FISMA and SANS Critical Security Controls Driving Compliance

In a bid to bolster cyber security today's highly networked computing environment, the Federal Information Security Management Act (FISMA) imposes strong requirements on federal agencies and private organizations to secure government information. The requirements apply to both federal government agencies and any outside entities that exchange data with federal information systems.

The requirements span three major categories:

- Assessment—determining the adequacy of federal asset security
- Enforcement—implementing and managing key information security provisions
- Compliance—establishing provisions for managing information security programs and the accountability for compliance and reporting

FISMA directs the National Institute of Standards and Technologies (NIST) to create and manage the technical standards in each of the above categories. Key standards include the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations and the NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. The Office of Management and Budget (OMB) manages FISMA compliance audits.

The broad scope of technical standards specified by NIST for FISMA compliance presents a challenge for federal agencies and organizations that exchange data with federal systems. For example, the security framework in SP 800-53 includes 17 areas of security covering 205 technical and program management controls. Mapping these to the IT operations of a large organization followed by implementation and ongoing management is a complex process.

To help address the FISMA challenge, current and past federal chief information officers (CIOs) and chief information security officers (CISOs), working in conjunction with the SANS Institute, created the Consensus Audit Guidelines (CAG). CAG includes 20 critical controls for effective cyber defense. Following these recommendations can enable federal agencies and private organizations to block known high-priority attacks and new, emerging types of attacks.

The SANS Institute has also issued controls to guide compliance for both federal agencies and private organizations. The SANS 20 Critical Security Controls Revision 4.1 (soon to be under the aegis of the Council on CyberSecurity) aims to achieve the following:

- Strengthen the defensive posture of an organization's information security
- Reduce compromises, recovery efforts, and associated costs
- Protect critical assets and infrastructure

The SANS controls help organizations achieve these goals by providing guidelines for establishing continuous, automated monitoring of the riskiest portions of information technology infrastructures. The controls also present a prioritized, risk-based approach to security based on actual threats.

Continuous Monitoring Thwarts Advanced Malware and Advanced Threats

The Risk Management Framework (RMF) developed by NIST describes a disciplined and structured process that integrates information security and risk-management activities into the system-development life cycle. A critical part of that risk-management process is Information Security Continuous Monitoring (ISCM), which NIST defines as follows:

> *Maintaining on-going awareness of information security, vulnerabilities, and threats to support organizational, risk-management decisions.*

FISMA recognizes the need to detect advanced threats in real time. To that end, it provides guidelines to replace a periodic-assessment approach to improve cyber security posture and overall situational awareness. Section 3541 of FISMA acknowledges that commercially developed information security products offer advanced, dynamic, robust, and effective information. FISMA also acknowledges that cyber security solutions can be integrated immediately for real-time threat assessment; rapid and actionable threat analysis; and proactive blocking and risk remediation—before information or infrastructure damage takes place.

Section 3541 also states continuous monitoring can replace the current periodic assessment approach to improve security capacity and protect critical infrastructure systems. When federal government agencies expand their compliance standards to actionable models of threat prevention, they gain a never-before-possible opportunity to track malware to its source as part of the risk-remediation process. This statement by FISMA reflects the widely available market solutions provided by the private sector for protecting critical information infrastructures. These solutions also serve an important role in the nation's defense and economic security.[1]

FISMA Section 3544 calls out advanced malware and the importance of detecting and blocking zero-day threats and the responsibilities of federal agencies and their delegated authorities, such as the agency's CISO.

Here are key excerpts from that section, which identifies advanced malware detection and remediation as critical components of a robust continuous monitoring program:

- Federal agencies must ensure senior officials provide information and secure information systems that support the operations and assets under their control. This includes assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information systems. Both systemic and targeted attacks on the information infrastructure systems of government agencies are typically directed at specific data and/or controls, so the ability to perform real-time, deep forensic analysis on detected and proactively-blocked malware increases agency insight into how malware is designed and specifically what it attempts to access. In some cases, real-time forensic analysis can determine which command-and-control (CnC) components the malware is designed to communicate with, thereby broadening the impact and tracking the reach of continuous monitoring and remediation.[2]
- An agency's CIO or comparable official must ensure compliance with the requirements imposed on the agency. This includes training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities. The training must also focus on understanding that compliance is not always synonymous with security, and that threat analysis, detection and blocking paradigms must be actionable and track malware back to its source.[3]

- Agencies must establish procedures for real-time analysis detection, active blocking, and reporting while also responding to security incidents as actionable threats consistent with standards and guidelines—such as mitigating risks associated with such incidents before substantial damage occurs. This can be achieved by blocking advanced malware and creating new blocking rules in real time with continuous monitoring. For example, automated data streams fed to the DHS through its cyberscope reporting system can be improved with security platforms that employ actionable detection and real-time blocking technologies to prevent zero-day and APT attacks. Agencies must also shift away from static compliance to real-time awareness of the threat landscape through continuous cyber monitoring, active analysis, threat agnostics, and real-time blocking of APT and zero-day attacks. For example, real-time blocking—which is essential for mitigating risk—is widely available. But analysis tools are also available that can more rapidly assess the threats posed by zero-day and APT attacks to track them back to their source CnC centers.[4]

Fulfilling NIST and SANS Controls: The FireEye Platform

Traditional signature-based products are ineffective against today's advanced malware. These threats, launched by hostile nation-states and organized crime, seriously jeopardize national secrets and sensitive information. But many federal agencies and private organizations lack the tools to proactively monitor for zero-day exploits and associated call-backs. These organizations are likely compromised and unaware of the persistent threats already permeating their enterprise.

To help federal agencies and private organizations resolve this challenge in accordance with the NIST and SANS controls, FireEye provides a leading platform for detecting advanced malware when it first appears on the network. Security-conscious organizations can deploy the FireEye platform to complement traditional signature-based solutions to detect, contain, and block advanced malware that traditional defenses miss.

Taking this approach addresses many of the compliance controls outlined in the NIST 800-53 Revision 4 and SANS Critical Controls Revision 4.1 manuals. The tables below illustrate how the FireEye platform addresses the most progressive controls while also providing invaluable tools for incident response teams that need to quickly detect, block, validate, and remediate advanced malware incidents.

FireEye Capabilities for Advanced Malware Detection and Incident Response Compliance Controls

Key NIST Compliance Controls	FireEye Platform Capabilities
SP 800-53—SC-44 Detonation Chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of quickly determining whether the associated attachments/ applications contain malicious code and prevent lateral movement.	FireEye identifies and blocks advanced cyber attacks through a virtual machine-based security platform built from the ground up to combat a new generation of threats. These highly sophisticated attacks easily slip through traditional signature-based defenses such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye platform does not use malware signatures, so it can identify and block these never been seen before threats in real time. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, that protects the primary threat vectors: Web, email, files, and mobile devices The patented FireEye® Multi-Vector Virtual Execution™ (MVX) engine detonates suspicious files and Web objects within instrumented virtual machines to analyze behavior. The MVX engine conducts deep packet inspection to identify systems under attack (along with previously infected machines) with pinpoint accuracy that virtually eliminates the problem of false positives. Analysis occurs in two stages. Phase one includes aggressive capture analysis that identifies suspicious network activities. This ensures all potential attacks are identified, avoiding false negatives. Outputs from phase one flow into phase two, the confirmation stage. Network traffic flows are replayed within the MVX engine to validate whether the code is indeed malicious, avoiding false positives.
SP 800-53—SC-35 Requirement: Honeyclients Honeyclients proactively seek to identify malicious websites and/or web-based malicious code. Honeyclients require some supporting isolation measures (e.g., virtualization) to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational information systems.	The FireEye platform proactively detects malware when end host systems fetch content from websites or execute Web-based malicious code. The patented FireEye MVX engine supports isolation techniques by detonating the Web objects within instrumented virtual machines to analyze behavior. The FireEye MVX engine approaches threat prevention from a perspective of efficacy and timeliness of response. The core of MVX begins with the FireEye hardened hypervisor, a purpose-built hypervisor designed for threat analysis with built-in countermeasures against malware. This hardened hypervisor supports numerous parallel execution environments or virtual

Key NIST Compliance Controls	FireEye Platform Capabilities
	machines with a combination of operating systems, service packs, and applications. The key FireEye technology differentiation is that there is no additional traffic generated to detect the malicious websites.
SP 800-53—IR-4 (4) Incident Handing/ Information Correlation The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. Supplemental Guidance: Sometimes the nature of a threat event, such as a hostile cyber attack, can only be observed by bringing together information from different sources including various reports and reporting procedures established by the organization.	FireEye exposes the entire cyber attack life cycle by correlating intelligence across all major threat vectors and callback channels. The FireEye platform weaves together intelligence from individual threat prevention platforms—the NX series for Web, EX series for email, and FX series for file shares—for a complete picture of advanced attacks. This integrated view of threats helps protect agencies against advanced attacks that utilize multiple attack vectors across various stages of malware infiltration. To guard against sophisticated spear-phishing attacks, security teams must discover Web-based attacks in real time. They must be able to trace the initial email that spawned the attack and analyze it to determine whether the attack has targeted others within the organization. Working with the FireEye NX series and EX series threat prevention platforms, the FireEye CM series central management platform correlates malicious URLs with the originating emails and the intended targets to expose the entire attack life cycle and inoculate other potential targets. In addition, the FireEye AX series threat prevention platform features robust and detailed incident forensic analysis. When threat analysts need a secure environment to test, replay, characterize, and document advanced malicious activities, they can simply load a suspicious email attachments, PDF documents, and Web objects into the AX series platform to get a 360-degree view of the attack—from the initial exploit and malware execution path to the callback destinations and follow-on binary download attempts.
SP 800-53—IR-4 (2) Incident Handling/ Dynamic Reconfiguration The organization includes dynamic reconfiguration of organization-defined information system components as part of the incident response capability.	Leading security and incident response teams agree that speed at the exploit-detection phase of the kill chain is critical. That's because the rest of the attack steps—reconnaissance, malware control, command and callback, and data exfiltration—can be hidden. FireEye can effectively detect, block, and mitigate the threat at the initial indicator of compromise to disrupt the kill chain and block the attacker from infiltrating further.

Key NIST Compliance Controls	FireEye Platform Capabilities
Supplemental Guidance: As an example, dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. As another example, organizations perform dynamic reconfiguration of information systems to stop attacks, misdirect attackers and isolate components of systems—thus limiting the extent of the damage from breaches and compromises. Organizations should also include time frames for achieving the reconfiguration of information systems in the definition of the reconfiguration capability while considering the potential need for rapid response to effectively address sophisticated cyber threats.	The FireEye platform, which includes the FireEye Dynamic Threat Intelligence™ (DTI) cloud, detects and stops attacks coming in through multiple vectors that exploit zero-day vulnerabilities—when they first appear on the network, within minutes rather than weeks or months. In addition, the FireEye platform integrates with endpoint, Web gateway, and data security tools to quickly confirm breach incidents, validate the extent of malware infiltration, and quarantine the endpoint or host to limit any lateral damage. This integration balances timeliness and accuracy so that incident response teams can quickly restore systems for maximum business continuity and uptime.
SP 800-53—IR-5 Incident Monitoring Control: The organization tracks and documents information system security incidents. Supplemental Guidance: For example, documenting information system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources such as incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	Incident response teams can gather complete cyber forensic details of attacks in real time from the FireEye platform. The solutions capture the exploit point of Web, email, and file threat vectors and complete details of blended attacks through continuous monitoring, packet capture, and heuristics of all incoming Web and email traffic in the FireEye MVX engine. • Email: Spear-phishing emails are one of the most common approaches for launching APT attacks on federal agencies. The FireEye EX series threat prevention platforms block these types of threats while providing real-time analysis of URLs in emails and email attachments, to determine whether they are malicious. • Web: Browser-based threats and malicious communications can take many forms and move across a range of protocols, including FTP, HTTP, and IRC. The FireEye NX series threat prevention platforms track websites and communications in real time across these different protocols to thwart APT attacks. • Content/Files: Malicious content in files target application vulnerabilities and can be introduced into a network in any number of ways, whether through USB drives, mobile devices, or remote downloads from a cloud service. In addition, these malicious files can be purposely or inadvertently saved to any number of locations throughout an organization and then lie dormant for a period of time before they exhibit malware behavior. The FireEye FX series threat prevention platforms solve this challenge by continuously scanning and eliminating malware resident on file shares.

Key NIST Compliance Controls	FireEye Platform Capabilities
NIST SP 800-53—IR-6 (1) Incident Reporting Control—The Organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within organization-defined time period; b. Reports security incident information to organization-defined authorities. Supplemental Guidance: This control addresses both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. For example, suspected security incidents include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.	The FireEye platform detects malware command-and-control (CnC) servers while aiding attribution as part of a security ecosystem. Integration with security information and event management (SIEM) tools allows incident response (IR) teams to add context from other security systems to FireEye data, then automate reporting and response tracking as part of an active defense. The FireEye platform integrates with security incident-management and event-management tools to enable IR teams to view a complete correlation and pattern of malware attacks in relation to other attacks. Because IR teams spend a lot of time in logs, the ability to quickly close out false positives and duplicates saves significant effort and reduced churn within IT teams performing remediation. Getting this holistic view of threats and patterns over time shows the effectiveness of different tools, defense-in-depth layers, and processes applied within an organization's security deployment.

<table>
<tr><th>SANS 20 Critical Security Controls</th><th>FireEye Platform Capabilities</th></tr>
<tr><td>Control 4—Vulnerability Management

Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers often engineer exploited code and then launch that code against targets of interest. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, giving them control over the vulnerable machines and access to their sensitive data.

Organizations that do not scan for vulnerabilities and do not proactively address discovered flaws face the significant likelihood of compromised computer systems. Vulnerabilities must also be tied to threat intelligence.

As vulnerability scans become more common, attackers utilize them as a point of exploitation. Federal agencies and private organizations thus must carefully control authenticated vulnerability scans and the associated administrator account. Otherwise, attackers will take over one machine with local privileges and wait for an authenticated scan to occur against the machine.

When the scanner logs in with domain admin privileges, the attacker either grabs the token of the logged-in scanning tool or sniffs the challenge response to crack it. Either way, the attacker can then pivot anywhere else in the organization as a domain administrator.

Quick Win #1: Run automated vulnerability scanning tools against all systems on their networks on a weekly or more frequent basis using a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (CVE) and configuration-based vulnerabilities (CCE). Any vulnerability identified should be remediated in a timely manner, with critical vulnerabilities fixed within 48 hours.</td><td>SANS quick win and configuration guidelines to address this control include use of authenticated vulnerability scanners. However, such scanners only work against known or previously-reported vulnerabilities with known Common Vulnerabilities and Exposures (CVE) identifiers.

The FireEye platform exceeds this requirement by detecting zero-day vulnerabilities. The FireEye MVX engine detects both known and unknown vulnerabilities in applications and operating systems.

FireEye is the only solution that takes into account threat intelligence on zero-day vulnerabilities while also isolating and blocking attacks at the exploit phase—the top of the attack kill chain, before an attacker can pivot or gain administrative privileges. Leading security and incident response teams agree that speed at the exploit detection phase of the kill chain is critical, because subsequent phases can be obfuscated.

FireEye is the leading solution for detecting an exploit occurrence when malware first appears on the network.

The following table, lists 11 of the 12 zero-day attacks that were identified by FireEye and occurred in the recent past:

<table><tr><th>Date</th><th>CVE ID</th><th>App</th></tr><tr><td>Aug 2012</td><td>CVE-2012-4681</td><td>Java</td></tr><tr><td>Dec 2012</td><td>CVE-2012-4792</td><td>IE</td></tr><tr><td>Jan 2013</td><td>CVE-2013-0422</td><td>Java</td></tr><tr><td>Feb 2013</td><td>CVE-2013-0634</td><td>Flash</td></tr><tr><td>Feb 2013</td><td>CVE-2013-0640
CVE-2013-0641</td><td>PDF</td></tr><tr><td>Feb 2013</td><td>CVE-2013-1493</td><td>Java</td></tr><tr><td>May 2013</td><td>CVE-2013-1347</td><td>IE</td></tr><tr><td>June 2013</td><td>CVE-2013-1331</td><td>Office</td></tr><tr><td>Sept 2013</td><td>CVE-2013-3893</td><td>IE</td></tr><tr><td>Nov 2013</td><td>CVE-2013-3906</td><td>Office</td></tr><tr><td>Nov 2013</td><td>CVE-2013-3918</td><td>IE</td></tr></table></td></tr>
<tr><td>Control 5—Malware Defenses:

Quick Win #5: Scan and block all email attachments entering the organization’s email gateway if they contain malicious code or file types not in use by the organization. Scanning should be done before email is placed in the user inboxes. This includes email content filtering and Web content filtering.</td><td>The FireEye EX series threat prevention platform stops cyber attacks that use spear phishing to evade signature-based and reputation-based defenses to compromise the majority of today’s networks. Spear phishing is extremely effective with the availability of user-specific information on social networks and other Internet resources. Cybercriminals abuse this information to craft an email that unsuspecting users are lured into opening.</td></tr>
</table>

SANS 20 Critical Security Controls	FireEye Platform Capabilities
	The FireEye platform weaves together intelligence from individual threat prevention platforms—the NX series for Web, EX series for email—for a complete picture of advanced attacks. This integrated view of threats helps protect agencies against advanced attacks that utilize multiple attack vectors across various stages of malware infiltration. FireEye EX series also analyzes all email for malicious URLs and attachments to protect against zero-day and APT attacks. In addition, the solution complements existing email spam gateways.
Control 5—Malware Defenses Quick Win[5] #7: Deploy features and toolkits—such as Data Execution Prevention and Enhanced Mitigation Experience Toolkit—that provide sandboxing (e.g., running of browsers in a virtual machine) and other techniques that prevent malware exploitation.	FireEye identifies and blocks advanced cyber attacks through a virtual machine-based security platform built from the ground up to combat a new generation of threats. These highly sophisticated attacks easily slip through traditional signature-based defenses such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye platform does not use malware signatures, so it can identify and block these threats in real time. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, that protects the primary threat vectors: Web, email, files, and mobile devices. The patented FireEye MVX engine detonates suspicious files and Web objects within instrumented virtual machines to analyze behavior. The MVX engine conducts deep packet inspection to identify systems under attack (along with previously infected machines) with pinpoint accuracy that virtually eliminates the problem of false positives. Analysis occurs in two stages. Phase one includes aggressive capture heuristics that identifies suspicious network activities. This ensures all potential attacks are identified, avoiding false negatives. Outputs from phase one flow into phase two, the confirmation stage. Network traffic flows are replayed within the MVX engine to validate whether the code is indeed malicious, avoiding false positives.
Control 5—Advanced Malware Defenses Visibility/Attribution Measure[7] #10: Ensure automated monitoring tools use behavior-based anomaly detection to complement and enhance traditional signature-based detection.	Integration and correlation of analysis from the FireEye platform and endpoint security tools identify and block malware before infiltration. The FireEye platform leverages a two-stage, multi-protocol inspection of objects and packets and a dynamic real-time analysis in a virtual execution environment.

SANS 20 Critical Security Controls	FireEye Platform Capabilities
Visibility/Attribution Measure #11: Utilize network-based, anti-malware tools to analyze all inbound traffic and filter out malicious content before it arrives at the endpoint.	Analysis occurs in two stages. Phase one includes aggressive capture heuristics that identify suspicious network activities. This ensures all potential attacks are identified, avoiding false negatives. Outputs from phase one flow into phase two, the confirmation stage. Network traffic flows are replayed within the MVX engine to validate whether the code is indeed malicious, avoiding false positives.
Control 5—Advanced Malware Defenses Advanced Sub-Control #13: Implement an incident response process that allows the IT support organization to supply the security team with samples of malware running undetected on corporate systems. Samples should be provided to the security vendor for "out-of-band" signature creation and deployed to the enterprise by system administrators.	The FireEye CM series central management platform consolidates management, reporting, and data sharing within the FireEye platform. Incident response teams can quickly analyze unknown malware to generate new signatures. In addition, the FireEye DTI cloud disseminates threat intelligence to stop cyber attacks—a critically useful tool for system and security administrators. The DTI cloud is a real-time, global exchange cloud platform that efficiently shares anonymized, standards-based threat intelligence metadata. The FireEye platform integrates with security incident-management and event-management tools that allow IR teams to view a complete correlation and pattern of malware attacks to reveal how they relate to other attacks. IR teams spend significant time examining logs. So the ability to quickly close out false positives and duplicates saves effort and reduces churn within IT teams performing remediation. Over time, getting a holistic view of threats and patterns demonstrates the effectiveness of different tools, defense-in-depth layers, and processes applied within an organization's security deployment.
Control 5—Malware Defenses: Advanced Sub-Control[6] #14: Utilize network-based flow analysis tools to analyze inbound and outbound traffic and to look for anomalies, indicators of malware, and compromised systems.	The patented FireEye MVX engine detonates suspicious files and Web objects within instrumented virtual machines to analyze behavior. The MVX engine conducts deep packet inspection to identify systems under attack (along with previously infected machines) with pinpoint accuracy that virtually eliminates the problem of false positives. Analysis occurs in two stages. Phase one includes aggressive capture heuristics that identifies suspicious network activities. This ensures all potential attacks are identified, avoiding false negatives.

SANS 20 Critical Security Controls	FireEye Platform Capabilities
	Outputs from phase one flow into phase two, the confirmation stage. Network traffic flows are replayed within the MVX engine to validate whether the code is indeed malicious, avoiding false positives. The FireEye platform examines the entire malware life cycle. Multi-vector, multi-flow analysis correlates activity in both inbound and outbound traffic in real time. The FireEye platform provides the following: • Exploit detection • Malware executable identification • Cross-matrix of OS and apps • Originating URL • Subsequent URLs • OS modification report • CnC protocol descriptors
Control 13—Boundary Defenses Quick Win #1: Deny communications with or limit data flow to known malicious IP addresses (blacklists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (un-routable or otherwise unused IP addresses) into the network to verify they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet. To control the flow of traffic through network borders and to police content by looking for attacks and evidence of compromised machines, boundary defenses should be multi-layered—relying on firewalls, proxies, and DMZ perimeter networks as well as network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic.	SANS quick win and configuration guidelines to address this control include use of signature-based tools and layered approaches—including IPS, IDS devices or next-generation firewalls—and network and endpoint whitelist and blacklist solutions. But these traditional signature-based defenses protect against only known or previously reported threats, those for which signatures have been written. FireEye is the leading protection against zero-day vulnerabilities and unknown threats. FireEye combines virtual machine-based detection and analysis with global threat intelligence to defend against attacks. When deployed in-line at the boundary defense, FireEye isolates and blocks attacks at the exploit phase. It also works in subsequent phases to prevent malicious inbound and outbound traffic from reaching CnC centers. FireEye NX series threat prevention platforms operate as turnkey appliances that can be deployed at Internet egress points to block inbound exploits and outbound multi-protocol callbacks. The FireEye platform also integrates with existing boundary defense technologies—including as endpoint, data, and Web gateway security products—to confirm the exact location and criticality of the malware infiltration.

SANS 20 Critical Security Controls	FireEye Platform Capabilities
Control 17—Data Loss Prevention Visibility/Attribution Measure #2: Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.	The FireEye platform stops cyber attacks by detecting and eliminating advanced malware residing on file shares that contain sensitive information. While traditional data loss protection solutions focus on data loss due to unintentional data disclosures or insider threats, the FireEye platform focuses on identifying and preventing malware infections from external threats. Because the FireEye platform is deployed in-line, the technology blocks outbound callbacks to prevent data loss. In addition, the FireEye MVX engine performs signature-less, stateful attack analysis within the most sophisticated virtual machines in the world. The FireEye platform detects and blocks callbacks and communications on various protocols to CnC servers, which allow remote control of malware exfiltrating the data. Early and preemptive detection—before the callback phase—enables agencies to stop malware from spreading laterally or compromise sensitive systems and user accounts.
Control 17—Data Loss Prevention Advanced Sub-Control #8: Block access to known file transfer and email exfiltration websites.	FireEye provides the only multi-vector solution that can effectively detect, analyze, and protect against unknown malware and targeted APT attacks, whether they come through the Web, email, file, or blended attack vectors. In addition, FireEye provides automated, multi-stage advanced protection to contend with all stages of the attack life cycle—especially exfiltration after malware is detected. FireEye spots attacks by identifying the initial exploit, analyzing the malware binary, and stopping outbound callbacks to CnC servers. The FX series and EX series threat prevention platforms also correlate with the NX series threat prevention platforms to prevent exfiltration.
Control 18—Incident Response and Management The process and tools to ensure an organization develops a properly-tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events. Note: This control has one or more sub-controls that must be validated manually.	FireEye services (including Oculus Continuous Monitoring) and FireEye Labs feature a global team of incident and forensics consultants to assist with breach response in case of a malware incident and to help organizations establish organizational and process best practices. These consultants, some of the industry's top cyber analysts, combine leading-edge forensics skills with the latest research findings from the threat community and FireEye development teams. This threat intelligence is critical to evolving the knowledge base and response workflows against new threats.

SANS 20 Critical Security Controls	FireEye Platform Capabilities
Considerable damage has been done to organizational reputations and a great deal of information has been lost in organizations without fully-effective incident response plans. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact—causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible if an effective incident response had been deployed.	

Transforming Cyber Operations from Reactive Remediation to Proactive Intelligence

Legacy, signature-based solutions and file-based sandbox analysis fail to detect and stop advanced malware. Federal agencies and private organizations need a fundamentally new approach to develop situational awareness in an environment of a rising volume of advanced threats. At the same time, organizations must also understand that compliance is not always synonymous with security. Threat analysis, detection, and blocking paradigms must be actionable and track malware back to its source.

FireEye solutions solve these challenges by detecting advanced malware as soon as it appears on the network. The FireEye platform offers these unmatched capabilities:

- Detection speed within minutes vs. weeks or months
- Identification at the critical exploit phase
- Discovery at all subsequent phases of malware attacks—exploit, download, callback, and data exfiltration
- Visibility into malware's lateral movement
- Real-time intelligence and cyber forensics across the entire attack life cycle
- High accuracy—the lowest number of false positives and negatives

Gaining these capabilities enables security teams to conduct real-time forensic analysis to determine which CnC components malware attacks try to reach. Agencies and organizations that leverage the FireEye platform can also discover much greater volumes of advanced malware. This benefit enables them to transform their cyber operations focus from reactive remediation to proactive intelligence, generating advanced visibility to stop threats.

The FireEye platform also enables security teams to leverage automated data streams by employing actionable detection and real-time blocking technologies that prevent zero-day and APT attacks. Ultimately, this enables federal government agencies and private organizations to effectively address the most progressive monitoring compliance mandates, including the latest malware detection guidelines issued by NIST and SANS.

For More Information

For more information on how the FireEye platform can help your organization protect your networks, data, and intellectual property and fulfilling the NIST and SANS control recommendations, click on the following links:

FireEye Platform

FireEye Multi-Vector Virtual Execution (MVX) engine

FireEye Dynamic Threat Intelligence (DTI) cloud

FireEye Web Security (NX series)

FireEye Email Security (EX series)

FireEye Content Security (FX series)

FireEye Forensic Analysis (AX series)

FireEye Central Management (CM series)

Footnotes

1. **FISMA Section 3541 of the Purpose Section (5):** Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information and cyber security solutions that can be immediately integrated for real-time threat assessment, rapid and actionable threat analysis, proactive blocking and risk remediation before information or infrastructure damage takes place, and continuous monitoring as a replacement for the current periodic assessment approach, in order to improve security capacity and protect critical infrastructure systems, recognizing that when agencies expand their compliance standards to actionable models of threat prevention, the unprecedented opportunity to track malware to its source becomes part of the risk remediation process, reflecting widely available market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector.
2. **FISMA Section 3544 federal agency responsibilities section 2 (A):** Ensure that senior agency officials provide information Security for the information and information systems that support the operations and assets under their control, including through—(A) Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems, recognizing that both systemic and targeted attacks on government agencies and information infrastructure systems are directed at specific data and/or controls, so the ability to perform real-time deep forensic analysis on detected and proactively blocked malware increases agency insight into how the malware is designed and specifically what is was attempting to access and, in some cases, to which C&C the malware is designed to communicate, thereby broadening the impact and tracking reach of continuous monitoring and remediation;
3. **FISMA Section 3544 federal agency responsibilities section (3):** Delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this sub-chapter, including—(D) Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities, with a focus on understanding that compliance is not always synonymous with security, and that threat analysis, detection and blocking paradigms must be actionable and able to track the malware back to its source;
4. **FISMA Section 3544 Agency program requirements (7):** Procedures for detecting via real-time analysis, active blocking, reporting within the agency as well as across infrastructures and agencies, and responding to security incidents as actionable threats, consistent with standards and guidelines issued pursuant to section 3546(b), including—(A) Mitigating risks associated with such incidents before substantial damage is done by blocking advanced malware and creating new blocking rules in real-time with continuous monitoring. For example, the automated data streams that are fed to the DHS through its cyberscope reporting system can be improved upon by systems available today that employ actionable detection and real-time blocking technologies that prevent zero-days and APTs; D) Directing a concerted shift from static compliance to real-time awareness of the threat landscape via continuous cyber monitoring, active analysis and threat agnostics, and real-time blocking of APTs and zero-day attacks. For example, real-time blocking is essential risk remediation and is now widely available, but there are also analysis tools available that can more rapidly assess the threats posed by zero-days and APTs to track them back to their source command and control centers.
5. **SANS Quick Win Definition:** fundamental aspects of information security to help an organization rapidly improve its security stance without major procedural, architectural, or technical changes to its environment.
6. **SANS Advanced Sub-Control Definition:** uses new technologies that provide maximum security but are harder to deploy or more expensive than commoditized security solutions.
7. **SANS Visibility/Attribution Measure Definition:** to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.