COMPLIANCE SOLUTIONS BASED ON FISMA AND SANS CRITICAL SECURITY CONTROLS

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

FISMA 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 and NIST

FISMA directs the National Institute of Standards and Technologies (NIST) to create and manage the technical standards in each of those 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 controls to the IT operations of a large organization and then implementing and managing them is a complex process.

FISMA and the SANS Institute

To help address the FISMA challenge, current and past federal chief information officers (CIOs) and chief information security officers (CISOs) worked with the SANS Institute to create the Consensus Audit Guidelines (CAG).

CAG includes 20 critical controls for effective cyber defense. Following those recommendations can enable federal agencies and private organizations to block both known high-priority attacks and new, emerging attacks.

Federal agencies and private organizations need a new approach to develop situational awareness as advanced threats become more prevalent.

FireEye

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 aims to:

- 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 provide guidelines for establishing continuous, automated monitoring of the riskiest portions of information technology infrastructures. They also present a prioritized, risk-based approach to security based on actual threats

Continuous Monitoring to Combat 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 the risk-management process is information security continuous monitoring (ISCM), which NIST defines as:

> 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 improve cyber security posture and overall situational awareness, it provides guidelines to replace periodic-assessment approaches with continuous monitoring approaches. FISMA section 3541 and 3544 (see Endnotes) outline the purpose and agency requirements for continuous monitoring approaches. They outline the complexity of the threat landscape, the importance of real-time threat detection, rapid remediation and detailed analysis to understand and eliminate advanced persistent threats and zero-day attacks. They also explain how cyber security measures can be more effective, given the scale, scope and complexity of federal information systems.

Fulfilling NIST and SANS Controls with FireEye Solutions

Traditional signature-based products are ineffective against today's advanced malware. These threats, launched by hostile nation-states and organized crime, 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 in their enterprise.

To help federal agencies and private organizations resolve this challenge in accordance with the NIST and SANS controls, FireEye provides integrated solutions for detecting advanced malware when it first appears on the network. Security-conscious organizations can deploy FireEye solutions to complement traditional signature-based products.

Taking this approach helps detect, contain, and block advanced malware that traditional defenses miss. It also addresses many of the compliance controls outlined in the NIST 800-53 Revision 4 (Table 1) and SANS Critical Controls Revision 4.1 (Table 2) manuals.

TABLE 1. FIREEYE SOLUTIONS THAT MEET NIST COMPLIANCE CONTROLS FOR DETECTING AND RESPONDING TO ADVANCED MALWARE.

NIST COMPLIANCE CONTROL	FIREEYE SOLUTION
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.	**The FireEye Multi-Vector Virtual Execution™ Engine** This patented technology at the heart of all FireEye® web, email, endpoint, file and mobile solutions detonates suspicious files and web objects within virtual machines purpose-built for security. It goes far beyond the capabilities of a typical sandbox. The FireEye Multi-Vector Virtual Execution™ (MVX) engine detects threats traditional signature-based products (next-generation firewalls, IPS, antivirus software and gateways) miss, and blocks those threats to prevent lateral movement. 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 and accelerates response time.
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 MVX Engine** Because the MVX engine is positioned as an inline defense that isolates and analyzes all objects that pass through it with near-real time results, it automatically behaves as a honeyclient. The MVX engine is built around a hardened hypervisor that supports numerous parallel execution environments or virtual machines with built-in countermeasures against malware. It generates no additional traffic to detect 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 Central Management, Malware Analysis, Dynamic Threat Intelligence and the MVX Engine** All FireEye detection and response solutions are fully integrated through underlying technologies. Its network, email, endpoint, file and mobile security solutions all share the same MVX engine to detect, identify and protect against sophisticated threats. If a threat is detected along one vector at one location, the entire MVX engine user base is updated with via Dynamic Threat Intelligence (DTI) to protect all other systems and vectors from similar threats. Threat intelligence can be further advanced by putting suspect objects into the secure environment of Malware Analysis thoroughly detail the attack lifecycle. Central Management provides a single console to manage configurations and helps correlate activity across FireEye deployments to reveal multi-stage, multi-vector attack patterns. It also speeds reporting and audit preparation. For more information see: • FireEye Central Management • Malware Analysis • DTI
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. 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.	**FireEye Incident Response Services and DTI** Incident Response (IR) teams, available on retainer, have over 100,000 hours of front line experience emphasize detection speed and threat analysis as a way to help quickly reconfigure your information system components to better protect your organization against threats. FireEye DTI facilitates the efforts of IR teams by providing critical information that helps detect and stop multi-vector attacks that exploit zero-day vulnerabilities. With fully integrated endpoint, web gateway and data security tools, FireEye can quickly confirm incidents and the extent of malware infiltration and quarantine the endpoint or host to limit lateral damage. For more information see: • IR Services • DTI

TABLE 1 CONTINUED

NIST COMPLIANCE CONTROL	FIREEYE SOLUTION
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.	**FireEye IR Services, Network and Endpoint Forensics and Investigation Analysis** When FireEye Network Forensics and Investigation Analysis systems are deployed in conjunction with other MVX engine-powered products, they give Incident response teams the ability to gather complete cyber forensic details of attacks in real time. These solutions capture all traffic and identify the exploit point of web, email, endpoint and file threat vectors to derive complete details of blended attacks through continuous monitoring, packet capture and heuristics. This solution helps detect many advanced threats, including: • Email-based spear-phishing attempts • Browser-based threats across FTP, HTTP, IRC and other protocols • Endpoint-based threats that use heavily researched and closely guarded exploits • File-based threats that use USB drives, mobile devices or remote downloads from a cloud service For more information see: • Incident Response Services • Network Forensics and Investigation Analysis • Endpoint Forensics
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	**FireEye Threat Analytics Platform (TAP), Advanced Threat Intelligence (ATI) and Endpoint Security** FireEye Threat Analytics Platform (TAP) reports all validated suspect incidents and aids attribution as part of a security ecosystem. TAP also integrates with security information and event management (SIEM) tools. This allows IR teams to see and validate patterns across multiple systems to uncover obscured malware, add context from Advanced Threat Intelligence (ATI) and other security systems to FireEye data, then automate reporting and response tracking as part of an active defense. 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. Endpoint Security adds complete visibility and investigative capabilities into every endpoint, enabling the discovery and containment of known IOCs and unknown threats. It can also conduct wide and deep searches of the current and historic state of each endpoint to uncover any current or past evidence of a threat. For more information see: • TAP • ATI • Endpoint Security

TABLE 2. FIREEYE SOLUTIONS THAT MEET SECURITY CONTROLS ESTABLISHED BY SANS 20.

SANS 20 CRITICAL SECURITY CONTROL	FIREEYE SOLUTION
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.	**FireEye MVX Engine and Endpoint Security** SANS quick win and configuration guidelines to address this control include the 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 portfolio exceeds this requirement by detecting zero-day vulnerabilities. The FireEye MVX engine detects both known and unknown vulnerabilities in applications and operating systems. Endpoint Security includes the Exploit Guard feature that detects if a threat actor is targeting vulnerability in a common application. ExploitGuard uses behavioral analysis to determine if an exploit attack cycle is in process by looking at overall process activities and how they relate to an exploit attempt. When enough evidence is assembled it notifies an administrator of exploit actions. 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 lifecycle, 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 attack lifecycle 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. These are 11 of the 12 recently discovered zero-day attacks identified by FireEye: **Date** — **CVE ID** — **App** Aug 2012 — CVE-2012-4681 — Java Dec 2012 — CVE-2012-4792 — IE Jan 2013 — CVE-2013-0422 — Java Feb 2013 — CVE-2013-0634 — Flash Feb 2013 — CVE-2013-0640 — PDF CVE-2013-0641 Feb 2013 — CVE-2013-1493 — Java May 2013 — CVE-2013-1347 — IE June 2013 — CVE-2013-1331 — Office Sept 2013 — CVE-2013-3893 — IE Nov 2013 — CVE-2013-3906 — Office Nov 2013 — CVE-2013-3918 — IE For more information see: • Endpoint Security
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.	**FireEye Email Security** FireEye Email Security and Email Threat Prevention Cloud (ETP) are inline defenses that detect and stop email-based cyber attacks, including those that use spear phishing to evade signature- based and reputation-based defenses. Spear phishing is a highly targeted attack that leverages user-specific information on social networks and other Internet resources. With the addition of FireEye Network Security you can gain a complete picture of the advanced multi-vector and multi-stage threats beyond the spear-phishing attack. FireEye Email Security and ETP also analyze all email for malicious URLs and attachments to protect against zero-day and APT attacks. This solution complements existing email spam gateways. For more information see: • Email Security and ETP

TABLE 2 CONTINUED

SANS 20 CRITICAL SECURITY CONTROL	FIREEYE SOLUTION
Control 5 — Malware Defenses **Quick Win5 #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.	**The FireEye MVX Engine** This patented technology at the heart of all FireEye web, email, endpoint, file and mobile solutions detonates suspicious files and web objects within virtual machines purpose-built for security. It goes far beyond the capabilities of a typical sandbox. The FireEye MVX engine detects threats traditional signature-based products (next-generation firewalls, IPS, antivirus software and gateways) miss, and blocks those threats to prevent lateral movement. 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 and accelerates response time.
Control 5 — Advanced Malware Defenses **Visibility/Attribution Measure7 #10:** Ensure automated monitoring tools use behavior-based anomaly detection to complement and enhance traditional signature- based detection.	**The FireEye MVX Engine and DTI** This patented technology at the heart of all FireEye web, email, endpoint, file and mobile solutions detonates suspicious files and web objects within virtual machines purpose-built for security. It goes far beyond the capabilities of a typical sandbox. The FireEye MVX engine detects threats traditional signature-based products (next-generation firewalls, IPS, antivirus software and gateways) miss, and blocks those threats to prevent lateral movement. 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 and accelerates response time. As the MVX engine detects and analyzes threats, its findings are validated and added to DTI, which automatically updates all other MVX engine-powered products every 60 minutes for the fastest and most current threat detection capability. . For more information see: • DTI
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	**FireEye Endpoint Security and the MVX Engine** FireEye Endpoint Security is based on the same MVX engine used by all FireEye solutions. 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. Endpoint Security includes the Exploit Guard feature that detects if a threat actor is targeting vulnerability in a common application. ExploitGuard uses behavioral analysis to determine if an exploit attack cycle is in process by looking at overall process activities and how they relate to an exploit attempt. When enough evidence is assembled it notifies an administrator of exploit actions. For more information see: • Endpoint Security

TABLE 2 CONTINUED

SANS 20 CRITICAL SECURITY CONTROL	FIREEYE SOLUTION
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.	**FireEye Central Management, DTI, Endpoint Security, TAP and Incident Response Services** The FireEye Central Management series consolidates management, reporting, and data sharing for FireEye solutions. FireEye TAP contributes reports on all validated suspect incidents and aids attribution as part of a security ecosystem. TAP also integrates with security information and event management (SIEM) tools. This allows IR teams to see and validate patterns across multiple systems to uncover obscured malware, add context from ATI and other security systems to FireEye data, then automate reporting and response tracking as part of an active defense. 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. Endpoint Security adds the ability to discover and contain and further analyze the impact of known IOCs and unknown threats. Even if IOCs are not discovered, it can conduct wide and deep searches of the current and historic state of each endpoint to uncover any current or past evidence of a threat. Incident response teams can quickly analyze Central Management information on unknown malware to generate new signatures. The FireEye DTI cloud, a real-time, global intelligence exchange, efficiently shares anonymized, standards-based threat intelligence metadata to all FireEye solutions to stop cyber attacks. For more information see: • Central Management • DTI • Endpoint Security • TAP • Incident Response Services
Control 5 — Malware Defenses: **Advanced Sub-Control6 #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 FireEye MVX Engine** This patented technology at the heart of all FireEye web, email, endpoint, file and mobile solutions detonates suspicious files and web objects within virtual machines purpose-built for security. It goes far beyond the capabilities of a typical sandbox. The FireEye MVX engine detects threats traditional signature-based products (next-generation firewalls, IPS, antivirus software and gateways) miss and blocks those threats to prevent lateral movement. The MVX engine conducts deep packet inspection to identify systems under attack (and any previously infected machines) with pinpoint accuracy that virtually eliminates the problem of false positives and accelerates response time. 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. The FireEye MVX engine examines the entire malware lifecycle. Multi-vector, multi-flow analysis correlates activity in both inbound and outbound traffic in real time to identify and report on: • Exploits • Malware executables • Cross-matrix of OS and apps • Originating URLs • Subsequent URLs • OS modifications • CnC protocol descriptors

TABLE 2 CONTINUED

SANS 20 CRITICAL SECURITY CONTROL	FIREEYE SOLUTION
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.	**FireEye Network Security and Endpoint Security** 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 can only protect against known or previously reported threats. FireEye is a leading provider of 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 inline at the network boundary, FireEye isolates and blocks attacks at the exploit phase. FireEye Network Security solutions include turnkey appliances that can be deployed at Internet egress points to block inbound exploits and outbound multi-protocol callbacks. They can readily integrate with other existing boundary defense technologies — including endpoint, data, and Web gateway security products — to confirm the exact location and criticality of the malware infiltration. For example, if an analyst detects a threat with Endpoint Security, they can contain one or more endpoints to restrict lateral movement of the attack while they investigate further. For more information, see: • Network Security • Endpoint Security
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.	**FireEye File Content Security and the MVX Engine** FireEye File Content Security stops cyber attacks by detecting and eliminating advanced malware residing on file shares that contain sensitive information. Traditional data loss protection products focus on unintentional data disclosures or insider threats. File Content Security is deployed inline to block outbound callbacks and prevent data exfiltration. The MVX engine that powers File Content Security and other FireEye solutions performs signature-less, stateful attack analysis within sophisticated virtual machines. It detects and blocks callbacks and communications on various protocols to CnC servers, which allow remote control of the malware exfiltrating data. Early and preemptive detection — before the callback phase — enables agencies to stop malware from spreading laterally or compromising sensitive systems and user accounts. For more information, see: • File Content Security
Control 17 — Data Loss Prevention **Advanced Sub-Control #8:** Block access to known file transfer and email exfiltration websites.	**FireEye MVX Engine-based Solutions, including Network Security, Email Security and ETP, File Content and Endpoint Security** FireEye provides a powerful multi-vector solution that can effectively detect, analyze, and protect against unknown malware and targeted APT attacks. Web, email, file, and blended attack vectors are protected with their respective combination of FireEye solutions. FireEye solutions also provide 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. File Content Security and Email Security correlate information with Network Security to prevent exfiltration. For more information, see: • Network Security • Email Security and ETP • File Content Security • Endpoint Security

TABLE 2 CONTINUED

SANS 20 CRITICAL SECURITY CONTROL	FIREEYE SOLUTION
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. 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.	**FireEye as a Service, Incident Response Services and Other Assessment and Planning Services** FireEye as a Service, as well as an array of additional services, feature a global team of incident and forensics consultants who assist with breach response in case of a malware incident and to help organizations establish organizational and process best practices. These consultants include some of the industry's top cyber analysts. They 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. For more information, see: • FireEye as a Service • Incident Response Services • Other FireEye Services

Transforming Cyber Operations from Reactive Remediation to Proactive Intelligence

Legacy security products, signature-based solutions and file-based sandbox analysis fail to detect and stop advanced malware. Federal agencies and private organizations need a new approach to develop situational awareness as advanced threats become more prevalent. 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. They offer:

- Detection speed within minutes to minimize time to block and remediate threats
- Identification at the critical exploit phase
- Discovery at all subsequent phases of malware attacks — exploit, download, callback and data exfiltration
- Visibility into the lateral movement of malware
- Real-time intelligence and cyber forensics across the entire attack lifecycle
- 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 solutions can also quickly discover more advanced malware and more kinds of malware. They can then transform their cyber operations focus from reactive remediation to proactive intelligence, generating advanced visibility to stop threats.

With FireEye solutions, security teams can also use automated data streams by employing actionable detection and real-time blocking technologies that prevent zero-day and APT attacks. Ultimately, federal government agencies and private organizations will be able 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 FireEye can help your organization protect your networks, data, and intellectual property and fulfill the NIST and SANS control recommendations, please visit **www.fireeye.com**.

Endnotes: FISMA and SANS Excerpts

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 cyber scope 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.

For more information visit our **Government solution** web page.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
(703) 935 1701 | 800.647.7020 | info@fireeye.com

www.FireEye.com

FireEye