

Critical Infrastructure Protection

Securing the Cyber Fabric of Critical Infrastructure from Ground to Grid

Critical infrastructure, the systems that keep our water running, our electricity on, and our phone lines up, presents a natural target for increasingly sophisticated cyberthreats. It's no wonder that more government regulations are mandating more protection for these systems and networks. For compliance and long-term success, you will need to build in efficiency, visibility, and flexibility as you heighten protection for IT networks, control system networks, and the cyberinterfaces that connect them. McAfee can help guide your organization through the necessary optimizations that will reduce immediate exposure, improve situational awareness, and support a long-term architecture for security and compliance.

Every minute, more links in the supply chain interface with more of our critical infrastructure. Contractors, employees, billing departments, and field staff rely on a complex combination of leading edge as well as legacy technologies to support our demand for energy, communications, transportation, and financial services. However, we now have a treacherous combination of increasing cyberterrorism and distributed, under-protected systems. Critical infrastructure providers must accelerate their efforts to reduce risk while architecting IT systems for long-term safety.

Securing Our Critical Assets

One of the most pressing concerns today is that a vulnerability or control gap in IT systems will provide saboteurs and cyberthieves an entrance into less well-defended control systems networks, including supervisory control and data acquisition (SCADA) networks. These control networks were originally designed for availability, not security, since they were isolated from other networks.

However, in recent years, these networks have been interconnected for better efficiency and availability, connecting to each other and to management systems through IP-based infrastructure in IT networks. In turn, these IT networks interoperate over the Internet with other networks for efficient service delivery. Every connection opens doors for Internet-borne threats.

Since our economy and our lives depend on this infrastructure, industry regulators, consumers, and the government are all raising the alarm. They demand more investment, more oversight, and more assurance that these interconnected systems are secure. These demands come despite tight spending by consumers and cutthroat competition. The dilemma: regulation puts more pressure to invest on organizations whose executive teams are demanding operational savings and staff cuts.

McAfee is helping organizations around the world optimize their approaches to security and compliance. We have found that optimized security can cut operational costs. One survey found our customers spend 36 percent less time and manage security with 22 percent fewer staff than customers without centralized management.¹ So it is possible to improve security and cut costs. In fact, these efficiencies contribute to resilience and control that enable critical infrastructure to operate reliably. Instead of a paradox, we see an opportunity.

"A growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government. These actors have the ability to compromise, steal, change, or completely destroy information."

—Director of National Intelligence, Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record, March 10, 2009, at 39, as referenced in the *Cyberspace Policy Review*

¹ Research conducted by Insight Express.

McAfee Industry Collaboration

- CSIS Commission to Advise the 44th President on Cyber Security
- Co-Chair, Working Group on Public-Private partnership and Federal Coordination
- Co-Chair, Critical Infrastructure Protection Congress 2009 producing first global strategic plan for CIP
- IT-Sector Coordinating Council Member
 - Control Systems Working Group
 - Cross-Sector Cyber Security Working Group
 - R&D Working Group
- Critical Infrastructure Protection Congress Conference Committee 2007-2008
- InfraGard Founding Chairman and Chairman Emeritus, Board of Directors, InfraGard National Members Alliance
- Messaging Anti-Abuse Working Group (MAAWG), Board
- Microsoft Security Response Alliance, Technical expert members
- Organization for Internet Safety, Member adopters
- Anti-Phishing Working Group (APWG), Board
- Anti-Spyware Coalition (ASC), member
- Anti-Virus Product Developers (AVPD), member
- Computer AntiVirus Research Organization, member
- Common Vulnerabilities and Exposures (CVE), Board
- Open Vulnerability Assessment Language (OVAL), Board
- Common Configuration Enumeration (CCE), member
- Common Platform Enumeration, member
- Significant roles in Storm I and II

Requirements: Reduce Exposure and Plan for Change

In our work with the critical infrastructure industry, we have identified two classes of security investments for critical infrastructure providers today. The first reduces existing risk by eliminating vulnerabilities and improving run-time controls that support situational awareness, your ability to identify and respond to local and global events.

The second job requires recognition that threats and regulations constantly change and escalate. We need resilience in our systems so we can accommodate these changes gracefully, with minimal disruption. We have to plan for change. Through an open, unified architecture for security and compliance, you give yourself the long-term flexibility to add in protections and processes as needed.

The McAfee Advantage: Experience, Products, and Thought Leadership

McAfee brings valuable perspective to this dialog, as a security industry leader with a track record of service to critical infrastructure and the government. We bring more than two decades of deep expertise in information security, as well as experience protecting the most critical networks within utilities, network operation centers, banks, manufacturers, defense agencies, enterprises, and 150 million users around the world. Through outreach and collaboration, McAfee works closely with critical infrastructure providers and government agencies to fight cybersecurity threats.

McAfee experts lead and support global industry education, collaboration, and standards efforts specific to critical infrastructure, most recently the National Cybersecurity Initiative and the National Infrastructure Protection Plan. We also demonstrate our commitment with third-party validation: FIPS and Common Criteria product certifications as well as independent testing in the Pacific Northwest National Labs SCADA testbed and NSS Labs. Our industry commitment is one reason McAfee's largest deployment, more than five million nodes, is with the U.S. Department of Defense.

Through our understanding of critical infrastructure requirements, McAfee has developed solutions that protect the confidentiality, integrity, and availability of critical infrastructure IT networks. We offer protection for every threat vector, where it is needed: on mobile devices and endpoints, throughout distributed networks, and in the cloud. This breadth enables layered end-to-end security for distributed critical assets and IT infrastructure.

We understand that the different networks and systems in critical infrastructure require different approaches. We have network and endpoint security solutions appropriate to both IT and control system networks and specific tools to patrol trust boundaries around them.

Two distinctive investments unify our solutions: global threat intelligence and integrated management.

- *Global threat intelligence*—Extensive, multi-vector threat research infrastructure around the world allows us to predict breaking threats and gauge risk levels, bringing effective responses to products in real-time to protect you ahead of threats
- *Integrated management*—Our unified, open management platform connects the systems you count on; it eliminates redundant operational tasks to cut operational complexity, speed incident response, and support continuous compliance

With maximum protection and minimum effort, we help you achieve today's security goals quickly and, at the same time, grow your security infrastructure to achieve the resilience tomorrow requires.

Reducing Risk

Security job one today requires reducing vulnerabilities and adding protections that help you anticipate threats. The goal is to reduce risk through real-time visibility, consistent control, and reinforcing layers of coverage.

An Optimized Security Architecture

As you protect more threat vectors and more of your critical assets with McAfee® solutions, you move to an optimized security architecture. In addition to the security benefits and cost savings of global threat intelligence, you benefit from the efficiency and agility of a unified security and compliance management platform.

McAfee's Optimized Security Architecture enables one security product to leverage intelligence from other products. Integrations prepare you with real-time visibility, centralized security management, multi-layered protection, and automated compliance.

Key McAfee Products for Critical Infrastructure Protection

- McAfee Application Control
- McAfee Change Control
- McAfee Change Reconciliation
- McAfee Email Gateway (IronMail®)
- McAfee Encrypted USB
- McAfee Endpoint Encryption
- McAfee ePolicy Orchestrator® (ePO™)
- McAfee Firewall Enterprise (Sidewinder®)
- McAfee Integrity Monitor
- McAfee Network Access Control
- McAfee Network DLP Discover
- McAfee Network DLP Monitor
- McAfee Network DLP Prevent
- McAfee Network Security Platform
- McAfee Network User Behavior Analysis
- McAfee Policy Auditor
- McAfee Total Protection for Endpoint
- McAfee Vulnerability Manager
- McAfee Web Gateway (formerly Webwasher®)

Risk assessment

Risk reduction starts with understanding your weaknesses and the likelihood of different threats or attacks. For an unbiased evaluation, McAfee® Foundstone® professional services experts can check the health of your security technologies and processes throughout your environment, weighing your situation against industry best practices. For SCADA environments, a tailored critical infrastructure security assessment can help you identify weaknesses in your SCADA security posture. You will emerge with actionable recommendations for mitigating risks from external attackers, insider threats, automated worms, and network management errors.

Risk mitigation

Once you understand where your gaps are, McAfee has solutions you can deploy quickly. Some of the ways we can help improve protection for IT networks include:

- Network control
 - » Enable and control secure remote access for employees, contractors, and the supply chain
 - » Raise protections against targeted attacks, application-layer attacks, insider attacks, spam, and malware delivered through email, web, and other protocols
 - » Verify segregation of duties and patrol trust boundaries at network interfaces
 - » Use network shielding to limit emergency patching of systems
- Application control
 - » Apply application controls, such as application-layer firewalls and whitelisting, to manage use of sensitive applications
 - » Restrict use of potentially risky software, such as peer-to-peer or social networking
- System control
 - » Layer anti-malware, intrusion prevention, and other protection on IT systems, including portable storage, laptops, email servers, and virtualized systems
 - » Lock down configurations of highly critical assets, including field devices, to prevent compromise through malware and access violations
- Data control
 - » Enforce encryption of mobile devices, endpoints, and network transmissions
 - » Prevent leakage of critical asset information and regulated data through Improved data controls, such as data discovery, monitoring, and policy-based enforcement
- Situational awareness
 - » Gain real-time visibility into anomalous user, application, and system activities that could signal the presence of malware, attacks, or an insider threat
 - » Quickly assess, prioritize, and respond to new vulnerabilities
 - » Leverage more than two decades of experience with worldwide activities in malware, network and application attacks, email and web exploits
 - » Increase preparedness and protect proactively through real-time visibility into new global and local threats that might affect your operations

Several of these capabilities can also improve monitoring and limit access to restricted control system networks. For example, network user behavior analysis can dynamically report unusual activity at the cyberinterfaces between IT and control system networks. Activities might be precursors to an attack, attempts to bypass required controls, or evidence of malicious activity.

McAfee Global Threat Intelligence available for Critical Infrastructure

Malware Research

- 50,000 samples/day
- 1.5M malware detections in 2008

Vulnerability Research

- 100 sources monitored daily
- 20 vulnerabilities discovered

Network Security Research

- 10M IPS alerts monitored/analyzed daily
- 1000T traffic monitored/analyzed daily

Web Security Research

- Rated over 30 million sites classified in over 96 categories
- 200,000 zombies identified per day

Email Research

- Over 10 billion messages processed each month

Customer Installations

- 50 million enterprise nodes
- 100 million consumer nodes

Efficient, Resilient Infrastructure for Today and the Future

As you weave in appropriate controls, if you choose standalone products, each new protection has the potential to add a separate management and monitoring environment. This is where McAfee integrations shine. Our strategy is to help you create a cybersecurity command and control platform. Based on policies, not hard-coded rules, our open, unified management platform will help you evolve with changing threats, industry changes, and—naturally—regulations.

Our single agent design supports multiple protections with ease and minimizes system and user impact. Post-installation, you can maintain policies centrally and monitor events with unified dashboards that you define. They can present the data and events from the products you care about at the level of detail that matters. Every role—including auditors—benefits from its own view.

Situational awareness

When things go wrong or an attack threatens, real-time alerts will notify you immediately. Instead of popping open several different consoles to investigate, you view integrated displays. You can drill down to identify affected systems, diagnose causes, and marshal effective responses. Integrated displays and tasks help you turn awareness into appropriate action, fast.

For forensic studies of events, data monitoring tools create an indexed database that provides details of changes and context for events. Network security tools can aggregate and archive log data, eliminate unneeded data “noise,” and present it when needed within crisp reports. View system state “before” and “after” to investigate changes. Actionable reporting dashboards help you quickly navigate attack details.

Behind this integrated control environment sits McAfee Global Threat Intelligence. Our worldwide research infrastructure collects threat data from millions of sensors and client nodes. Applying content inspection, reputation, and research across threat vectors, we can correlate these data sources to identify new threats and predict their levels of risk.

Critical infrastructure providers can work with us to receive custom data feeds from this global pool. This early warning of events with informed risk assessments can let you determine if activity you are facing is a targeted threat, a broad-based action, or a non-event.

Continuous compliance

From the start, every investment you make in McAfee security has a payoff for compliance. Our integrated security and compliance platform eases the effort of implementing policies, compiling data, and generating consistent, meaningful reports. These functions are built in to our solutions, reducing the need for manual, incremental steps to prove compliance. Only McAfee lets you enforce policies end-to-end with dynamic whitelisting and application trust technology, anti-virus, anti-spyware, host intrusion prevention, policy auditing, and firewall technologies.

We also offer a range of governance, risk, and compliance solutions to help you build out compliance policies, processes, and programs, such as risk assessment, auditing, and vulnerability management. These, too, integrate into our centralized management platform for seamless operation. Together, our solutions enable sustainable, continuous compliance. You can:

- Customize policies, dashboards, and data formats for your organization
- Implement and maintain policies consistently throughout your environment
- Reduce risk of data loss and other violations by applying run-time network, system, data, and application controls and monitoring for unusual behavior
- Centrally view security status and policy compliance of endpoint, network, and data controls
- Reliably audit both agent and agentless systems and easily collect and collate audit data
- Schedule automated reports with the confidence that data will always be up-to-date
- Program waivers, blackouts, and scheduled audits for minimum operational impact

Summary and Next Steps

The cyberthreat is real. McAfee enables an optimized security architecture that helps critical infrastructure providers invest wisely. We can help you reduce vulnerabilities, manage risk, and create an efficient command and control environment for maintaining security and compliance. This broad, integrated approach means you can defend immediately while laying a resilient foundation that can embrace the future.

Only McAfee offers interlocking protections from the cloud to the endpoint, enabling the reinforcing controls required for secure, non-stop operation and continuous compliance.

Only McAfee has the global reach and multi-vector threat research to predict threats and equip you to gauge their risk to you.

Only McAfee has an integrated security and compliance platform to help improve your resilience and your ability to cost-effectively monitor and respond to changing situations and compliance demands.

Connect with McAfee at www.mcafee.com to learn more.

