IT and security personnel are challenged to establish and maintain maximum security while supporting huge increases in workloads and minimizing impact of attacks on their networks. The need to handle higher data volumes and transaction speeds is constantly growing. Meanwhile, the proliferation of cloud, social, mobile, and big data requires simpler, smarter protection from threats.

The costs of failure are high. A Juniper-sponsored Ponemon study reveals the average cost of a data breach is now $12 million. Few organizations can easily absorb that kind of financial impact to their bottom line.

And it doesn’t stop there. The Verizon 2015 Data Breach Investigations Report shows that the threat is not only clear and immediate, it’s only going to get worse (see Figure 1).

In the midst of these escalating threats, the data center—with its increasingly central role in the organization—is more vulnerable than any other place in the network.

This solution brief discusses the security threats that businesses are facing in the data center, the consequences of substandard or nonexistent security measures, and the primary solutions to these problems.

**Challenge**
Growing data volumes, an escalating threat landscape, demands for microsecond network latencies, and costly data breaches pose a serious threat to business prosperity and reputation. Meanwhile, the proliferation of cloud, social, mobile, and big data requires simpler, smarter protection from threats.

**Solution**
Juniper Networks SRX5000 line of services gateways features next-generation security platforms that deliver the industry’s highest performance and most resilient solutions for protecting data centers and service provider networks across all sectors.

**Benefits**

- Comprehensive security services and open policy enforcement protect businesses against a multitude of threats.
- Designed for physical and virtual environments to provide private and hybrid cloud security capabilities.
- Scalable hardware and software design featuring custom silicon enables throughput in excess of 2 Tbps.
- Pay-as-you-grow flexibility combines business excellence and investment protection with affordability.

Source: Verizon 2015 Data Breach Investigations Report

Figure 1: Data threat and breach statistics
The Challenge

In a world where e-commerce is rapidly replacing traditional brick and mortar stores, today’s businesses must either run entirely online or offer numerous customer-facing assets and Web applications to remain competitive. Forrester predicts that e-commerce in the U.S. will experience a 9.5% compound annual growth rate (CAGR) over the next several years, reaching $414 billion in online sales by 2018—representing a full 11% of total retail sales. At the same time, the Internet of Things (IoT) is opening up new opportunities to enhance operations and provide new services. Gartner forecasts the number of devices connected to the IoT growing from 4.9 billion in 2015 to 25 billion in 2020.

The accompanying growth in network traffic will severely strain existing network security measures, degrading organizational effectiveness and introducing entirely new security risks.

Low-Latency Demands

Predictable network speed isn’t just about consistent throughput. It’s also about predictably low latency. Most business enterprise networks run a variety of applications; some require deep Layer 7 inspection while others must be transacted at high speeds and with ultra-low latency.

Security cannot be compromised in either instance. In individual wire-speed network transactions, microseconds count. High or variable latency is unacceptable for many financial data centers. Regulatory drivers put downward pressure on transaction revenue, and every nanosecond counts in trading; high application response times directly impact trading revenue and are therefore unacceptable. With the move to mobility, financial firms must be even more resilient, offering higher speeds and more secure networks that will enable 24/7 trading. Security solutions deployed in these and other mission-critical networks must be able to secure both normal and latency-sensitive traffic with six-nines of reliability—without compromising the required security posture for either traffic type, and without introducing latency.

For example, high frequency financial trading requires software-driven transactions measured in millions of a second. Algorithms use tick-by-tick data processing and small changes in the price quote streams to trigger trades. These transactions depend on minimal latency and jitter for top speed and efficiency; downtime is not an option, and mean time between failures (MTBF) must be as high as possible for all components within the system, including firewalls.

Securing Against Known and Unknown Attacks

In the battle against hackers and malware, traditional firewall services deliver effective protection against signature-based application-borne attacks. However, a new wave of more dangerous cyber menaces—such as advanced persistent threats (APTs)—requires a different, nontraditional type of defense that can capture threat data as it becomes available and deliver it in the form of actionable intelligence to the firewall enforcement point. Enterprises today face a daunting task, trying to make sense of the numerous disparate tools that provide access to threat data. Ultimately, however, the lack of quality actionable data leaves security staff unsure whether they have adequate network security in place.

In fact, a recent Juniper-sponsored RAND survey of CISOs at leading companies found that hackers are constantly developing countermeasures that limit the effectiveness of existing security tools, requiring companies to keep investing in new tools that increase training and operational costs. Fortunately, not all tools are vulnerable to compromise; the RAND study found that technologies focused on automation and firewall policy enforcement across the corporate network provided a significant ROI and should be prioritized, as they were less prone to hacking countermeasures.
Consequences of Ineffective Network Security
As traffic and data volumes grow, network security performance and resiliency become critical to the business. A lack of reliable network protection can damage corporations in several ways:

- Businesses become more vulnerable to malware and denial-of-service (DoS) attacks, reducing their ability to compete effectively.
- The end-user experience is negatively affected if applications or systems are unavailable due to an attack, resulting in lost productivity, revenue, and reputation.
- Network outages degrade operational effectiveness, diverting resources from where they are needed most.
- Potentially significant financial losses resulting from financial fraud and/or theft of sensitive data can do irreparable harm.
- Solutions that do not scale to deployment needs or are unable to deliver security at network speed can directly impact business agility.

Resolving Technical and Business Issues
A data center security solution must perform three vital functions:

- Stop all types of attacks (internal and external) with comprehensive security efficacy
- Deliver maximum performance and scale to adapt to growing needs, ensuring that network and applications are always available to optimize user experience and business agility
- Enable unified, consistent security policy from a single point of control for ease of management, network-wide visibility, and operational efficiency

“"At MCB Bank, our business is our customers and we value ourselves on delivering a high-performance, reliable and, most importantly, a secure network with continued uptime. By implementing the SRX Series Services Gateways in our data center, we can protect our customers’ sensitive data from threats while continuing to deliver new services with security and more quickly, resulting in optimization of operations and simplifying the management of our systems.”

- Imtiaz Mahmood, Chief Information Officer, MCB Bank

The SRX5000 Data Center Security Platform
The Juniper Networks® SRX5000 line of services gateways has been purpose-built to accommodate capacity and performance increases, helping businesses keep pace with modern data center growth and change. These advanced, resilient, and extremely high-performance firewalls deliver several key benefits:

- Unparalleled protection against advanced threats
- Market-leading performance and scale that meets network demands
- Six-nines of reliability and availability, resulting in virtually no downtime
- A rich set of automation capabilities to automate firewall repetitive tasks, reduce human error and enhance operational efficiency
- Centralized management for consistent policy enforcement and visibility across physical and virtual assets
- Investment protection by allowing customers to mix and match hardware and software features to suit their needs for scale, as well as “pay as you grow” flexibility

Comprehensive Protection for Different Types of Data Centers
The SRX5000 line delivers secure and resilient protection for a variety of data center scenarios spanning enterprises and service providers. Offering a next-generation firewall, integrated threat intelligence, and advanced intrusion prevention services coupled with maximum throughput, scalability, and in-service software and hardware upgrades, the SRX5000 line more than meets the needs of data centers engaged in a variety of critical operations. These include high-performance computing, content service delivery, enterprise IT, transactional services, hybrid environments that combine physical and virtual resources, and any modern data center with customer-facing Web 2.0 applications and revenue-generating assets.

Unique SRX Series Features for Critical High-End Security
To optimize business benefits, the SRX5000 line has been designed and developed for clear differentiation from other networking security alternatives. The SRX5000 line features the following unique attributes:

- **Next-generation firewall:** The SRX5000 line services gateways include AppSecure with AppID 2.0, providing application visibility and control while delivering strong protection against L2-L7 threats via user-based policies, threat remediation, and comprehensive event correlation, logging, and tracking. Juniper’s signature engine is also open, allowing customers to view, edit, and create their own signatures.
- **Open threat intelligence platform:** Featuring Spotlight Secure integration, the SRX5000 line is the industry’s first open threat intelligence platform that integrates...
feeds from Juniper, customer and third-party sources to protect against cybercrime, botnets, GeoIP location-based threats, advanced malware, and APTs. Administrators can define and dynamically enforce threat policies via Juniper Networks Junos® Space Security Director, the centralized management system for the SRX Series.

- **Express Path**: The Express Path software optimization capability securely optimizes SRX Series performance and dramatically improves throughput and latency by identifying and fast-pathing traffic flows that do not require additional inspection or deep processing. Juniper’s next-generation input/output line cards (IOCs) for the SRX5000 line, including the IOC2 and the IOC3, support the Express Path software.

- **Very high capacity flows**: The SRX5000 line supports single, extremely high-bandwidth flows of 40 Gbps and 100 Gbps. Highly valued in high-performance computing and science DMZ environments, this unique capability dramatically increases the amount of secured traffic that can be exchanged for express downloads and frequent data transfers.

- **Industry-leading throughput**: Juniper leverages its custom silicon and hardware along with software innovation to achieve dramatic performance results. Unlike any other platform in the industry, the SRX5800 Services Gateway delivers a highly resilient 2 Tbps network firewall with shared state and full high availability.

- **High-density interfaces**: Each IOC3 line card supports two Packet Forwarding Engines (PFEs) and a high-density configuration of 2x100GbE and 4x10GbE high-speed interfaces.

- **Superlative reliability**: Boasting less than 14 seconds of downtime per year, independently verified by Telcordia, the six-nines reliability of the SRX5000 line ensures business continuity and application availability.

- **Robust scalability**: Easily handles up to 100 million concurrent sessions.

- **Separate data and control plane architecture**: Multiple processing cores enable administrators to maintain access to the system even in the face of an attack.

**SRX Series Delivers Business Solutions**

Juniper’s technological leadership in networking security technologies addresses clear business needs:

- **Best-in-class threat protection**: Strong, high-performance network security solution delivers high quality, actionable threat protection against a broad spectrum of malware and cyber threats. The SRX5000 line integrates seamlessly with virtual environments to create an ideal solution for hybrid data centers and address the fundamental need for a unified view of deployed physical and virtual security infrastructure.

- **Optimal network performance**: Express Path is a software optimization capability that ensures optimal speed for certain (customer-specified) traffic. Active session flows are identified and prioritized to receive appropriate security treatment based on whether they are low-latency flows or normal traffic. Dynamic selection of the traffic to be fast-patched to IOC hardware guarantees optimal network performance, without compromising network security. The SRX5000 line is the industry's first security platform for combating threats at wireline speeds.

---

**SRX Series Advanced Services**

**Next-Generation Firewall Services**
- Application Control
- Intrusion Prevention
- User-Based Firewall

**Unified Threat Management**
- Antivirus
- Web/Content Filtering
- Anti-Spam

**Threat Intelligence**
- Command and Control
- GeoIP Feeds
- Custom Feeds

**SRX Series Foundation**
- Firewall
- VPN
- NAT
- Routing
- Management
- Reporting
- Analytics
- Automation

**Figure 4: SRX Series network security services**
• **Rich automation:** Juniper’s market-leading solution automates network and security functions, utilizing automation tools such as Juniper Networks Junos operating system scripting and NetConf to speed up repetitive tasks such as firewall configuration, management, and event response. This enables more user-friendly firewall management, reduces human error, improves staff efficiency, and simplifies operations—dramatically reducing outage time and related costs. In particular, it results in significant OpEx savings. The SRX Series open XML API supports integration with leading automation tools, such as Puppet, Chef, Ansible, and other NetOps and SecOps tools.

• **High resiliency and availability:** The separation of control and data planes is a key architectural design feature in the SRX5000 line, enabling access to the system even when it is under attack. This allows for attacks to be controlled and mitigated while the network stays up, providing peace of mind to security personnel that they have not disrupted operations. Further, the six-nines resiliency of the SRX5000 platforms ensures that the system will continue to run year after year with virtually no downtime.

• **Investment protection:** Unlike most other platforms, the SRX5000 line of services gateways comes with all advanced security services already included with the system, ready to be turned on when needed through a simple activation license. No additional hardware or software is required, reducing complexity. As needs change, services can be turned on without delay, eliminating the need to pay upfront for services that are not yet required.

• **Premium support services:** A combination of advanced services that mitigate tasks, reduce learning curves, and accelerate time to value keeps networks in a state of optimum readiness.

“Juniper is focused on delivering high-performance security services that provide for rapid network scale. (The) SRX (Series) is also built to optimize productivity in a highly available, always-on cluster with easy, secure access. ESG Lab recently tested the latest release of the Juniper SRX5400, and found that it offered an architectural approach, next-generation IOCs and SPCs, and Express Path for performance, scale, and security efficacy. This makes the SRX5400 a good candidate for organizations considering a next-generation data center firewall with strict performance requirements for throughput and latency.”

- Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group

---

**Figure 5:** Separate Data Plane and Control Plane Architecture of SRX Series
SRX Series Features and Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive Security</td>
<td>Real-time Threat Elimination, Next-Generation Firewall, IPS, UTM, 3rd Party and Customer Feeds</td>
</tr>
<tr>
<td>Operational Efficiency</td>
<td>Consolidation of Services, Rich Automation, Open and Programmable, Six-Nines Reliability</td>
</tr>
<tr>
<td>High Performance</td>
<td>Express Path, 2 Tbps Throughput, Very High Bandwidth Flows, Low Latency</td>
</tr>
<tr>
<td>Business Agility</td>
<td>Industry-Leading Scalability, Avoid Rip and Replace, Pay-As-You-Grow</td>
</tr>
</tbody>
</table>

Figure 6: SRX Series Services Gateways features and business benefits

“As a leading provider of cloud solutions in the UK, we needed a cutting edge security solution to help us deliver on our promise to partners and customers that we provide 99.9999 percent service availability. Through our partnership with Hardware Group and by leveraging Juniper Networks SRX5000 Services Gateways, we are supplying the high performance and intelligent security solution required to keep up with our resilient, scalable, and flexible cloud services. With the SRX Series, we have the maximum level of defense for high-speed networks and protection against all levels of attacks.”

- Piers Linney, Co-CEO and Founder, Outsourcery

Summary—Juniper Offers the Highest Performing Security Platforms for Data Centers

As cybercrime is becoming more pervasive, enterprises and service providers increasingly face the same serious issues when it comes to protecting their valuable network assets. The evolving data climate is fueling an essential need for top-tier firewall protection with excellent performance and superior efficacy.

The SRX5000 line has been designed from the ground up to help businesses stay on top of their performance and scalability requirements while maintaining effective and comprehensive network security. The innovative Juniper Networks SRX Series Services Gateways empower business agility and cost effectiveness and give customers a market-leading security platform now and into the future.

Next Steps

Contact a Juniper representative today to discuss how you can properly respond to modern data center threats. A variety of SRX Series solutions and configurations are available to meet your unique business needs. For these reasons, Juniper emphasizes a nuanced and personal approach to deliver the ideal service and environment for each individual enterprise and organization.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.