

# ADAPTIVE THREAT MANAGEMENT SOLUTIONS – PUBLIC SECTOR

## High-Performance Security Solutions That Work Together

### Challenge

Because the network is critical to achieving mission-critical objectives for local and national services, public sector organizations cannot afford a security breach or unplanned downtime. Unfortunately, today's disparate point security and networking products have been deployed as a patchwork of devices resulting in ineffective network security that is costly to operate.

### Solution

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.

### Benefits

- Comprehensive security that identifies, mitigates and reports on even the most sophisticated attacks
- Reduced cost of ownership with lower CAPEX and OPEX compared to disparate point products
- Improved response times while requiring less 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

Juniper Networks® innovation in Government is a high-performance network infrastructure that enables next-generation networks, providing the responsive and trusted environment needed to fuel government transformation. For public sector organizations like military defense, public administration, homeland security, healthcare, and research and education organizations, threat management continues to be a high priority to help protect people, privacy, and assets. None of these organizations can afford a security breach, compromised network performance, or unplanned downtime that can occur because of security incidents, continual upgrades, network expansions, or changes to security policy within the infrastructure. These organizations need to ensure business continuity for mission-critical operations and services from the battlefield to higher education campuses to hospital emergencies amidst real-world disasters (such as pandemics, strikes, and natural disasters) while meeting strict federal security compliance and reporting regulations.

Although various types of security protections are being integrated into public sector network infrastructures, many departments and organizations are still struggling with a mixture of security solutions that may or may not work together. Many of these security solutions are not able to adapt and scale to meet a constantly changing security landscape. Gaps between these disparate devices may leave the network more vulnerable and hamper network-wide visibility and control. And, in many cases, users are required to deploy and manage another device to provide network-wide visibility. Ultimately, the paradox for most network security specialists today is providing users, partners, and citizens with the optimized network access they need and expect, while preventing hackers from accessing and attacking the system.

Juniper Networks® Adaptive Threat Management Solutions deliver a consistent and comprehensive approach to security while providing the freedom to deploy a best-in class approach that is right for your agency or department. Gain peace of mind by deploying security that will protect your environment both today and tomorrow while allowing you to focus on your mission-critical objectives.

### The Challenge

For most public sector organizations today, the network has evolved over time into a patchwork of dedicated point products, each of which solves a specialized problem. For example, one government agency may have added intrusion prevention to comply with legislation and firewalls to protect the highly sensitive information in the data center, a healthcare institution may be using an SSL VPN to provide remote access to doctors without having to support a pc-based client, and an educational institution may be integrating smaller firewalls to protect smaller campuses and may be considering overall LAN access control. Each product likely does its job well. Unfortunately, blended threats are designed to take advantage of the gaps between these point products because, good as they may be on their own, they are not designed to communicate with one other. For example, an intrusion prevention system (IPS) may detect an application anomaly as

a firewall logs reconnaissance activity and the access control devices capture a series of login attempts in the campus or across the VPN. While each product may be doing its individual job, they do not communicate with each other and as a result, more complex attacks are easy to miss. By the time a breach is detected, if at all, the damage has already been done and mission-critical services are affected.

Public sector network administrators are often faced with the additional challenge of consolidating the information coming from each of these devices into comprehensible reports required for security purposes as well as by federal auditors or regulators such as Health Insurance Portability and Accountability (HIPAA). This is often a daunting, error prone task that is costly and time consuming. And even if it were possible to assemble the massive log output of all devices, there is no single method for separating or correlating meaningful data from background noise. This challenge grows exponentially when one tries to identify the root cause of an attack, where reports and logs need to be looked at from multiple systems and several hundred devices, spread over many locations. Reactive forensic analysis becomes inconsistent and error prone and it is certainly not a way to take a proactive view of the overall network.

Finally, scaling such a network or adding more security only further contributes to the cost and complexity, which is usually not an option for public sector organizations that are being asked to do more with less. The learning curve is steep, since each product has its own operating system, management tools, and troubleshooting techniques. This difficulty gets compounded with the addition of each new product, since most point products are not created with incremental additions in mind. Total Cost of Ownership (TCO) therefore, must not only include the expense of the equipment itself but also the less obvious disturbance to normal operations that results from deploying, testing, troubleshooting and managing new installations.

## Juniper Networks Adaptive Threat Management Solutions

Juniper Networks offers public sector organizations the industry's only high-performance adaptive threat management solution that leverages a dynamic, cooperative product portfolio. This solution provides network-wide visibility and control to increase security and reduce the TCO associated with delivering applications and services.

Each of the Juniper security products contributing to Adaptive Threat Management Solutions are best-in-class in their own right. But because they are from Juniper, these products offer something that other products don't—the ability to work together. The tight integration between devices enables Juniper Networks Adaptive Threat Management Solutions to provide value beyond the sum

of its parts. These solutions empower the network itself to change based on parameters you set, as variables within the network, users, and threat landscapes change. All policy creation and device configuration in the solution can be managed using Juniper Networks Network Security Manager (NSM). With only a single provisioning solution to learn, operating costs drop significantly, policy and configuration changes are faster, and there are fewer human errors. Juniper Networks STRM Series Security Threat Response Managers can take data from all of your network and security devices to provide an "aerial" view of your network that gives you the perspective you need to be proactive. The STRM Series comes prepackaged with over 500 different reports, and greatly simplifies generating the network security, trending, and compliance reports that you need.

To help public sector IT administrators working with limited budgets, Juniper Networks Adaptive Threat Management Solutions can be deployed in phases, because each piece of the solution adds more value to the whole, regardless of the order in which pieces are implemented. Because Juniper builds its products to industry standards, each device will integrate into an existing government, educational, or healthcare installation, offering greater choice and flexibility than proprietary solutions that are designed to lock you in to a specific vendor. Together, Juniper security solutions provide the product-specific security, as well as the network-wide visibility, mitigation, control and reporting needed to adapt and secure the network against constantly evolving threats.

Key characteristics of this solution include:

- Consistent and granular policy based access control regardless of the location where you access the network
- A single network-wide view for identification, mitigation, and reporting of complex attacks that eliminates false positives with a highly advanced correlation system, enabling you to concentrate on actual security incidents
- Centralized management capabilities reducing management complexity, supporting compliance requirements, and reducing TCO
- Automatic and self-remediation of noncompliant users and devices that significantly reduces the cost of operations as it well as increasing the security posture of the network
- Automation of mundane threat mitigation and reporting activities that frees up IT staff

## Reduce TCO While You Increase Agility

Juniper Networks Adaptive Threat Management Solutions feature unparalleled security and compliance functionality with a low TCO, achieved by reducing both obvious capital expenditures and hidden operational expenses. CAPEX is reduced with products designed to scale via an incremental, pay-as-you-grow model. OPEX is reduced with features such as a single management system that provisions all products in the solution, simplifying learning and reducing deployment and provisioning times. The solution also provides correlation of multi-vendor devices, yielding network-wide monitoring and reporting as well as automation of mundane security operations. With the reduced burden of management and the adaptable capabilities of the network, operational efficiency is increased. New services like e-government web sites or Health Information Technology (HIT) can be rolled out more quickly and with less concern that human error will create new security risks or that sophisticated attacks will be missed.

## Lower Capital Expense

Getting started with Juniper Networks Adaptive Threat Management Solutions can be done with minimal capital outlay. Because Juniper leverages the security you already have deployed in your network and has a complete line of products that scale from the smallest campuses to the largest data centers, there is always a high-performance product at the right cost to meet your requirements. In addition, a pay-as-you-grow model allows you to incrementally add network protection as your agency or department requirements expand. A few examples of this pay-as-you-grow model include the SRX Series, built on Juniper's new Dynamic Security Architecture and specifically designed for simple, seamless expandability up to 120 Gbps of firewall. Once an SRX Series gateway is in place, adding additional security processing power requires just another Service Processing Card (SPC), with no additional software or wiring configuration required. All functions use the same SPCs, resulting in extraordinary flexibility and choice when choosing services such as firewall, intrusion detection and protection, Network Address Translation (NAT), or VPN that require additional processing cycles.

Policy enforcement products such as UAC and the SA Series can scale to tens of thousands of devices and users for providing network access control for sensitive data like Emergency Medical Records (EMR) and Patient Health Information (PHI). However, since these products employ a pay-as-you-grow license model, once the infrastructure is in place, you only purchase additional licenses on an as-needed basis. The additional license implementations only require a simple cut-and-paste into the management tool to increase the scale of support. No other configuration is required.

## Lower Operational Expense

Provisioning any of the products within Juniper Networks Adaptive Threat Management Solutions is accomplished with NSM. NSM supports routing, switching, and security products by default, so per-device management applications don't need to be purchased and planned for. This means that you can simply grow device licenses as your network grows. The result is that ongoing maintenance costs begin to evaporate, learning is accelerated, and IT coverage is simplified, since administrators can easily manage different products using the tool they are already familiar with. With Juniper Networks Adaptive Threat Management Solutions, NSM administrators can create policy across a network from a single console. For example, new access policies are pushed to both UAC and the SA Series for consistent policy and network entitlements no matter where the user is located. UAC enforcement on firewalls and Juniper Networks EX Series Ethernet Switches are also defined within NSM.

Network-wide monitoring, correlation from multiple feeds, and reporting from a single STRM Series console means that all device logs are correlated and consolidated, enabling identification, mitigation and reporting of complex and blended attacks. No longer do you have to wait for a third party such as a credit agency, law enforcement agency, or the press to let you know about lost intellectual property, as you can proactively detect user misbehaviors. Not only does the STRM Series allow you to be proactive, it also eases compliance reporting by including over 500 predefined and easy-to-customize reports. Like the other products in the solution, the STRM Series can be scaled up as you grow. All supported devices and reports are always included, so there are no management costs and complexity surprises as your network is required to support new demands and devices.

## Increase Operational Efficiency

The requirements of today's network—as well as what threatens it—change all the time. New organizational requirements, like healthcare organizations moving toward electronic records, demand at new locations, audiences and applications being added to the network all open new threat vectors. These new offerings also create new compliance headaches. The investments you make in your network today must enhance the organizations operational efficiency in the face of such a mission-critical climate.

Juniper Networks Adaptive Threat Management Solutions are designed to make fluid changes in scale, threat response, and compliance easy. For example, adding new capabilities to the SRX Series doesn't mean that you need to add a new firewall—just a new SPC. The IDP Series responds to threats in real time, even zero-day attacks. And the STRM Series features a breadth of reports to make new compliance requirements easier to meet.

## Mitigate Risk and Raise Productivity

### Secure Access by Organizational Roles and Responsibilities, Independent of Location

As access to an asset goes up, so does the risk. As the network has become mission critical and users increasingly depend on it to be operational, the risk associated with access to the network has also increased. Resources used to be protected by the network perimeter, much as a castle would be protected by a moat, and it was assumed that anyone who could get past that perimeter had a right to access the data and applications within. As government employees, higher education professors, and medical employees have become increasingly mobile, the conventional view of the network perimeter has dissolved. Users no longer know or care where an asset is housed. They require seamless access to key resources from anywhere in order to do their jobs. While this approach increases productivity, it also poses incredible risk. In today's public sector organizations, an attack could come from inside the LAN, from a branch office, or from a remote location; a breach could originate from an unknowing employee, a student or a business partner.

This new paradigm is not supported with typical, location-specific security point products. Protection cannot be device-specific; a consistent security posture must be adopted and enforced throughout the network in order to be effective. Threats must be recognized and prevented from wherever they are detected, and the rest of the network must be alerted to prevent attack spread or data loss.

While this appears to be obvious, according to 2008 quarterly Trends and Analysis Reports from the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT), the largest percentage of cyber security incidents continue to be from scans/probes/attempted access followed by improper usage, malicious code, unauthorized access, and denial-of-service. Common sense shows that risk mitigation must be holistic, and such protections are required by strictures such as Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) or Sarbanes Oxley Act (SOX), which require that access to regulated data be confined to certain departments and individuals. Unfortunately, the fact remains that most network managers are so overloaded with simply keeping the network running, that it is difficult to see how to add overarching security protection with granular access control that can be tailored to the user group or individual user, even given the compelling mandated and security benefits.

Juniper Networks Adaptive Threat Management Solutions include the industry's only organization-wide access control capabilities that focus on users and applications, no matter where they access the network. Juniper firewalls can benefit from the application and threat information gleaned from the IDP Series appliances. The IDP Series alerts on malicious or noncompliant behavior trigger a change in access rights for a user throughout the network. Each individual device within the solution dynamically adds information to the whole, creating the dynamic risk mitigation you need.

### Juniper Networks Adaptive Threat Management Solutions Phased Deployment (an example)

SA Series and UAC ensure consistent policy enforcement regardless of user location, while federated identity eliminates the need for multiple sign-ons across globally protected resources.

Juniper firewalls can be made identity-aware and deployed as policy enforcers for the UAC solution, increasing choice and flexibility of where to deploy enforcement points.

IDP Series capabilities, which can be added to Juniper firewalls or deployed as a standalone platform, watch for anomalous behaviors, malicious traffic, and the use of noncompliant applications. The IDP Series can then instruct a variety of products throughout the solution to drop, quarantine, or remediate the user/session.

NSM provisions policies across the entire solution, greatly enhancing consistency and eliminating user errors.

STRM Series correlates all access and network usage information from Juniper firewalls, SA Series, UAC, IDP Series, networking products, and other vendor products, along with other corporate systems such as servers and applications. This completes the feedback loop required both for forensic activity and proactive planning. The STRM Series also eases compliance with over 500 reports that are prepackaged and very easy to customize.

UAC also addresses the common problem of how to provide appropriate access to temporary guests, with an easy-to-use Web interface designed to be used by non-technical staff. These guests can be granted customizable, limited time and access privileges on the network during the duration of their stay.

## Features and Benefits

Only Juniper Networks Adaptive Threat Management Solutions offer such a rich set of risk mitigation capabilities and network-wide policy control in an open and standards-based environment. Government, educational, and healthcare IT organizations experience increased productivity by provisioning security, access control, routing, and switching devices through a single management console. Simplified management leads to less human error, faster troubleshooting, and the ability to detect a security breach that may have slipped through a legacy environment. Users with different department roles can safely share the same network infrastructure with less ability to spread viruses and worms, since their endpoints must always be compliant with security policy and their access is restricted to only job-role entitled data and applications. Single sign-on, federated identity capabilities, and consistent policy experiences across a global public sector network with Juniper Networks Adaptive Threat Management Solutions means users can access the network easily and securely from anywhere, without placing a burden on IT to administer such productivity capabilities across the network.

Key features and benefits of this solution include:

- Organization-wide collaborative network security and granular access control
- Satisfy federally mandated compliance and regulatory requirements
- Centralized provisioning and policy management
- Universal log management and threat detection, with real-time and historical reporting
- Automated and proactive approach to risk mitigation
- Secure, high-performance infrastructure that supports the growing network and enables the delivery of new products, applications, and services.

## Solution Components

Juniper Networks is a leader in network security, with innovative products recognized as best in their category by analysts around the world. Security products that can be deployed as part of Juniper Networks Adaptive Threat Management Solutions across an entire public sector network include:

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 Juniper Networks ISG Series Integrated Services Gateways and Juniper Networks SSG Series Secure Services Gateways.</li> <li>• Tightly integrated set of unified threat management capabilities to protect against worms, viruses, trojans, spyware, denial of service (DoS), and blended attacks.</li> </ul>
The new Juniper Networks SRX Series Services Gateways	<ul style="list-style-type: none"> <li>• These gateways provide Firewall, IDP, VPN and other network and security services. Based on Juniper's revolutionary Dynamic Services Architecture, a stable, scalable platform designed to allow you to build the network you need today, with all of the headroom you could want for tomorrow.</li> <li>• SRX Series Services Gateways are available in a variety of form factors, enabling you to buy what you need for each location.</li> </ul>
Juniper Networks 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 Juniper Networks SA Series SSL VPN Appliances for remote and granular access control to group or individual level.</li> <li>• Juniper Networks Unified Access Control for users on the LAN.</li> <li>• Federated identity management enables single sign-on (SSO) across both platforms.</li> </ul>
Juniper Networks Network and Security Manager	<ul style="list-style-type: none"> <li>• Enables centralized provisioning of Juniper Networks routing, switching, and security products.</li> </ul>
Juniper Networks STRM Series Security Threat Response Managers	<ul style="list-style-type: none"> <li>• Single console for log, 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>

## Summary

Public sector organizations around the world view the network as critical to achieving mission objectives. To effectively protect their government, educational, or healthcare organization, network administrators, IT managers, and network security specialists must have insight into the multiple types and levels of evolving threats that impact the integral elements of the organization, including perimeter cyber security, critical resources, and remote access.

Juniper Networks Adaptive Threat Management Solutions offer robust and highly cooperative, network-wide solutions consisting of tightly integrated network security products. They provide industry-leading security that is dynamic and optimized for high-performance public sector organizations, as well as network-wide visibility and control that is essential in protecting your department or agency from today's highly volatile and damaging security threats. Juniper Networks Adaptive Threat Management Solutions help you achieve your mission objectives, while also realizing the benefits of superior point products that work better because they work together.

## Next Steps

For more information on Juniper Networks Adaptive Threat Management Solutions, please visit us at [www.juniper.net/adapt](http://www.juniper.net/adapt) and contact your Juniper Networks representative. If you are interested in learning about financing offerings, please ask about Juniper Financing Advantage, provided by IBM Global Financing. We offer comprehensive funding options at very competitive rates.

## 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 2009 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.