

ADAPTIVE THREAT MANAGEMENT SOLUTIONS

Intelligent Security and Performance
for the Distributed Enterprise

Juniper Networks Adaptive Threat Management Solutions Overview

Today's enterprise is at the center of a number of conflicting trends related to changes in the network. Data centers are consolidating as enterprises are scaling beyond headquarters to regional, branch, and remote locations, and often the network functions as the primary connection between these locations. In order to be competitive, today's enterprise network must be open for business wherever, whenever, and however business is done.

Unfortunately, these highly distributed environments can also open the network—and the enterprise itself—to threats that are motivated by everything from mischief to profit. Growing application use and user mobility mean that today's malware, killer worm, or virus is as likely to be inadvertently launched by a telecommuter as planted by a hacker. Small remote offices are just as vulnerable to these threats as well-protected corporate headquarters, and usually do not have the same IT staff or budget. Individual users, many of whom access the network via unmanaged devices, often do not proactively manage their own defenses on the daily basis that is required to ensure that the network as a whole remains safe and where applications can be flawlessly delivered.

Today's distributed enterprise network needs to have the ability to deliver a LAN-like experience, regardless of how far away from the LAN users may be. Business-critical online applications can strain the network, particularly in the case of remote users or branch offices. Poor performance or unplanned lapses resulting from security incidents, network-wide upgrades, changes to security policy, or even natural disasters and pandemics, can directly and substantially impact bottom-line business.

Network and security managers are in the eye of the storm. Most networks have evolved over time, often into a complex system that eats up IT resources in day-to-day maintenance. As the enterprise consolidates data centers and makes the most of networking with remote users and branch offices, overall management becomes still more complicated. And each additional location or user and new application installed or downloaded represents a new threat vector to the network. At the same time, attacks and attackers are growing increasingly sophisticated, leaving individual users and distributed branch offices vulnerable.

The only reliable way to identify, mitigate, and report on threats is with a cooperative security system which can provide real-time protection by correlating information about events occurring throughout the distributed enterprise. This system needs to be able to sift actionable data from unneeded detail. And, a true distributed enterprise security solution should proactively provide granular user-level protections and security without impacting speed, performance, and user productivity.

As network requirements have grown, so too have the threats affecting your business. Attacks are more intelligent and your security must be more intelligent as well. Juniper Networks® Adaptive Threat Management Solutions deliver a consistent and comprehensive approach to security, while providing you with the freedom to deploy best-in-class products that are right for every user and location in your business. These solutions can be added incrementally, so there are no forklift upgrades required. With Juniper, you move quickly from reactive to proactive by deploying security and performance that protects your environment both today and tomorrow, while allowing you to increase productivity and focus on securely expanding your business.

Challenges

As the enterprise has become increasingly reliant on the network, infrastructure has grown into a patchwork of dedicated point products, each of which solves a specialized problem. For example, a company may have added intrusion prevention to comply with legislation, firewalls to protect the data center, application acceleration to speed performance, SSL VPN to provide remote access without a client, smaller firewalls to protect the branch, and may even be considering overall LAN access control. Blended threats are designed to take advantage of the gaps between point products, which are typically not designed to communicate with each other. For example, an intrusion prevention system (IPS) may detect an application anomaly as a firewall logs reconnaissance activity and 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 well, it is easy to miss the hints of a more complex attack if these point products don't communicate and coordinate with each other. By the time a breach is detected, if it is detected at all, the damage is already done. As the enterprise becomes more distributed, these issues become compounded. And because remote users and branch offices may not have dedicated IT resources, they may not be as well defended as headquarters locations.

The Challenge

To meet growing demands for applications, locations, and access, many networks have grown into a patchwork of disparate point products. These products, because they are not designed to operate together, create significant areas of vulnerability in terms of security and application delivery. In addition, they do not allow for visibility across the network, which is problematic for monitoring and reporting requirements. What you need is an over arching solution that combines consistent security and performance with network-wide visibility and ease of use.

The Solutions

Juniper Networks Adaptive Threat Management Solutions make work forces more productive with fewer security and application delivery risks, all while significantly reducing total cost of ownership (TCO). This solution is built on a dynamic, scalable and cooperative security infrastructure, which provides real-time threat defense and application delivery along with unparalleled network-wide visibility and control.

Benefits

Juniper Networks Adaptive Threat Management Solutions provide a responsive and trusted security and application delivery solution for the high-performance network. This cooperative solution delivers:

- Comprehensive policy-based security and performance to all locations
- Lower total cost of ownership
- Open architecture
- Business agility and scalability

Interestingly, network managers also face the additional challenge of consolidating the information coming from a multitude of security devices into the reports that are required for internal, audit, or regulatory review. Because this daunting task must incorporate output from diverse sources that are not designed to correlate their information, it is enormously time-consuming, as well as subject to human error. And even if an organization could assemble the massive log output from all of its enterprise devices, there is no single automated 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 from multiple systems and several hundred devices that are spread over many branch locations need to be analyzed. Reactive forensic analysis becomes inconsistent and error prone, preventing businesses from taking a proactive view of their network and security as a whole. The result is that once an attack is found, it is only after the damage has already been done, and many attacks are never detected at all.

Finally, scaling such a network to handle more users, new applications, or enhanced security further contributes to greater costs and complexities. The learning curve is steep, since each product has its own operating system, management tools, and troubleshooting techniques. The cycle is often repeated 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 business require

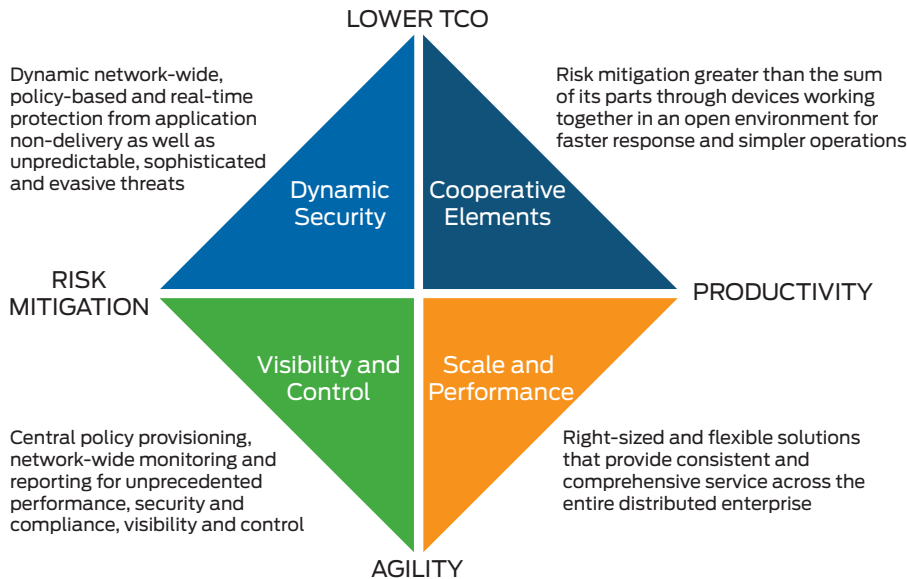
Trends

Commonly deployed security and performance solutions fall short of protecting high-performance networks because they:

- Fail to adapt to and mitigate evolving threats, leaving the enterprise still open to attack
- Lack multilayered security to protect against a wide range of threats coming from multiple attack vectors
- Lack network-wide visibility and control through tight integration and cooperation between security products, especially in distributed environments
- Lack real-time monitoring of traffic flows causing the network to be exposed to attack
- Lack coordination and automation to stop attacks in real time throughout the network
- Leave businesses prone to human error, resulting in exposure to security threats and possible compliance violations
- Create performance bottlenecks and application non-delivery in the network
- Lack centralized management and reporting capabilities needed to provision new security or performance policies, analyze the health of the network, ensure compliance, and correlate and analyze vast amounts of data for insightful analysis, recommendations, and reports across the enterprise
- Lack the ability to provide consistent policy and protection for all locations where users are accessing network resources, particularly when they are located outside of headquarters

Adaptive Threat Management Solutions Portfolio

Juniper Networks is a leader in networking, with innovative products recognized as best in their respective categories by analysts around the world. Furthermore, because they are from Juniper, these products offer something that other products don't—the ability to work together. The tight integration between Juniper's devices delivers a solution whose value exceeds the sum of its parts. This empowers the network itself to dynamically respond to threats in real time based on the policies the business sets, as variables within the network, users, and the threat environment change. Businesses do not have to compromise performance or productivity for improving risk mitigation, or incur higher network TCO when deploying new services and applications.



Juniper Networks Adaptive Threat Management Solutions include:

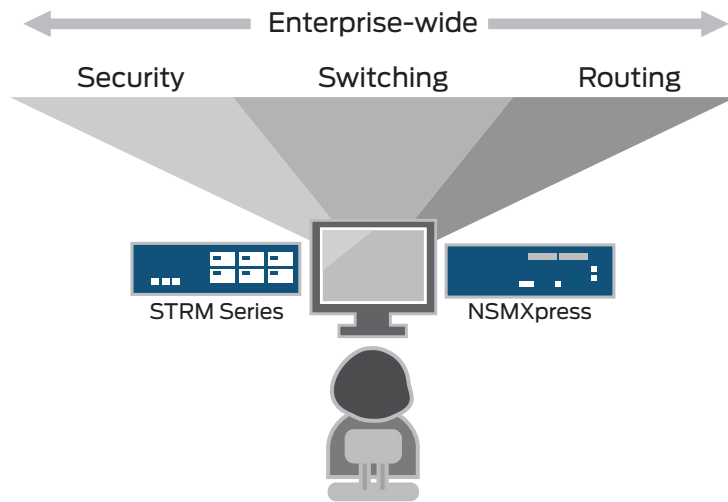
- Juniper's suite of firewalls
- WXC Series Application Acceleration Platforms
- SRX Series Services Gateways
- SA Series SSL VPN Appliances
- Unified Access Control and Juniper Networks IC Series Unified Access Control Appliances
- IDP Series Intrusion Detection and Prevention Appliances
- Network and Security Manager
- STRM Series Security Threat Response Managers

Business Benefits of Juniper Networks Adaptive Threat Management Solutions

Benefit: Lower Total Cost of Ownership

Total cost of ownership for networks includes two different categories—OpEx or the cost of keeping the equipment running day-to-day; and CapEx, which includes equipment purchasing costs. Juniper Networks Adaptive Threat Management Solutions can help organizations lower both.

According to leading analysts, OpEx can consume up to 80 percent of the total cost of running a network. Tasks included in this category range from device life cycle management including configuration, provisioning, troubleshooting, and maintenance, to hiring skilled technical staff and training them on multiple disparate platforms and management systems. These OpEx issues multiply rapidly when branch offices are considered. With Juniper Network Adaptive Threat Management Solutions, all devices in the distributed enterprise are managed by a single management platform— Juniper Networks Network and Security Manager. With NSM, your staff has only one console to learn. You can use NSM to create and revise policies, provision equipment, or troubleshoot issues on Juniper routing, switching, access control, and security products and solutions, regardless of where these devices are physically located. Juniper Networks STRM Series Security Threat Response Managers simplify the picture even further by providing a single monitoring system for your entire network, handling logs and flow data from Juniper devices as well as from many other vendor devices. The STRM Series comes with more than 1,300 predefined, easy to customize reports, so the handling of new audit and compliance requirements can be implemented quickly and cost effectively.



Enterprise-Wide Common and Consistent Provisioning, Monitoring, Reporting, Log Management, and Threat Management Significantly Lower TCO

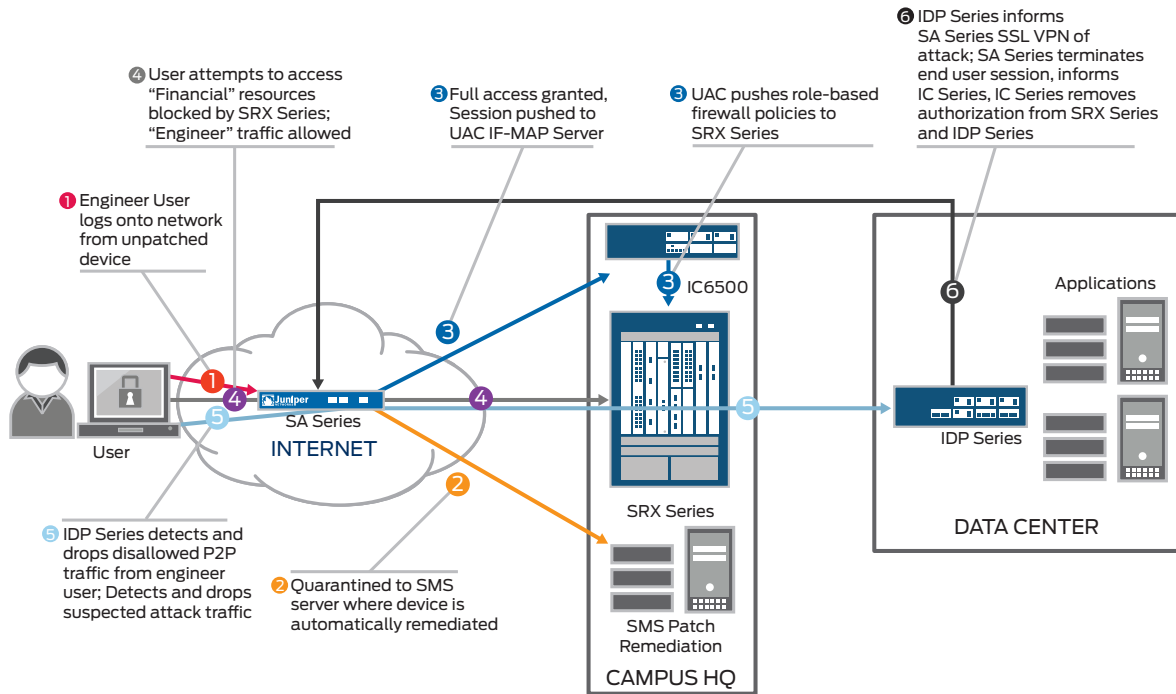
Juniper Networks Adaptive Threat Management Solutions have been designed to scale to support at all locations while also lowering CapEx. Juniper Networks SRX Series Services Gateways are available in a variety of scalable form factors to provide right-sized processing and network connectivity in addition to natively integrated IPS, VPN, and other networking and security services—from your smallest branch office to the core of the data center. Other products in the solution, such as NSM, STRM Series, Juniper Networks WXC Series Application Acceleration Platforms, Juniper Networks Unified Access Control (UAC) for network access control (NAC), and Juniper Networks SA Series SSL VPN Appliances can be scaled via licensing. Adding licensing and processing or connectivity is operationally fast and simple, as there is minimal to no additional configuration, racking, or wiring required.

Benefit: Comprehensive Risk Mitigation

Juniper Networks Adaptive Threat Management Solutions also work together to eliminate risk. Because IPS is integrated throughout the solution components, early detection is achieved regardless of the location from which suspect traffic originates in the distributed enterprise. For example, network access is protected with antispyware which is dynamically provisioned when the user connects to the network remotely via the SA Series; or, when local network access control is secured by UAC. Once the user is connected, the Juniper Networks IPS functionality, available in standalone appliances or as an integrated feature, can be configured to automatically drop the user session, quarantine the users, or simply notify them if anomalous traffic is detected. The same policy applies to traffic that the IDP Series might see from a user on the LAN who is going through the UAC solution, and full IPS capabilities are integrated from the smallest SRX Series branch firewall to the largest data center platforms. This means that a single policy can be applied consistently, regardless of the user or device used to access critical resources. And every security event across the network is logged and reported via STRM Series.

As Juniper Networks Adaptive Threat Management Solutions expand across the network, greater risk mitigation is realized with minimal IT intervention. In the figure below, for example, all Juniper Networks devices are provisioned with NSM. Policy can be defined once and pushed to both the LAN and remote policy decision points. Enforcement devices such as Juniper Networks EX Series Ethernet Switches and SRX Series firewalls are provisioned with the same tool, and are available to accommodate a variety of locations. The system works in a cooperative fashion to ensure consistent access rights for all network users, from guests to contractors, and all employee roles.

Antispyware is dynamically provisioned to users of SA Series appliances and the UAC solution. The result is seamless, uninterrupted service, regardless of whether the user is remote or local. For IT, this means every user and device accessing the network is accounted for and forced into compliance, and the individual user's ability to inflict damage on the network is restricted. Anomalous and non-compliant behaviors, whether intentional or due to malicious code on a server or a user's device, can be rapidly identified and isolated by limiting access and directing traffic away from any infected applications, users, or network segments. Meeting compliance is made easier with reports which are automatically and proactively generated for auditors and other compliance bodies.



Enterprise-Wide Access Control in Action

Benefit: Enhance Productivity

Juniper Networks can help you raise your productivity in a variety of ways. One example is the Juniper Networks WX client, now integrated with the SA Series SSL VPN appliance that provides application acceleration based on user identity. Remote users will also enjoy federated identity capabilities with the UAC solution, so user sessions can be seamlessly provisioned into Unified Access Control upon login. This capability delivers a consistent, uninterrupted end user experience regardless of the user's location.

Because Juniper Networks Adaptive Threat Management Solutions cooperate with one another, productivity is further enhanced with the automation of tasks like log management and alarm prioritization that so often burden the networking staff. Auto remediation and self remediation capabilities provide a self-administering, integrated access control solution that also lightens the IT staff's workload by empowering users to rectify their security posture on their own, in many cases eliminating the need for human intervention. Furthermore, compliant endpoints lead to more stable endpoint devices, fewer calls to IT, and a more productive workforce across the company.

JUNIPER NETWORKS SERVICE AND SUPPORT

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services/.

The STRM Series enhances IT productivity even further, as it collects logs from across the entire network, reducing the number of logs from millions to prioritized events to address. This is all accomplished in real time, bringing a heightened ability to detect even the most complex network breaches and attacks. This enterprise-wide view in a single monitoring system is required to defend against today's blended attacks that often spread reconnaissance efforts, use multiple entrance vectors, proliferate from within, and then attempt to capture and send sensitive information back to the hacker. IT productivity skyrockets once IT personnel can remove themselves from the burdens of log management and data collection for reporting.

Benefit: Increase Business Agility

Juniper Networks can help your business increase its agility throughout the network, by enabling compliance, application delivery and threat mitigation in real time, to maximizing your budget. With Juniper Networks Adaptive Threat Management Solutions, you have the flexibility to roll out just the equipment you need across your distributed enterprise with standards-based products that scale. Remote or mobile users will enjoy the robust connectivity of the SA Series, the dynamically provisioned WX client, antispymware functionality, and the consistency of granular policies that follow users even as they change locations. STRM Series Security Threat Response Managers feature more than 1,300 different report and compliance templates, so if your business expands into an area with new reporting and auditing requirements, these can be easily met. With fewer hardware changes and configuration updates required, new services and applications can be rolled out across the network more quickly and securely. In addition, these solutions can deliver the means to enact policy-based, real-time decisions that are built on identity and application awareness across your network. This means that adding or removing new user organizations and changing application service levels for each organization can be accomplished through changes in a centralized policy server, making your business more agile.

The adoption of standard protocols maintains choice and flexibility in your network. You are not restricted to a single vendor's view of how to transform your network into a competitive advantage. You have the freedom to innovate and spend your budget based on your own business cycles and requirements. A recent example of Juniper Networks Adaptive Threat Management Solutions' support of standards is Interface for Metadata Access Point (IF-MAP) protocol from the Trusted Computing Group (TCG)'s Trusted Network Connect (TNC) workgroup. By implementing IF-MAP in the SA Series and UAC, Juniper enables a seamless, uninterrupted end user experience for both remote and local users, and provides network-wide, single sign-on support. This greatly simplifies the deployment of new applications and services. And supporting this standard means that third-party security products can work within Juniper Networks Adaptive Threat Management Solutions.

Key Differentiators of Juniper Networks Adaptive Threat Management Solutions

Products Designed to Work Together

Any one of Juniper Networks Adaptive Threat Management Solutions can be deployed as a best-in-class point product on its own—after all, each has consistently been rated among the top devices in its category. But because these devices are designed to work together, they offer benefits that go beyond the unique functionality that each offers individually. Their ability to communicate interactively, regardless of location, makes the network work with you to maximize productivity, mitigate risk, and ensure compliance with regulatory statutes.

Unified Management and Control

One of the biggest drawbacks in running a collection of disparate point products is managing them. Traditionally, in order to deploy a consistent security and performance policy, you have to enable it on one device, then move to the next device in the network and enable it again. Because each device has its own management system—effectively, its own language—the process is inherently time-consuming and prone to errors that can lead to a breach of your network. As the organization becomes more distributed and remote users proliferate, this process gets even more difficult.

All of the products in Juniper Networks Adaptive Threat Management Solutions are designed to be managed by a single system. NSM is a robust solution that has developed over decades to be a rock solid, easy-to-use platform for you to build on. Policies can be built once and pushed across the distributed network, enhancing consistency, raising overall security, improving user experience, and reducing human error. In addition, IT staff only needs to learn one management platform to manage the entire solution. The result is a demonstrable reduction in operations costs, freeing you and your staff from day-to-day maintenance so that you can focus on higher priority tasks.

High-Performance Security

In networking, there has been an historic trade-off between performance and security. If a network runs fast, the security devices may not be able to keep up, rendering the investment you've made in “bigger pipes” moot. With Juniper Networks Adaptive Threat Management Solutions, you have security products that move as fast as the rest of your network.

One example of the way Juniper Networks combines security and performance is the new WX Client, which can be dynamically provisioned with SA Series SSL VPN Appliances. Now users can enjoy both the performance and the security they need while working remotely. Another example is the family of SRX Series Services Gateways, which provides a host of standards-based security features from the branch to the data center. The SRX Series can be deployed as an enforcement point for the Unified Access Control solution and can also be deployed with full IPS capabilities.

All devices in Juniper Networks Adaptive Threat Management Solutions are built to scale and have been deployed in the world's most demanding enterprise and service provider networks.

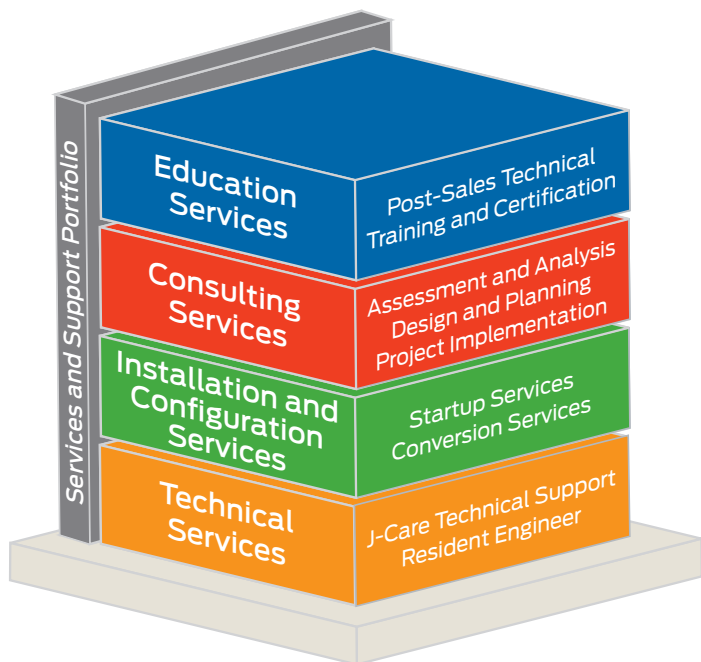
Visibility and Control

You cannot control what you cannot see. Juniper offers comprehensive and innovative centralized management, monitoring, and reporting capabilities with its STRM Series and NSM devices. Juniper Networks Adaptive Threat Management Solutions offer exceptional visibility and support for previously deployed third-party devices, giving you the freedom to select new or build on existing products that are right for you.

Moreover, IT departments gain a network-wide view for monitoring, trending, and reporting. The cooperative approach between security and performance products that make up Juniper Networks Adaptive Threat Management Solutions enable IPS inspection, anomaly detection, application inspection and application delivery all correlated to the user and the relevant user group. In combination with the SA Series and UAC Host Checker capability, along with new proactive antimalware detection, firewall inspection, and reporting by the STRM Series, Juniper Networks Adaptive Threat Management Solutions protect both managed and unmanaged devices. Sophisticated correlation methods can uncover the true attacks that can bring down the business, while reducing performance bottlenecks, and false positives that can needlessly waste IT time.

Solution Planning, Implementation, and Deployment

Juniper Networks offers performance-enabling services that accelerate, extend, and optimize your deployment of Juniper Networks Adaptive Threat Management Solutions. Leveraging Juniper's cooperative product portfolio and network-wide visibility, Juniper can help you use these solutions to manage risks, control costs, fuel growth, and improve operations at every phase of your network lifecycle.



Education Services

Improve the productivity and self-sufficiency of your technical staff

Consulting Services

Accelerate your network's value with expert assistance

Installation and Configuration Services

Start your high-performance, high-value network rapidly, confidently

Technical Support

Protect your high-performance business investment through operational assistance

- **Accelerate** adaptive threat management for your business with Juniper services.
 - Quickly align your IT staff with your business requirements to improve workforce productivity
 - Accelerate the deployment of your adaptive threat management solution by leveraging Juniper experts to augment your staff
- **Extend** the capabilities of your solution with Juniper services.
 - Extend your network and security infrastructure reach to maximize Juniper's product features and capabilities
 - Ensure business continuity and protect assets against internal and external threats
 - Support new capabilities and requirements while securely adding new applications and users
- **Optimize** your business and technical goals by reducing TCO (CapEx and OpEx) with innovative Juniper services.
 - Simplify operations by streamlining security infrastructures
 - Improve operating expenses by leveraging automation features for improved uptime
 - Improve risk mitigation

Financing

The Juniper Financing Advantage, provided by IBM Global Financing, provides qualified customers with flexible financing at competitive rates, enabling lower TCO, higher risk mitigation, and the ability to affordably acquire the total solution, including Juniper hardware, software, and services—through a single contract.

To take advantage of special offers and learn more, visit www.juniper.net/us/en/how-to-buy/financing-advantage/.

Summary: Ensuring the Security of Your High-Performance Network

Juniper Networks Adaptive Threat Management Solutions provide network-wide visibility and control to address the constantly evolving security and performance landscape. Business benefits include proactive risk mitigation, higher business agility, greater IT and employee productivity, and lower TCO. IT benefits include fewer network disruptions and IT resources freed from mundane tasks to deal with more strategic issues. As threats and business requirements change, Juniper Networks Adaptive Threat Management Solutions will continue to adapt to ensure proactive protection, application delivery, and compliance. To learn more about Juniper Networks Adaptive Threat Management Solutions, contact your Juniper Networks representative for more information. Additional information can be found at www.juniper.net/adapt.

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.

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

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

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. Junos is a trademark of Juniper Networks, Inc. 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.

 Printed on recycled paper