated task. There are multiple zones that must be secured, including enterprise IT, SCADA, and industrial control systems (ICS), and each of these zones has unique technical and political challenges. Adding to the complexity are regulatory mandates requiring demonstration of compliance and the critical job of maintaining operational availability. Historically, security companies tried to provide "bolted on" technologies that were designed for IT. They attempted to repurpose these IT technologies for SCADA and ICS. Unfortunately, this didn't work well, given the specialized nature of SCADA and ICS applications and protocols and even had a negative impact on availability. Purpose-built solutions designed to work across all three zones are necessary for the success of any critical infrastructure security program.

Most organizations are aware of what can happen when critical infrastructures are not adequately protected. Consequences range from regulatory penalties to breaches that compromise sensitive data on the IT side and can disrupt availability for SCADA and ICS operations. Air gaps and security through obscurity, which once supplied a somewhat more secure buffer, have been replaced by greater interconnectivity through wired and wireless networks running over IP, dial-up modems, and cellular solutions. Many SCADA and ICS systems run atop common hardware with popular operating systems and applications. While these changes have introduced greater operational efficiencies, flexibility, and reduced cost, they have also introduced a new layer of risk.

McAfee empowers organizations to address security and regulatory mandates while maintaining availability across IT, SCADA, and ICS. The Security Connected strategy breaks down the silos that segregate these zones from a protection, detection, and incident response perspective and allows for a much more robust security posture. In the past, solutions like this weren't conceived for critical infrastructure environments. They lacked the overarching capabilities to protect endpoint, network, and data across IT, SCADA, and ICS. But McAfee has changed all that. We offer solutions that are integrated across all zones, run in production environments within critical infrastructure organizations around the world, and protect those environments without impacting operational availability.

Many of the solutions operating within critical infrastructure environments—including those found in SCADA and ICS zones—run atop common hardware, operating systems, and applications. These solutions are connected through a variety of mechanisms: wired and wireless IP networks, modems, and cellular networks. At the same time, proprietary communications buses are used extensively. This duality exposes critical infrastructures to a broad range of exploits, while at the same time making it difficult to monitor and assess the consequences of that exposure.

In the Dark, a survey of 200 critical infrastructure organizations in 14 countries, revealed that one in four entities said they had been the victims of extortion. Eighty percent of respondents in Mexico and sixty percent in India stating that they had been targets of cyberextortion attempts.

Solutions

Protecting critical infrastructure is about a comprehensive solution—not a single product. To provide a solution that works, multiple products must operate together without introducing great complexity or impacting availability while providing high levels of protection. McAfee offers a number of products that are relevant in various zones—network firewalls, anti-malware, data loss prevention, change control, mobile security, security SaaS, and more. The four primary needs of critical infrastructure customers and partners are situational awareness, multizone protection, native support for SCADA and ICS solutions, and continuous compliance. To address these needs, McAfee leverages a select group of products and technologies that are highly relevant to critical infrastructures: dynamic whitelisting, security information and event management (SIEM), intrusion prevention systems (IPS), and database activity monitoring (DAM). These essential components of the Security Connected framework work in unison with the entire McAfee® and partner product portfolio.

Situational awareness

Getting visibility into what is happening across enterprise IT, SCADA, and ICS is essential to operational security and compliance. McAfee is unique in that it provides situational awareness across these zones with purpose-built solutions that allow for real-time security awareness and compliance with regulatory mandates. McAfee situational awareness capabilities also encompass forensic reporting and analysis capabilities for root cause analysis and audits. McAfee solutions that support situational awareness include: SIEM, reputation-based threat intelligence, risk prioritization, and centralized security management.

Multizone protection

Beyond awareness, organizations need security solutions that provide discovery, prevention, detection, response, audit, and management capabilities across the enterprise IT, SCADA, and ICS zones. McAfee delivers a number of security controls at the data, network, and endpoint layers for intelligence in depth within each zone. Key McAfee solutions that support multizone protection include Intel's secure silicon (McAfee Deep Defender), dynamic whitelisting, change management, network IPS and fire-walling, agent-based host and network-based DAM and DLP (data loss prevention), SIEM, centralized security management, risk prioritization, vulnerability management, and reputation-based threat intelligence.

Native support

There are a large number of vendors and protocols across IT, SCADA, and ICS solutions. Native support for these devices is key to enabling effective situational awareness and multizone protection. McAfee has native integration with McAfee and McAfee Security Innovation Alliance partner products for IT support. McAfee also natively monitors SCADA and ICS applications and protocols and supports log and event collection from SCADA and ICS devices. For example, the McAfee DAM solution provides application programming interface (API) integration with the OSIsoft PI System and pulls asset information tags into the McAfee SIEM solution for more accurate correlation and analysis. Dynamic whitelisting helps prevent any unauthorized code or malware from operating on fixed function devices and is ideal for SCADA and ICS systems that perform a finite set of operations. The McAfee IPS solution also features one of the broadest sets of ICS and SCADA-specific attack signature sets. Key McAfee solutions with native SCADA and ICS support include dynamic whitelisting, SIEM, DAM, and IPS.

Best Practices Considerations

- Employ solutions that supply situational awareness across data, network, and endpoint controls
- Implement controls that work across IT, SCADA, and ICS zones and can correlate information across all three
- Take advantage of solutions that are purpose-built for critical infrastructure environments and don't negatively impact availability
- Leverage anti-malware solutions that are not scan based, have small footprints and resource requirements, and don't require frequent updating or even network access
- Demand solutions that can help demonstrate compliance with regulatory mandates and offer capabilities that map directly to mandates
- Require a connected security framework that addresses security and compliance while reducing complexity and optimizing operational processes

Continuous compliance

Organizations responsible for critical infrastructure are forced to comply with a number of regulatory mandates ranging from NERC to PCI. This is a slow and costly manual process. McAfee helps by automating the process of reporting and demonstrating compliance with multiple regulatory mandates across enterprise IT, SCADA, and ICS. Because McAfee has situational awareness across these zones; controls across endpoint, network, and data; and native support to include SCADA and ICS protocols and applications, we can provide continuous compliance in an automated, fast, and easy-to-use interface and address auditor requirements in minutes instead of hours or days. Key McAfee solutions that support continuous compliance include centralized security management and SIEM.

Value Drivers

Solutions for protecting critical infrastructure should provide operational value by going beyond breach prevention and focusing on asset availability. Security for critical infrastructure should:

- Help limit legal fees, fines, and compliance costs in the event of a regulatory incident
- Provide more efficient and effective security controls across all zones, thus diminishing operational downtime
- Enable increased visibility across all operational environments to measure and maximize availability

Related Material from the Security Connected Reference Architecture

Level II

- Securing Fixed Function Devices
- Protecting Information
- Controlling and Monitoring Change

Level III

- Protecting Databases

For more information about the Security Connected Reference Architecture, visit: www.mcafee.com/securityconnected.

About the Author

Brian Contos, CISSP, is senior director, vertical and emerging market solutions at McAfee. He is a recognized security expert with nearly two decades of security engineering and management experience. He is the author of several books and has worked with government organizations and Forbes Global 2000 companies throughout the world. He is an invited speaker at leading industry events and has been interviewed by industry and business press. Brian is a Ponemon Institute Distinguished Fellow and graduate of the University of Arizona.

brian_contos@mcafee.com || http://siblog.mcafee.com/author/brian-contos/ || @BrianContos

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

42409sg_critical-infrastructure-L2_0212_wh