

# MITIGATING CYBERSECURITY ATTACKS USING JUNIPER NETWORKS SECURITY SOLUTIONS

---

Preparing Government Agencies to Comply with the Consensus Audit  
Guidelines (CAGs)

## Table of Contents

|  |    |
|--|----|
| <b>Executive Summary</b> .....   | 4  |
| <b>Introduction</b> .....  | 4  |
| Scope .....  | 5  |
| Intended Audience .....  | 6  |
| <b>Governmental Challenges Associated with Cybersecurity</b> .....                                       | 6  |
| <b>Juniper Networks Network Security Guidelines</b> .....  | 6  |
| Insider Threat Protection .....  | 7  |
| Perimeter Protection .....   | 7  |
| Remote Access Protection .....   | 7  |
| Network and Security Management .....  | 8  |
| Network Monitoring and Incident Response .....   | 8  |
| <b>Consensus Audit Guidelines</b> .....  | 8  |
| Meeting CAG Guidelines with Juniper Networks Adaptive Threat Management Solutions .....                  | 9  |
| Critical Control 1: Inventory of Authorized and Unauthorized Hardware .....                              | 9  |
| Critical Control 2: Inventory of Authorized and Unauthorized Software .....                              | 9  |
| Critical Control 3: Secure Configurations for Hardware and Software .....                                | 9  |
| Critical Control 4: Secure Configurations of Network Devices such as Firewalls and Routers .....         | 10 |
| Critical Control 5: Boundary Defense .....   | 11 |
| Critical Control 6: Maintenance and Analysis of Complete Security Audit Logs .....                       | 11 |
| Critical Control 7: Application Software Security .....  | 12 |
| Critical Control 8: Controlled Use of Administrative Privileges .....                                    | 12 |
| Critical Control 9: Controlled Access Based On Need to Know .....  | 12 |
| Critical Control 10: Continuous Vulnerability Testing and Remediation .....                              | 13 |
| Critical Control 11: Dormant Account Monitoring and Control .....  | 13 |
| Critical Control 12: Anti-Malware Defenses .....   | 13 |
| Critical Control 13: Limitation and Control of Ports, Protocols, and Services .....                      | 14 |
| Critical Control 14: Wireless Device Control .....   | 14 |
| Critical Control 15: Data Leakage Protection Additional Critical Controls .....                          | 15 |
| Critical Control 16: Secure Network Engineering .....  | 15 |
| Critical Control 18: Incident Response Capability .....  | 15 |
| Critical Control 19: Data Recovery Capability .....  | 16 |
| <b>Juniper Networks Adaptive Threat Management Solutions</b> .....                                       | 18 |
| Solving Agency Challenges with Adaptive Threat Management Strategies .....                               | 19 |
| <b>Reducing Total Cost of Ownership with Juniper Networks Adaptive Threat Management Solutions</b> ..... | 20 |
| Certification Programs .....   | 20 |
| Comprehensive Product Brand Integrity Management .....   | 21 |
| Security Certifications .....  | 21 |
| <b>Conclusion</b> .....  | 21 |
| <b>About Juniper Networks</b> .....  | 22 |

## List of Figures

Figure 1: Juniper Networks solution for addressing CAGs ..... 5  
Figure 2: Juniper Networks Adaptive Threat Management Solutions ..... 19

## List of Tables

Table 1: Juniper Networks Adaptive Threat Management Solutions—Capabilities Satisfying CAG Guidelines ..... 17  
Table 2: Solution Components ..... 18  
Table 3: Solving Agency Challenges via Juniper Networks Adaptive Threat Management Solutions ..... 19

## Executive Summary

Cybersecurity threats are ever increasing and becoming more and more sophisticated, as professional hackers not only strive to compromise federal networks directly but also attack non-compliant mobile government employees' and contractors' devices that have access to critical infrastructure.

Most agencies' security infrastructure is a patchwork of disparate point products designed to mitigate certain types of security risks. Although point products may be effective in mitigating traditional and localized network attacks, they do not easily adapt to countering modern threats. This is because each device operates in an isolated manner, only detecting a specific type of security violation in a specific part of the network. Ideally, we would want security solutions to share all kinds of risk information from all network locations in order to gain the necessary network-wide visibility required to mitigate the most sophisticated network attacks.

In addition to these point devices not being able to communicate with each other, they are expensive to manage and maintain because they use many different operating systems and management platforms. To compound the challenge further, it is becoming more important to maintain tight endpoint compliance to reduce the risk of hackers who piggyback on mobile workers' devices in order to instigate an internal attack.

To prepare for the next generation of cybersecurity threats, the United States government has formed a group of federal agencies and private organizations to draft a set of rules to protect federal and contractor information systems. This set of rules, or controls, are known as the Consensus Audit Guidelines (CAGs).

The objective of this paper is to show how agencies can use Juniper Networks® Adaptive Threat Management Solutions to address these federal guidelines and overall enhance the federal government's security infrastructure. These solutions help enable a comprehensive, cooperative, standards-based, dynamically secure network that delivers granular policy-based access control, endpoint compliance, single pane provisioning, and network-wide visibility and reporting.

## Introduction

According to Zero Day, in July of 2008, the Russian military used distributed denial of service (DDoS) attacks and other network compromising capabilities as part of an offensive against Georgia, taking down not just Georgian President Mikhail Saakashvili's website but Georgia's entire infrastructure as well. These techniques for probing weaknesses in the Internet and global networks are growing more sophisticated every year, with some even receiving considerable funding. And external attacks aren't the only major concern; internal threats and attacks pose just as much of a problem. The current commander of U.S. Strategic Command (USSSTRATCOM), Air Force General Kevin Chilton, cautioned Congress in March of 2009 that the United States is vulnerable to cyber attacks "across the spectrum" and that additional efforts need to be put in place to thwart potential attacks which could "potentially threaten not only our military networks but also our critical national networks."

According to a recent article published in *Ars Technica: The Art of Technology* titled, "All eyes on cybersecurity at midpoint of federal review," the Institute for Information Infrastructure Protection (I3P), a consortium of leading universities, national laboratories, and nonprofit institutions (dedicated to strengthening the cyber infrastructure of the United States), recently sent a report to Congress noting that 85% of the nation's critical infrastructure is privately owned and operated. That report highlighted the security problems generated by the process control systems that regulate essential flows of oil, gas, and electricity. Unfortunately, these utilities are supported by an infrastructure that primarily consists of an accumulated patchwork of legacy devices that are laborious to secure and manage because they must operate 24/7 and cannot afford the performance hit that traditionally results from deploying additional legacy security solutions.

Therefore, since the federal government's existing infrastructure comprises a patchwork of legacy security devices that are not compatible, nor easily manageable, only some attacks and threats get mitigated, while many do not. Carl Staton, deputy CIO at the Energy Department states, "The current system allows for some security, but until it is integrated into all components of the network, it will be a challenge to keep up with and ahead of the bad guys."

In addition, responding to a compromised government computer system costs enormous amounts of money. In one recent hacking attack, successfully accomplished by a veteran IT employee, the cost to retrieve more than 10,000 user accounts from health departments, hospitals, prisons, and Supreme Court servers took five days, required 130 security experts, and cost more than \$1.25 million to correct the breach. This cost doesn't even consider the risk to 10,000 users of having their private data stolen.

Major motivation for the recently drafted CAGs comes down to standardizing priority security efforts and simplifying the existing National Institute of Standards and Technology (NIST) guidelines that currently consist of thousands of pages and, according to IT managers, are quite difficult to implement and even more difficult to audit. Former Air Force and Energy Department CIO John Gilligan, who led the project, called it a “no brainer.” “We are in cyberwar. The federal government is being targeted. Our ability to defend against attacks is quite weak. We’re bleeding badly and need to focus on keeping the patient alive. If you know that attacks are being carried out, you have a responsibility to prioritize your security investments to stop those attacks,” Gilligan said.

Juniper Networks, with its comprehensive, adaptable, and integrated open standards security solutions, addresses these CAGs. As a proven leader in network security, Juniper can meet these requirements by offering a solution that enhances the government’s existing infrastructure, provides granular access control, and meets compliance and regulatory requirements. Juniper Networks Adaptive Threat Management Solutions provide insider threat protection, remote access protection, and perimeter protection with a comprehensive and consolidated provisioning, monitoring, and reporting system.

By examining this paper, federal and local agencies will discover how this solution satisfies the government’s CAGs while reducing on-going operational costs, simplifying security operations, and raising the security posture of the entire network and its users. Capital costs are minimized by leveraging existing infrastructure, consolidating management, advancing open standards, and integrating security and networking capabilities.

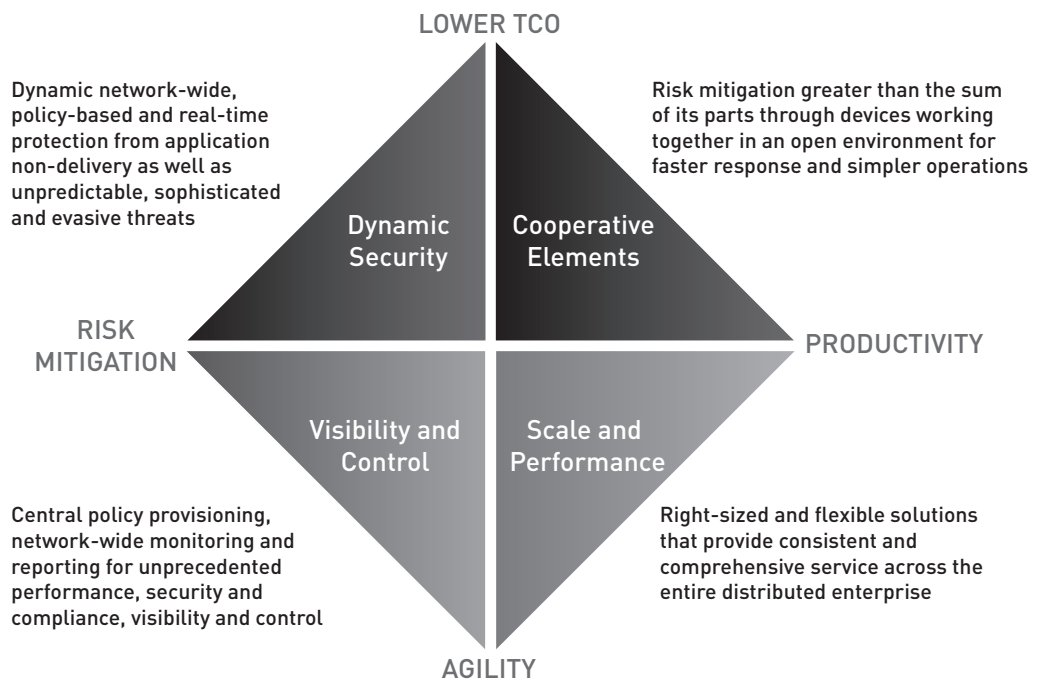


Figure 1: Juniper Networks solution for addressing CAGs

## Scope

This paper explains how Juniper Networks Adaptive Threat Management Solutions address the federal government’s CAGs for enhancing and providing cybersecurity against all forms of threats and attacks, both internal and external. By addressing these guidelines, we also list the advantages and cost savings that can be achieved by implementing Juniper Networks Adaptive Threat Management Solutions.

## Intended Audience

- Information technology specialists
- Deputy directors of security
- Deputy directors, Chief Intelligence Officers (CIOs)
- Network operations managers
- Chief engineers
- Enterprise network architects
- Chief information security officers
- Chief Technology Officers (CTOs)
- Security engineers

## Governmental Challenges Associated with Cybersecurity

Although various types of security devices and applications are being integrated into government network infrastructures, many departments and organizations are still struggling with a mixture/patchwork of security solutions that may or may not be compatible with each other. Many of these security solutions cannot adapt and scale to meet a constantly changing security landscape. Gaps between disparate devices can leave the network more vulnerable and hamper network-wide visibility and control. Also, in many cases IT managers are required to deploy and manage additional devices in order to provide network-wide visibility, adding to network complexity and costs.

Because the network has become such a critical asset with zero unplanned downtime as the goal, real-time communication and instant deployment of needed resources are essential requirements for government organizations that deal with critical situations on a daily basis. The challenge is how to meet this goal, while also enhancing the network in the areas of security, scalability, performance, usability, and manageability.

From a cybersecurity perspective, existing solutions lack the ability to adapt and respond proactively in real time to constantly evolving cyber threats such as hacking, scanning, denial of service (DoS) attacks, worms, and viruses. These become serious issues, especially when organizations must deal with national or local security matters, sensitive patient records, or defense-related research information. In addition, the lack of tight integration between security products such as firewalls, VPNs, Web filtering, and antivirus software, as well as the proliferation of remote offices, large campus locations, and data centers pose a serious challenge to security and IT personnel.

Government security and IT administrators are also faced with the challenge of making sure that the products they deploy scale to support ever increasing network traffic while maintaining fast, reliable, and secure access to applications and network resources. Performance and scalability are other considerations, especially when services must be provided under heavy traffic loads such as those that occur during a natural disaster, across a battlefield environment, or during college/university registration.

Because existing solutions consist of a mix of products and technologies that are not tightly integrated, administrators must also understand and manage multiple security products and management systems. Working with disparate systems poses a particular challenge when trying to identify the root cause of an attack by reviewing reports and logs from multiple systems and hundreds of devices spread over many diverse locations. The time required to manage and analyze such an environment leaves the network exposed to threats that take advantage of a vulnerable situation.

## Juniper Networks Network Security Guidelines

Below are five major components needed to provide comprehensive network security and threat management.

- Insider threat protection
- Perimeter protection
- Remote access protection
- Network security management
- Network monitoring and incident response

## Insider Threat Protection

Critical information is accessible within internal networks for business productivity purposes, and it is essential to protect this information. Insider attacks can come from various sources such as disgruntled employees, a contractor, guests connecting to the network, malware (virus/trojan) on an employee's mobile device, or a hacker gaining access to a device on the internal network. An organization's network security infrastructure plays an important role in preventing such attacks.

The network security infrastructure should integrate with inventory management systems and application authentication systems (RADIUS, directory services, public key infrastructure, etc.) and provide differentiated, role-based access for the following criteria:

- Authorized/unauthorized device
- Managed/unmanaged device
- Security compliance state of the device (antivirus, antispyware, personal firewall, hardened OS installations, etc.)
- Location of the device

To achieve differentiated, role-based access from internal networks, enterprises should segment their network. The logical control points should be defined to control access to critical data, as well as to contain any threat within the smallest segment of the network as possible. The network and security infrastructure (switches, routers, wireless access points, firewalls) should integrate with inventory management and authentication systems, as well as with network management and monitoring systems.

## Perimeter Protection

Perimeter protection is the first line of defense against any attack or threat to critical data and network resources. It is critical to deploy a multilayered defense at the perimeter to protect against attacks from cyberspace.

Perimeter defense should be applied to the Internet connection as well as to any extranet type of connections to other networks. The Internet, extranet, or internal WAN connections should be physically or logically separated, as each may require different levels of security protection. The WAN connections to other branch office locations should be encrypted. Perimeter defense should define a DMZ to separate the systems that are accessible to the outside world, and it should strictly control inbound as well as outbound services. Perimeter defense should include techniques to hide internal network information (with the use of Network Address Translation or proxy). All allowed traffic should go through additional inspection before it can reach internal systems.

Unified threat management (UTM) is considered a security services layer within the greater network architecture, and must be deployed at the perimeter for operational simplicity and scalability purposes. Perimeter defense should integrate with centralized monitoring and incident response systems, to provide traffic profiling information and visibility to any threat detected at the perimeter. It should integrate with the network and security management systems to enhance incident response capability. Data Leak Prevention (DLP) techniques should be deployed at the perimeter to protect proprietary and sensitive data transferred out of the network.

## Remote Access Protection

Increased mobility has helped improve agency productivity and response time. Remote access is a scenario where a user/device is outside the network, and hence must come through the perimeter. Because remote users have access to internal network resources behind the DMZ, remote access must be protected by techniques used for insider protection as well as perimeter protection.

Remote access should be controlled through a centralized authentication system, and access policy should be the same for remote users as it would be if they were accessing the network from their own onsite offices. Certainly their access rights should not be more relaxed when accessing the network remotely. In addition, access control techniques ensuring which inbound/outbound services are permitted should be deployed and combined with traffic inspection technologies. There should be the ability to form stricter incident response guidelines for remote access protection or to easily ensure consistency between insider and remote access guidelines. The communication from perimeter device to remote user device must be encrypted to protect authenticity, integrity, and data confidentiality.

Similar remote access protection requirements should be enabled between fixed remote sites like branch and campuses that are connected over wide, private networks (or VPNs).

## Network and Security Management

All network and security devices should be securely managed. Management control to the devices should be restricted to only authorized management platforms. There should be role-based access to allow users to only modify/view the configurations to which they require access. The management system should support appropriate change management and notification controls along with audit trails to ensure that only authorized changes are performed. For example, it may be useful to separate network and security management or policy management of the perimeter and data center to provide multilayer security. Network management systems may integrate with monitoring and incident response systems to quickly respond to any identified threat in the network.

## Network Monitoring and Incident Response

Network devices and servers produce a tremendous number of logs, and analyzing them manually to identify a threat is time-consuming and increases response times. Also, administrators may have to correlate logs from multiple locations and devices to identify blended and sophisticated threats. For these reasons, it is important to have a centralized log management and correlation system.

The centralized monitoring system should be able to receive logs from all network and security devices. It should have automated analysis and correlation to notify administrators when a threat is identified and provide sufficient information, such as priority of threat, type of threat, source of threat, and duration of the threat to reduce the incident response time. Depending on the requirements, security administrators also can provide separate monitoring for critical resources in offering an additional layer of security and separate functionality. The centralized monitoring system also should have reporting capabilities for long-term trends as well as network security status. Strong reporting capabilities can significantly streamline any audit process. Bottom line—known devices, known users, and known administrators are the key to network security.

## Consensus Audit Guidelines

Consensus Audit Guidelines (CAGs) are a set of rules for protecting federal and contractor information systems, originally established by a group of federal agencies and private organizations. The CAG effort began early in 2008 as a response to critical data lost by leading industries in the U.S. Defense Industrial Base (DIB). The team that put together the CAG initiative, which is part of a larger effort that resides at the Center for Strategic and International Studies (CSIS) in Washington, D.C., asked for key recommendations from the Commission on Cybersecurity for the 44th presidency. They consulted with a number of key government agencies to gather data on the latest attack patterns. As a result, these experts agreed on 20 guidelines (requirements/controls) that enterprises must take to mitigate not only known attacks, but future attacks as well. For each of the 20 controls, the experts identified specific (actual) attacks that the control stops or mitigates, highlighted best practices in automating the control (for 15 controls that can be automated), and defined tests that can determine whether each control is effectively implemented. The CAGs are expected to become the standard baseline for measuring computer security in organizations that are likely to be under attack.

The CAGs go through many testing stages, such as:

- Public review (by security professionals worldwide)
- Pilot implementation (within federal agencies)
- CIO Council review (by a security committee of the federal CIO)
- Inspector General review (by a team from the Federal Audit Executive Council)
- CAG Automation Tools Workshops (lessons learned by federal users and requirements documents for automation of each of the 15 controls)
- Global validation ((CAGs compared with the audit guides for ISO 2700x, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI), and Sarbanes-Oxley (SOX) compliance testing))

## Meeting CAG Guidelines with Juniper Networks Adaptive Threat Management Solutions

The following lists and defines the CAGs that can be satisfied with Juniper Networks Adaptive Threat Management Solutions.

### Critical Control 1: Inventory of Authorized and Unauthorized Hardware

Many attackers use automated systems that continuously scan address spaces of target organizations to uncover unprotected systems attaching to the target network, experimental/test systems that occasionally connect to the network, or systems making connections from remote locations. Attackers target these types of systems because they are often not properly secured or configured with the latest security patches and updates. By exploiting these weak link systems, attackers can gain access to the target network, and then go after additional systems where they can install backdoors for future exploitation.

Juniper Networks Adaptive Threat Management Solutions provide consistent and granular policy-based access control regardless of location (internal or remote). Juniper Networks Unified Access Control and Juniper Networks SA Series SSL VPN Appliances are components of Juniper Networks Adaptive Threat Management Solutions, and obtain user authentication, endpoint security state, and location data. They also define dynamic access control policies that are distributed to network enforcement points such as firewalls across the distributed network. For example, during a typical user attempt to connect a new system to the network, the centralized policy manager can be configured to check the system's antivirus and patch files, enabling automatic patch remediation if required, before actually allowing full network connectivity.

### Critical Control 2: Inventory of Authorized and Unauthorized Software

Computer attackers often use systems that scan target networks for vulnerable versions of software that can be remotely exploited. These attackers frequently focus on zero-day exploits where there is a known, published vulnerability for which no patch has yet been released by the software vendor. Again, once attackers penetrate one system, they use that system as a launching point to collect additional information and expand their attacks within the organization.

Similar to the solution discussed in Critical Control 1, Juniper Networks Adaptive Threat Management Solutions, UAC, and SA Series solutions provide consistent and granular policy-based access control for all systems both locally and remotely. User systems, attempting to connect to the organization's network, can be scanned for a variety of security applications and states, including antivirus, anti-malware, personal firewalls, and patches, and they can be automatically updated as required prior to obtaining full access to the network. In addition, Juniper Networks Adaptive Threat Management Solutions can automatically check an endpoint device for application or operating system patch updates and enable automatic patch remediation, if needed. For example, if a user attempts to connect remotely to the organization's network and that user's operating system is not running the latest set of patches, the centralized policy manager can either hold off network access until the necessary patches are installed or disallow user access altogether.

### Critical Control 3: Secure Configurations for Hardware and Software

Another key method of attack is to search target networks for systems that are still running factory-installed software, leaving them vulnerable to exploitation. These vulnerabilities are often due to the retaining of factory default settings for items such as username and password, or unnecessary services that can keep common communication ports open with medium security settings.

UAC and SA Series solutions help verify that endpoint devices meet organizational security policy requirements before granting access, remediating devices and quarantining users when necessary. Client computers can be checked both prior to and during a session to verify an acceptable device security posture that requires installed/running endpoint security applications (antivirus, firewall, etc). This solution also supports custom-built checks that include verifying ports opened/closed, checking files/processes and validating their authenticity with Message Digest 5 (MD5) hash checksums, verifying registry settings, machine certificates, and more.

For the above-mentioned controls, the following product capabilities are relevant and enable agencies to take inventory of all manageable and unmanageable network endpoints.

Juniper Networks Advanced Insight Solutions (AIS) maintain an inventory of all Juniper devices. For each device running Juniper Networks Junos® operating system, the scripts inventory and baseline system immediately detects issues, gathers and compiles relevant data, forms the correct problem definition, and reports details to the customer via SNMP traps or chassis alarms. AIS can be seen as a single repository and a go to place for the enterprise security team to analyze Juniper Networks hardware and software inventory.

Granting network access to non-compliant computers, even when they are being operated by authorized users, exposes critical infrastructure to an increased risk of vulnerability, and can even jeopardize regulatory compliance certification. In order to provide greater depth and granularity in network security, the authorization method itself must be multi-dimensional. Controls must be put in place to manage and authenticate not only the identity of the individual attempting to access network resources and applications, but also the security and health state of their endpoints.

#### **UAC/InsightIX Partnership for Unmanageable Devices**

The complex and dynamic nature of enterprise networks and the adoption of new IT technologies such as virtualization present enormous challenges for IT managers. Between 20% and 50% of today's devices reside on enterprise networks without an organization's knowledge! This severely undermines the security state of the network, as security measures can only be partially applied. Organizations cannot defend against or manage devices that they do not know about and cannot see. InsightIX's Business Security Assurance (BSA) product suite builds and maintains a real-time, complete, and accurate inventory of all devices on a UAC-enabled network.

The combination of InsightIX BSA and UAC creates a comprehensive network access control and authentication solution capable of operating with and against all devices attached to an enterprise network, regardless of whether or not they have user-based authentication. All devices are classified into different asset classes based on their usage.

#### **UAC/Shavlik/Microsoft Integration for Patch Management Policy Compliance for Managed Endpoints**

Juniper Networks Unified Access Control integrates with the world-class patch assessment engine of Shavlik NetChk. This integration aids in protecting and delivering the secure and scalable solution that companies need to ensure endpoint security and patch management policy compliance

The overall objective for these three controls is to ensure that only known administrators and users with known device endpoints are attaching to the network at any given time. UAC provides the shared database for security information via the Interface for Metadata Access Point (IF-MAP) protocol, which is an open standard for security and network coordination (published in May 2008 by the Trusted Computing Group). With IF-MAP, security information can be shared across a variety of security systems, to monitor who is connecting to the network, what device they are using, what is the state of each device, what is a device's expectation and behavior.

IF-MAP defines a powerful publish/subscribe/search protocol that enables a wide range of systems to share data in real time concerning network devices, policies, status, and behavior. For example, an intrusion prevention system (IPS) with a built-in IF-MAP client can publish an alert to an IF-MAP server indicating that a particular endpoint is sending anomalous traffic. A firewall that subscribes to information involving that endpoint will then receive a real-time update from the IF-MAP server, triggering an automatic response. This powerful integration of network and security components can strengthen the network beyond just admission control and assurance of endpoint integrity to continuous post-admission assessment and control.

#### **Critical Control 4: Secure Configurations of Network Devices such as Firewalls and Routers**

Often, during the normal course of implementing new services for business users, network devices are reconfigured with exceptions to allow these new services to function. For example, a new service application may require all users to start using a new browser-based interface rather than the older proprietary client. Attackers will often search for these electronic holes in network firewalls, routers, and switches to help them penetrate security defenses. Once attackers have taken control of a network device, they can intercept information passing through the device, or in some cases redirect traffic to another malicious system that is masquerading as a trusted system.

Juniper Networks Network and Security Manager (NSM) introduces a global template policy feature that allows security administrators to create one master security policy that can be applied to multiple devices. This feature allows security administrators to enforce mandatory corporate policies efficiently across all networks devices (routers, switches, security) and ensures uniform security across the enterprise. For example, new access policies are pushed to both UAC and SA Series SSL VPN Appliances for consistent policy and network entitlements, no matter where the user is located. Templates can enforce a common configuration per organizational policy and

minimize configuration errors. Templates are used to define a device configuration and then reuse that configuration information across multiple devices spread across the different enterprise locations. In a template, you must define only those configuration parameters that you want to set; you do not need to specify a complete device configuration. Centralized policy management also allows you to keep track of all changes made to security policies, with the ability to compare between versions and even roll back to previous working versions, if needed. Juniper Networks devices can also perform firmware integrity checks upon power on, and notify the administrator of any discrepancies. Some platforms require provisions to perform these self checks.

Juniper's network and security devices provide secure management options for restricting network management to only authorized network management systems (for example, Network and Security Manager). NSM supports role-based access to provide management granularity. NSM can also integrate with Common Access Card (CAC), Personal Identity Verification (PIV), and smart cards when agencies must meet strict security guidelines that mandate a two-factor authentication for workstations in federal agencies and business associate locations. It also provides audit trails for any management activity and facilitates change control. All of Juniper's network and security devices can be locked down and managed from a specific IP address or subnet, which serves as another layer of defense for preventing unauthorized administrative access to make configuration changes.

### **Critical Control 5: Boundary Defense**

Attackers will often target an organization's gateway system providing Internet connectivity to probe for security weaknesses. Once they have penetrated that gateway system, they will use it as a launching point to get inside the organization's boundary to steal or change information or to establish backdoors for future attacks. Some attackers will also attempt to infiltrate a business partner's network and then attack the target organization through an extranet partner connection, again exploiting extranet system vulnerabilities.

Juniper Networks Adaptive Threat Management Solutions' integrated firewall provides a comprehensive and layered defense environment that enforces strict security policies for all boundary gateway systems.

For agencies and enterprises that want to run externally-accessible services such as HTTP, email, FTP, and Domain Name System (DNS), we recommend that these publicly available services be physically or logically segmented from the internal network. Firewalls and the hardening of hosts and applications are effective ways to deter casual intruders. However, determined crackers can find ways into the internal network if the services they have cracked reside on the same network segment. Services that are externally accessible should reside on what the security industry regards as a demilitarized zone or DMZ, a logical network segment where inbound traffic from the Internet is only able to access those services and is not permitted to access the internal network. This is effective in that, even if a malicious user exploits a machine in the DMZ, the rest of the internal network lies behind a firewall on a separated segment. Juniper Networks firewalls are the core components when it comes to segmenting the corporate network and providing stateful firewall inspection.

### **Critical Control 6: Maintenance and Analysis of Complete Security Audit Logs**

The complexity and lack of proper procedures for performing in-depth and ongoing audits of security logs can hamper an organization's ability to respond quickly to an attacker's activities. Attackers often take advantage of these security logging deficiencies to provide a window of opportunity to infiltrate an organization's system and to place malicious software for future attacks. While many organizations keep audit records for compliance reasons, they fail to perform log analysis activities, thereby allowing attackers control of targeted systems for months at a time.

Juniper Networks STRM Series Security Threat Response Managers are an appliance-based security information and event management (SIEM) platform that provides situational awareness and compliance support to organizations that need to tighten security and improve policy monitoring with a modest investment in time and resources. The STRM Series goes beyond traditional network security products to create a command-and-control center that delivers:

- **Centralized command and control console:** Integrated log management, security information and event management (SIEM), and network behavior analysis in a single console reduces the cost of security management and improves IT efficiency. Integrated log management, SIEM, and network behavior analysis in a single console reduces the cost of security management and improves IT efficiency.
- **Network, security, application, and identity awareness:** The central management of network and security events, network and application flow data, vulnerability data, and identity information greatly improves the ability to meet IT security objectives.

- **Advanced threat and security incident detection:** The STRM Series unique offense management significantly reduces false positives and detects threats that other security solutions miss.
- **Compliance-driven reporting capabilities:** The STRM Series provides compliance-centric reporting that enables the delivery of IT best practices supporting compliance initiatives.
- **Scalable distributed log collection and archive:** The STRM Series distributed architecture scales to provide event and flow log management in any enterprise network. STRM Series devices can be easily deployed in large distributed environments and scale to large deployments as a business grows.

### **Critical Control 7: Application Software Security**

Another common attack scenario is for criminal organizations to focus on exploiting vulnerabilities in application software products that are in widespread use across an organization, such as antivirus tools, backup systems, or web-enabled applications that are off-the-shelf or custom-built. Once an attacker has infiltrated the application software of one system or a Web server, the attacker can then use that application as an infectious engine to infect hundreds or thousands of other systems running the same application.

To block malicious application-level attacks, Juniper seamlessly integrates IPS across all of its firewall products. The Juniper Networks ISG Series Integrated Security Gateways and Juniper Networks SRX Series Services Gateways tightly integrate the same software found on Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to provide unmatched application-level protection against worms, trojans, spyware, and malware. More than 60 protocols are supported, including those used by advanced applications such as VoIP and streaming media. With multiple attack detection mechanisms that include stateful signatures and protocol anomaly, ISG Series and SRX Series gateways perform in-depth analysis of application protocol, context, and state to deliver zero-day protection from application-level attacks.

### **Critical Control 8: Controlled Use of Administrative Privileges**

Attackers will commonly take a look at administrative privileges on target systems to see if they can take advantage of the many types of high-level administrative rights available to a user with this type of privilege. Some attackers use malicious application-level attacks like email attachments to take over a system and then install a variety of keystroke loggers, sniffers, and remote control software to help them with additional attacks. Other attackers break into a common system and take advantage of a loosely defined set of administrative privileges to elevate the privileges of the target system and gain control over large numbers of machines. An example of this would be gaining domain administration privileges in large Windows environments.

Juniper Networks Adaptive Threat Management Solutions include Network and Security Manager, which allows organizational IT departments to delegate appropriate levels of administrative access to specific users locally, or via RADIUS, for a wide range of tasks. Using role-based administration, organizations can provide or restrict system permissions to different individuals or constituencies within the organization based on skill set or responsibility. NSM also has a global policy feature which enables security administrators to create one master policy that can be applied to all regional management servers. This feature allows security administrators to enforce mandatory corporate policies efficiently across all devices in the network and to ensure uniform security across the organization. NSM role-based access controls can also integrate with CAC, PIV, and smart cards when agencies must meet strict security guidelines that mandate a two-factor authentication for workstations in federal agencies and their business associates' locations.

### **Critical Control 9: Controlled Access Based On Need to Know**

After an attacker has successfully penetrated a system within the targeted organization or department, access to sensitive information or files is solely based on what type of access control policies are in place. Unfortunately, in many places there are no access control policies. As a result, the attacker's job of finding and accessing sensitive information is much easier.

Juniper Networks Adaptive Threat Management Solutions provide a mechanism to control access based on a need to know approach. Virtualization technologies in Juniper's integrated firewall/VPN security solutions enable users to segment their network into many separate compartments, all controlled through a single appliance. Administrators can divide the network into distinct, secure segments with their own firewalls and separate security policies, thereby limiting security breach exposures. In addition, Unified Access Control combines the best of access control and security technologies while leveraging existing, deployed enterprise investments such as firewalls. UAC incorporates different levels of session-specific policy—including authentication/authorization, roles, and resource policies—to deliver extremely robust access control and security policies that are easy to deploy, maintain, and modify.

Finally, the identity-enabled profiler within UAC, which correlates user identity and role information to network and application usage, allows you to know when and exactly who is accessing your network and your sensitive applications, providing a log that is vitally important for regulatory compliance audits. The STRM Series can be used to detect privilege escalation attempts when all devices are configured to send logs to STRM Series appliances. All Juniper Networks devices support customizable login banners where organizations can enable customized Acceptable Use Policy (AUP) for the device that end users/administrators are attempting to access.

### **Critical Control 10: Continuous Vulnerability Testing and Remediation**

With the expanding number of applications being used within organizations, it is becoming quite difficult to keep up with patch releases for security vulnerabilities that are uncovered on a daily basis. The time delay needed for IT administrators to find or fix the application software with these vulnerabilities provides windows of opportunity for attackers to exploit these holes, take over target systems, and gain access to sensitive information.

For threat detection originating from remote users and remediation, Juniper Networks offers coordinated threat control functionality that enables SA Series SSL VPN Appliances and IDP Series Intrusion Detection and Prevention Appliances to correlate the user's identity (session) from the SSL VPN with the threat detection capabilities of the IDP Series.

For threat detection originating from trusted LAN users and remediation, Juniper Networks offers coordinated threat control functionality that enables Juniper Networks IC Series Unified Access Control Appliances and IDP Series Intrusion Detection and Prevention Appliances to correlate the user's identity (session) from UAC with the threat detection capabilities of the IDP Series. The remediation can be a decisive action such as quarantining the user, limiting user's role privileges, and blocking the user until an administrator takes action.

The STRM Series combines, analyzes, and manages an incomparable set of surveillance data—network behavior, security events, vulnerability profiles, and threat information—that empowers organizations to efficiently manage business operations on their networks from a single management console. Vulnerability assessment integration enables vulnerability assessment data to create profiles of attackers and targets. Vulnerability assessment data uses correlated event data, network activity, and behavioral changes to remove false positives to determine the threat level for each critical business asset.

The STRM Series' integration with vulnerability assessment tools allows you to schedule scans to keep your vulnerability assessment data up-to-date. STRM Series appliances integrate seamlessly with both commercial and open source vulnerability assessment tools such as IP360, Nessus, Nmap, Qualys, and Foundstone, to name a few.

### **Critical Control 11: Dormant Account Monitoring and Control**

Another favorite weak spot for attackers when probing an organization's systems is inactive user accounts—employees who no longer work for the company or outside contractors. These inactive accounts can be used by attackers or former employees to gain access to the organization's system and any sensitive data that resides on that system, depending on the level of privileges associated with that account.

Juniper Networks Adaptive Threat Management Solutions integrated firewalls provide advanced network segmentation through implementation of security zones, virtual LANs, and virtual routers, all of which allow administrators to deploy security policies to isolate accounts, guests, regional servers, or databases. This prevents unauthorized access, contains any attacks that may occur, and facilitates regulatory compliance.

In addition, Juniper Networks Adaptive Threat Management Solutions integrate with multiple common authentication systems (RADIUS, Active Directory, PKI, RSA SecurID, etc.), and once an account is disabled, the internal and remote network access for that account is blocked. This integration of user account network connection with strong authentication systems (CAC/PIV/smart card) provides an additional layer of security from dormant user account threats. The end user login activity information from all network devices can be correlated and viewed via STRM Series appliances. Customized alerts can be triggered when certain predefined unsuccessful login attempts have been exceeded.

### **Critical Control 12: Anti-Malware Defenses**

The explosion of viruses, worms, trojans, and other malicious software continues to grow across the Internet community. These various types of malware commonly transport themselves from place to place either as email attachments or downloads from a wide variety of common websites to unsuspecting victims. Once the malware is resident on the system, many types of malware have sophisticated mechanisms to actually turn off anti-malware applications, or to regenerate themselves when a system is rebooted during normal power-on activities.

Juniper Networks Adaptive Threat Management Solutions firewall functionality includes a complete set of unified threat management (UTM) security features such as stateful firewall, IPS, antivirus (Instant Message scanning, antispyware, anti-adware, and antiphishing), antispam, and Web filtering to stop worms, spyware, trojans, malware, and other emerging attacks.

For example, Juniper Networks Adaptive Threat Management Solutions' antivirus protection can actually scan for viruses embedded in both email and Web traffic by scrutinizing IMAP, Simple Mail Transfer Protocol (SMTP), FTP, POP3, IM, and HTTP protocols. In addition, Juniper Networks Adaptive Threat Management Solutions integration with UAC and the SA Series imposes a number of preconditions prior to allowing either a local or remote system a network connection. Prior to even allowing a login, Juniper Networks Adaptive Threat Management Solutions can check the requesting system's network and device settings, including scanning for malware such as keystroke loggers, and verifying the operation of endpoint security software such as antivirus applications and personal firewalls. If the system does not meet the preconditions, the end user is notified so that the system's security profile can be reconfigured and the option to download up-to-date security patches or releases can be provided, as needed.

### **Critical Control 13: Limitation and Control of Ports, Protocols, and Services**

In today's business environment, organizations use a wide variety of servers to help run many business applications across multiple departments. These servers may include Web servers, mail servers, DNS servers, and file/print servers. Unfortunately, many of the factory-installed software packages for these servers automatically install and activate services on end user systems, usually without the end user's knowledge. Attackers search for these common services and exploit known security holes.

Juniper firewalls include the ability to protect against network-level attacks using a dynamic packet filtering method known as stateful inspection. For administrators who want to run externally-accessible services such as HTTP, email, FTP, and DNS, we recommend that these publicly available services be physically segmented or logically segmented from the internal network, or both. Firewalls and the hardening of hosts and applications are effective ways to deter casual intruders. However, determined crackers can find ways into the internal network if the services they have cracked reside on the same network segment. Externally accessible services should reside on what the security industry regards as a demilitarized zone or DMZ, a logical network segment where inbound traffic from the Internet is only able to access those services and is not permitted to access the internal network. This is effective in that, even if a malicious user exploits a machine on the DMZ, the rest of the internal network lies behind a firewall on a separated segment. Juniper's firewalls are the core components when it comes to segmenting the corporate network.

By using centralized, policy-based management, organizations can create security policies that define the parameters of traffic that is permitted to pass from specified sources to specific destinations. Predefined port and protocol templates, as published in the DoD Security Technical Implementation Guidelines (STIGs), can be defined in NSM to be applied on multiple devices. Juniper Networks Odyssey Access Client, deployed on the endpoint, also consists of personal firewall functionality which can be leveraged to harden the endpoint to define allowed ports and protocols before the endpoint can attach to the enterprise network. The OAC agent can also be used to enforce protocols used only with Federal Information Processing Standards (FIPS)-approved algorithms at the endpoints.

### **Critical Control 14: Wireless Device Control**

The increasing use of wireless LAN environments and their associated wireless device connections to laptops, PDAs, and tables is placing a huge demand on IT departments to first know where all of their wireless locations are, and then understand what type of wireless devices are being used. Attackers can target an organization's wireless LAN environment and gain easy access through a security perimeter when the environment does not have the proper security policies in place, as an example, restricted access requiring a mobile user to log in. Attackers may also target wireless devices used for remote accessibility (hotels, cyber cafés, convention centers), by using software tools that infect the device, and then using that device as an entry point when the device reconnects to the organization's network.

The UAC solution combines the best of wireless access control and security technologies, while leveraging existing, deployed enterprise investments with any vendor's 802.1X-enabled wireless access points. UAC allows IT departments to easily create a unique access control policy for each user, or for groups of users depending on their identity, location, and device security state. Application access control includes any restrictions on network resources that a user or device is allowed to access and use. In addition, UAC controls network access for managed endpoint devices such as employee laptop and desktop computers, for unmanaged devices such as those used by guests and contractors; and for unmanageable endpoints such as printers and IP-based security cameras, environmental

system controls, bar code readers, and other computing and non-computing devices that are driven by and connected to the network. Odyssey Access Control, deployed on the endpoint, can also be leveraged to ensure that no weak encryption protocols are being used to access wireless access points.

### **Critical Control 15: Data Leakage Protection Additional Critical Controls**

There has been a lot of press recently detailing how attackers have penetrated network perimeters of both public and private organizations to steal large amounts of sensitive data such as personal customer information lists. In most of the profiled incidents, the loss of sensitive data was only realized by IT organizations after the loss had occurred, as they may not have had adequate access control policies in place and were not monitoring data outflows across network boundaries in real time.

Juniper Networks Adaptive Threat Management Solutions provide consistent and granular policy-based access control, regardless of a user's location when attempting to access the network. IDP Series appliances offer several signatures to detect and notify when sensitive information such as drivers' licenses, SSNs, or credit card information is leaving the network. The IDP Series allows customers to define custom signatures so that security engineers can identify and classify the most sensitive information in the enterprise, and write custom signatures to detect information leakage and take appropriate action. And SRX Series Services Gateways support basic DLP functionality combined with industry-leading UTM features.

Corporate espionage is often attributed to the fact that many organizations lack adequate enforcement of access control. The UAC and SA Series components of Juniper Networks Adaptive Threat Management Solutions obtain user authentication, endpoint security state, and location data, and they define dynamic access control policies for access to sensitive data that is distributed to network enforcement points such as firewalls across the distributed network. UAC also captures detailed logging of user roles, attempted access to resources, the state of compliance of the endpoint, and users' violation attempts of the security policy.

### **Critical Control 16: Secure Network Engineering**

Organizations can easily apply stand-alone security solutions to each of the environments discussed previously in this document. However, this may not provide the integrated, layered security architecture that is required to quickly and effectively handle threats both today and in the future. In addition, various products may require users to run a variety of management applications that might or might not enable a centralized view of what is happening across the network.

Juniper Networks Adaptive Threat Management Solutions deliver a consistent and comprehensive approach to security, while providing you the freedom to deploy a superior approach that is just right for your agency or department. Juniper Networks Adaptive Threat Management Solutions consist of best-in-class security products that cooperate with each other proactively and prevent attacks that evade security point products. These solutions enable the network to dynamically adapt to risks in the environment, and always with a full audit trail.

Juniper Networks Adaptive Threat Management Solutions support rapid response and shunning of detected attacks. The network architecture and the systems that comprise it are engineered for rapid deployment of new access control lists, rules, signatures, blocks, black holes and other defensive measures, as required by United States Computer Emergency Readiness Team (US-CERT).

### **Critical Control 18: Incident Response Capability**

Many organizations still have not put in place an effective incident response program to help deal with security incidents using a real-time approach. Such programs should include written procedures, clearly defined individuals with escalation responsibilities, and periodic testing.

Juniper understands the requirements for an effective incident response program and has defined how an incident response should conform to the following phases: (1) Identification, notification, and prioritization of incident; (2) Incident analysis and impact assessment; and (3) Definition and deployment of incident counter measures.

STRM Series solutions integrate logs from server, network, and security devices, and they provide automated analysis and correlation to quickly identify a threat. Once any threat is identified, the STRM Series device maps the details with the vulnerability state of the target, the business importance of the target, the spread of the attack, and provides notification to an administrator with the associated priority. The STRM Series also provides critical information for quick analysis of the incident, such as source of the threat, target of the threat, duration of the threat, etc., and helps administrators quickly define appropriate countermeasures.

### **Critical Control 19: Data Recovery Capability**

The procedure for implementation of control is once per quarter; a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

Juniper Networks WXC Series Application Acceleration Platforms accelerate data backup and recovery across the WAN. All Juniper Networks network and security infrastructure devices have device-level, high availability features built in, making the network more reliable and fault tolerant in the event of a device/link failure.

Table 1 lists and defines Juniper Networks Adaptive Threat Management Solutions portfolio and maps its major elements to the CAG guidelines. As outlined earlier in this white paper, Juniper Networks Adaptive Threat Management Solutions contain five major elements for providing security:

- Insider protection
- Perimeter protection
- Secure remote access
- Network management
- Visibility and control

Table 1 presents a traceability matrix for the mapping of controls into these five categories.

**Table 1: Juniper Networks Adaptive Threat Management Solutions—Capabilities Satisfying CAG Guidelines**

| Juniper Networks Adaptive Threat Management Solutions Portfolio                          | Insider Protection | Perimeter Protection | Secure Remote Access | Network Management | Visibility and Control |
|--|--------------------|----------------------|----------------------|--------------------|------------------------|
| CAG Guidelines   | Description        |                      |                      |                    |                        |
| 1. Inventory of authorized and unauthorized hardware                                     |                    | •                    | •                    | •                  | •                      |
| 2. Inventory of authorized and unauthorized software                                     | •                  |                      | •                    | •                  | •                      |
| 3. Secure configurations of hardware and software on laptops, work stations, and servers |                    |                      |                      |                    | •                      |
| 4. Secure configurations of network devices such as firewalls and routers                |                    |                      |                      |                    | •                      |
| 5. Boundary defense  |                    | •                    | •                    | •                  |                        |
| 6. Maintenance and analysis of complete security audit logs                              |                    |                      |                      | •                  | •                      |
| 7. Application software security   |                    |                      | •                    | •                  | •                      |
| 8. Controlled use of administrative privileges   | •                  |                      | •                    | •                  | •                      |
| 9. Controlled access based on need to know   | •                  | •                    | •                    | •                  | •                      |
| 10. Continuous vulnerability testing and remediation                                     | •                  |                      |                      | •                  | •                      |
| 11. Dormant account monitoring and control   | •                  | •                    | •                    | •                  | •                      |
| 12. Anti-malware defenses  | •                  | •                    | •                    | •                  | •                      |
| 13. Limitation and control of ports, protocols, and services                             | •                  | •                    | •                    | •                  | •                      |
| 14. Wireless device control  | •                  |                      |                      | •                  | •                      |
| 15. Data Leakage Protection (DLP) additional critical controls                           | •                  |                      |                      | •                  | •                      |
| 16. Secure network engineering   | •                  | •                    | •                    | •                  | •                      |
| 18. Incident response capability   |                    |                      |                      | •                  | •                      |

## Juniper Networks Adaptive Threat Management Solutions

Key benefits of Juniper Networks Adaptive Threat Management Solutions include the following:

- Comprehensive security that identifies, mitigates, and reports on even the most sophisticated attacks
- Reduced cost of ownership with lower capital expenditures (CapEx) and operational expenditures (OpEx) compared to disparate point products
- Improved response times while requiring fewer IT resources
- Eliminates the trade-off between security and performance
- Enhanced compliance via network-wide, real-time visibility
- Delivers network-wide and granular policy-based access control

**Table 2: Solution Components**

| Product  | Highlights  |
|--|---|
| A complete family of firewall/VPN solutions              | <ul style="list-style-type: none"> <li>• Suite of firewalls and integrated security products tailored for specific uses, including ISG Series Integrated Services Gateways and SSG Series Secure Services Gateways.</li> <li>• Tightly integrated set of UTM capabilities to protect against worms, viruses, trojans, spyware, DoS, and blended attacks.</li> </ul>   |
| SRX Series Services Gateways                             | <ul style="list-style-type: none"> <li>• These gateways provide firewall, IPS, VPN, and other network and security services. Based on Juniper's revolutionary Dynamic Services Architecture, SRX Series is a stable, scalable platform.</li> <li>• SRX Series Services Gateways are available in a variety of form factors, enabling you to buy what you need for each location, from the smallest branch office to the largest data center.</li> </ul> |
| IDP Series Intrusion Detection and Prevention Appliances | <ul style="list-style-type: none"> <li>• High-performance devices with up to 10 Gbps throughput.</li> <li>• Available as standalone devices or integrated functionality in select firewalls, including the ISG Series and SRX Series platforms.</li> </ul>  |
| End-to-end access control solutions                      | <ul style="list-style-type: none"> <li>• Market-leading SA Series SSL VPN Appliances for remote and granular access control at the group or individual level.</li> <li>• Unified Access Control for LAN users.</li> <li>• Federated identity management enables single sign-on (SSO) across both platforms.</li> </ul>  |
| Network and Security Manager                             | <ul style="list-style-type: none"> <li>• NSM enables centralized provisioning of Juniper Networks routing, switching, and security products.</li> </ul>   |
| STRM Series Security Threat Response Managers            | <ul style="list-style-type: none"> <li>• Single console for logging, compliance and reporting, event correlation across diverse data sources, application-level monitoring, network-based anomaly detection, for Juniper and other network and security vendors.</li> </ul>   |

Figure 2 illustrates how Juniper Networks Adaptive Threat Management Solutions identify, mitigate, and report a network attack in real time.

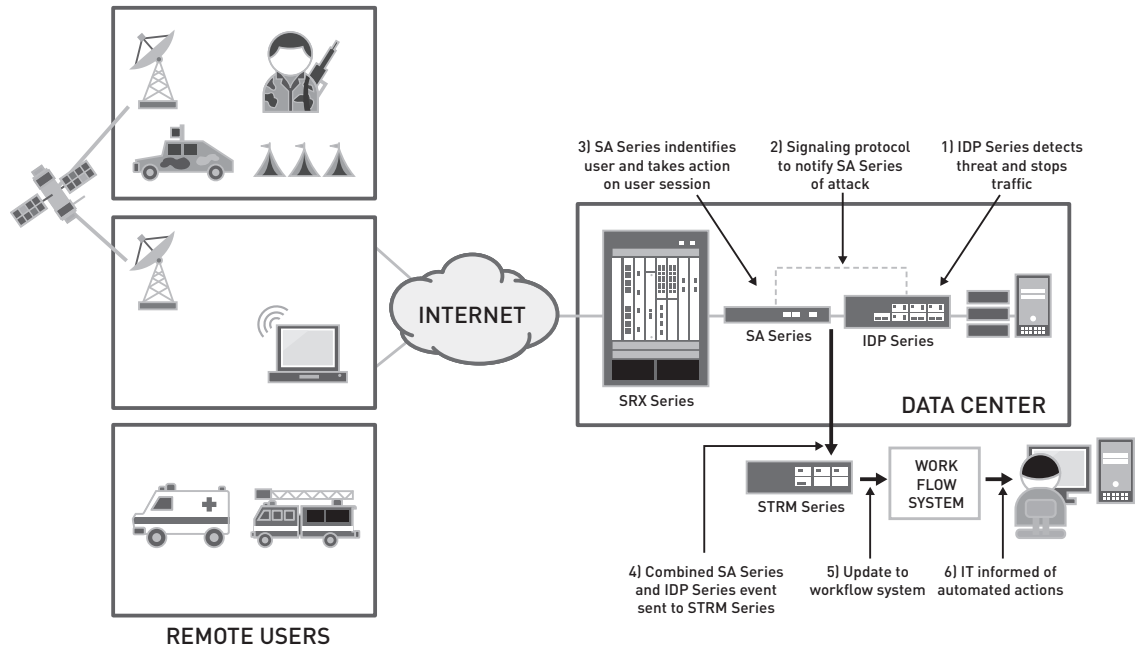


Figure 2: Juniper Networks Adaptive Threat Management Solutions

### Solving Agency Challenges with Adaptive Threat Management Strategies

Table 3 lists the security challenges that agencies currently face and how Juniper Networks Adaptive Threat Management Solutions can help solve these challenges.

**Table 3: Solving Agency Challenges via Juniper Networks Adaptive Threat Management Solutions**

| Challenges   | Juniper Networks Adaptive Threat Management Solutions  |
|--|--|
| Safeguard business and network during disruptions caused by attacks and real-world disasters | Proactive protection against known and unknown threats is provided, as well as the ability to identify, automatically remediate, and enforce security policy. These high-performance and scalable solution components support business continuity in the event of an attack, natural disaster, or other disruption.  |
| Protect critical data  | Cooperative system leverages intelligence across the network to adapt to changing conditions and protect critical assets. Administrators can easily segment and control access to data and network resources by user type—employee, customer, partner, or contractor.  |
| Provide network-wide visibility and control  | Provides multivendor collection and correlation of events and logs from all network devices across the enterprise. Advanced application and identity-aware visibility pinpoints threats and application policy violations. Incident notification is by actual user, as opposed to the IP address. Provides centralized policy management, configuration, and security device management. |
| Support compliance and log management  | Streamlined network log management and reporting supports and documents audits. High-performance appliances can scale to the largest environments, manage data from a wide variety of network and security devices, and ensure the integrity of collected data for forensic and compliance activities.   |
| Improve IT productivity and reduce TCO   | Scalable products allow users to consolidate the number of devices needed to support increased users and network traffic. With improved network and security visibility and automated response, IT resources can be streamlined or reallocated to focus on strategic projects.   |

## Reducing Total Cost of Ownership with Juniper Networks Adaptive Threat Management Solutions

Juniper Networks Adaptive Threat Management Solutions offer a comprehensive security portfolio that satisfies CAG requirements. Because these solutions are based on industry-leading security products that work better because they work together, compromising security to save money does not need to be a consideration.

Operational cost savings include:

- Single pane management for all routing, switching, and security devices, resulting in less to learn and easier maintenance
- Consolidated monitoring and reporting capabilities that support not only Juniper devices but third-party devices as well
- Follow-me policy for users logging in from headquarters, branches, or remotely—anywhere in the world
- Shared operating system between routing, switching, and security devices that simplifies learning, designing, and troubleshooting of a network
- Integrated security and networking capabilities that simplify network designs and operations

Capital expenditures are minimized:

- Unique pay-as-you-grow architectures, allowing you to spread your budget and spend over larger periods
- Integrated security and networking capabilities, requiring less equipment to purchase and maintain
- Open standards-based solutions, enabling flexibility and choice in innovating and vendor selection
- High-performance devices, even with many features enabled, allowing less expensive devices to meet requirements
- Complete product portfolio, providing proper scale for all locations and requirements without learning new devices and complicating support contracts

Juniper is focused on reducing both up-front CapEx as well as ongoing OpEx to deliver uncompromised security at low total cost of ownership (TCO). Point product solutions with disparate management systems, multiple interfaces, and proprietary protocols (created to lock you into their architecture) can never come close to the overall savings and security coverage that a well-planned and cooperative solution brings to the table.

### Certification Programs

Certifications are required or strongly desired by many government customers worldwide. Proof of security certification is especially important for governments in the U.S., Canada, UK, France, Germany, Australia, and Japan. Additionally, many commercial customers place high value on security certifications as well. There are several key certification programs that many government and public customers look for when evaluating cybersecurity products, such as Common Criteria and FIPS.

By obtaining security certifications, an equipment vendor demonstrates its commitment to Information Assurance (IA) and secure access across its product lines. This commitment helps vendors deliver more secure products, because the certification process may immediately uncover security-related issues. Also, the vendor's commitment to security certification helps foster a culture of security and assurance within the company, because certifications require substantial and repeatable investment to secure product development and product delivery.

The Common Criteria are a set of internationally recognized and accepted standards that allow vendors to make claims about the security functionality of their products and then demonstrate through third-party testing and verification that products actually meet those claims. Potential customers can use Common Criteria certifications to evaluate the secure nature of IT products that they wish to procure, without going through their own expensive and time-consuming security testing and qualifications. Today, more than 22 countries have adopted the Common Criteria certification.

FIPS have been developed by the National Institute of Standards and Technology (NIST) to ensure the security of algorithms and cryptographic functions. These standards are used as a guideline for federal procurements and are recognized by the U.S., Canada, and increasingly, by other governments around the world such as the UK. In addition, FIPS standards are likely to be adopted at least in some part by organizations and enterprises in the financial arena, as part of the American National Standards Institute (ANSI).

FIPS 140-2 are security requirements that must be met by a cryptographic module used in an IT security system that

protects unclassified information. FIPS validation verifies the secure design and implementation of the cryptographic module in question. Areas analyzed and validated by FIPS 140-2 include cryptographic algorithms, key management, software security, physical security, basic design, and documentation, to name a few.

## Comprehensive Product Brand Integrity Management

The final component of a comprehensive cybersecurity solution includes a vendor's product brand integrity, which can be defined as the implementation of defined best practices to identify IP risk and provide controls to minimize risk from the following:

- Understanding the risks to their products and intellectual property
- Applying brand integrity best practices to their internal process design
- Production processes and supply chain management
- Distribution channels and marketplace oversight

## Security Certifications

All levels of government and military networks are required to increase their level of cybersecurity to maintain confidentiality, integrity, and availability. New national security policies governing the acquisition of Information Assurance (IA) products require government and military officials to make sound, risk-based decisions when authorizing the placement of IA products into their networks.

NSTISSP #11 governs the acquisition of information assurance and IA-enabled information technology products. The policy, issued in January 2000 and revised in June 2003, mandates that departments and agencies within the executive branch shall acquire, for use on national security systems, only those commercial off-the-shelf (COTS) products or cryptographic modules that have been validated with Common Criteria or that adhere to the Federal Information Processing Standards (FIPS).

Another important part of the complete cybersecurity solution is recognized, professional security certification, which is a third-party verification of the vendor's security claims against defined security evaluation criteria. Certifications result in an independent measure of assurance, and increase government and military decision maker confidence in the security of the product. Security certifications provide government customers with a higher level of confidence about the quality of commercial security products. Securing information systems is all about managing risk, and the use of certified or evaluated products reduces the number of unknowns for overall security functionality.

## Conclusion

Federal agencies are aware that their existing infrastructures are not suitable for combating today's ever increasing and highly sophisticated cybersecurity attacks, whether these attacks come externally from rogue nations trying to bring down entire networks or internally from federal employees who inadvertently or intentionally compromise a portion of the network. Upgrading the existing infrastructure requires security solutions that are scalable and adaptable, and work in multivendor environments and applications so that they can be phased in without disrupting current operations.

Although the federal government's CAGs are just guidelines, implementing these controls is a positive step towards standardizing and enhancing security practices. Having to pass stringent reviews and global validation (comparing these guidelines to other audit guides for ISO 2700x, HIPAA, GLB, PCI, and SOX compliance testing) further enhances the value of these guidelines.

Compliance and regulatory requirements are other factors that must be seriously addressed by local and federal agencies in delivering reports and audit trails. However, it is important to keep in mind that these audit trails and reports, once again, are generated from multivendor management applications and devices, making it quite difficult for an IT staff to identify, define, coordinate, and compile data into comprehensive, easy-to-understand security reports, and do it in real time as well.

Sophisticated attacks are not always isolated; they tend to spread across the network looking for new systems to breach and to replicate. As viruses and worms spread throughout the network, so does the cost of regaining control. Isolating the cause while trying to analyze multivendor management applications and devices in real time is difficult and time-consuming, at best.

Therefore, to keep in step with the government's guidelines and to help reduce TCO while addressing the government's CAGs, Juniper remains committed to delivering dynamic and high-performance cybersecurity solutions. With Juniper Networks Adaptive Threat Management Solutions, we provide network-wide visibility and control to address the constantly evolving security landscape seen in today's government networks.

Business benefits include proactive data protection, business continuity, and reduced TCO. IT benefits include fewer network disruptions, IT resources freed from mundane tasks, and support for compliance requirements. Juniper is also committed to providing security solutions that meet multiple levels of security compliance based on the user's mission requirements, and to continuing to manage our product brand integrity program for all of our products. As security threats change, Juniper's comprehensive cybersecurity solutions will continue to adapt to ensure proactive protection, business continuity, and security compliance while reducing costs.

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

---

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.