

THE EVOLVING THREAT LANDSCAPE

Where the Key Security Battles Are Taking Place Today—
and Essential Strategies for Winning Them

Table of Contents

Executive Summary	3
Today's Shifting Threat Landscape	3
The Sophisticated Cybercriminal	3
The Threat from Within	3
Security's Evolving and Expanding Battle Fronts	3
The Enterprise's Strategic Security Imperatives	5
Security Functions	5
Multilayer Intelligence	5
Diverse OS and Device Type Support	6
Juniper Networks—Complete Solutions for Dynamic Threats and Environments	6
Juniper Solutions	6
The Juniper Advantage	7
Conclusion	7
About Juniper Networks	7

Executive Summary

Today's enterprise is under attack. Network-based threats are continually increasing in breadth, volume, and sophistication and represent an existential risk to organizations around the globe. This paper surveys emerging threats, profiles their highly organized perpetrators, and reviews some of the revolutionary technologies that make these attacks so persistent and effective. Finally, it reviews their implications to enterprise security organizations, revealing the critical "new network" elements necessary to defend against these evolving threats, prevent attacks, preserve sensitive assets, and maintain business continuity.

Introduction—Today's Shifting Threat Landscape

The Sophisticated Cybercriminal

The prototypical cybercriminal is no longer the student defacing a website from a personal computer for amusement and notoriety. Today's stakes and spoils are greater, attracting highly paid professionals working within a web of technology suppliers, career hackers, and legacy crime organizations.

At the top of the food chain are most often criminal organizations that profit directly from theft and sale of sensitive data. Instead of operating software development organizations themselves, these criminal organizations easily and inexpensively procure technology from crimeware vendors in order to accelerate their "time to crime." The technical and organizational sophistication of these independent software vendors (ISVs) often rivals and mimics modern enterprise software organizations. And like any business, their economic survival depends on the timely delivery of increasingly effective software in the race to win customers and profit from evermore innovative, persistent, advanced, and rewarding attacks.

There is certainly more to steal. Today's enterprise has become increasingly "target rich," as more valuable information is being stored on network accessible devices and services every day. Historically, enterprises have focused on securing sensitive customer data such as consumer credit card information, and these remain targets. But as the market for and the value of information increases, so do the available targets. Emails, CAD drawings, human resources (HR) and other records are now opportunistically targeted as well. If information has value to the enterprise or an individual, it most certainly has value to a cybercriminal.

That said, one can't assume that attacks are motivated by opportunistic criminals alone. The most innovative attacks often originate from intelligence or clandestine nongovernmental organizations whose interest is to further a political agenda or cause. Advanced Persistent Threat (APT), an ongoing, sophisticated, and strategic attempt to infiltrate a specific (rather than opportunistic) target, represents a new type of warfare waged among competing companies, countries, or political agents.

Their intentions are no less destructive. In 2010 StuxNet laid in wait for months, recorded normal system behavior and played it back to the management interface covering simultaneous attempts to destroy them, all in the targeted effort to impede Iran's nuclear ambitions.

Botnets, remotely controlled global networks of compromised computers, are among the latest technologies for both opportunistic and APT attacks. Especially difficult to detect, they are also extremely effective in perpetrating fraud and other malicious activity because they can leverage virtually limitless resources. Botnets currently control millions of personal computers around the world, which can be summoned as a kind of malicious software as a service (SaaS). Also in 2010, for example, clandestine supporters quickly mounted highly effective global denial-of-service (DoS) attacks to effectively shut down specific payment and government websites that opposed WikiLeaks for several well publicized days.

During the second quarter of 2010, botnets controlled almost 2.2 million computers in the US, representing 5.2 percent of every 1,000 PCs.

—Source: Microsoft, "Security Intelligence Report", Volume 9

Web 2.0: Blurred Boundaries, Clear Threats

Advanced attacks and botnet threats aren't the only things that information security personnel need to be aware of. In the enterprise and consumer domains, the Internet has ushered in an entirely new computing paradigm whose security implications are being felt in the enterprise. The traditional organization, and the very concept of having a definable, protectable perimeter, has literally been bypassed and blown away. Today, in addition to internal server farms and infrastructure, enterprises increasingly rely on infrastructure services delivered by SaaS, platform as a service (PaaS), and infrastructure as a service (IaaS) providers that extend "data center" borders. This is in addition to the many external vendors that are relied upon for a host of critical business functions such as accounts payable, product support, and sales management. Branch and home offices, laptop computers, and, increasingly, smart mobile devices constantly redefine physical enterprise boundaries. Finally, social networks have become a core means for both personal and business communications—and completely blur the line between the enterprise and the outside world in the process. With traditional borders bypassed in so many ways, security vulnerabilities are exposed, data privacy is compromised, and operational continuity can be more easily broken.

If that weren't enough, enterprise security teams must quickly grapple with a host of other issues that reduce visibility and control:

- **One Web, many uses.** Web-based applications have changed the dynamics of security. In the past, specific applications would be associated with specific protocols and ports, and setting and enforcing policies at the host were relatively straightforward. Now, given the reliance on Web applications, virtually all traffic is HTTP-based (ports 80/443). Consequently, network security solutions operating solely on basic IP layer information are unable to distinguish between permitted and malicious activity. Even more, the very advantage of Web applications—the fact that they can be accessed from anywhere by employees, contractors, partners, and service providers through the firewall—creates its own set of access control challenges.
- **Virtualization.** The virtualized nature of public clouds, private clouds, and on premise virtualized systems have ushered in an environment in which a given data set or process can dynamically migrate across networks, data centers, and physical machines—presenting a host of challenges for traditional, machine-based security mechanisms. While specific subsystems may remain secure, the increasingly interrelated nature of virtualized environments increases complexity, reduces visibility, and leaves vulnerabilities unchecked.

The Shifting Battlefield (Client and Mobility)

The evolving game of cat and mouse between security teams and criminals constantly changes the field of battle. In recent years, businesses have invested in a host of mechanisms to shore up the security of their core infrastructure. This has led to several countermoves from criminals. As strengthened security at the operating system level was implemented, application focused attacks increased. As security teams have shored up server protections, criminals have shifted to exploiting client systems. And as packet data has become less accessible because of encrypted communications (SSL/VPN), files and file readers have become the new focus. Office software, PDF viewers, and Web video players, for example, are all targets because of their popularity and complexity, and because their size allows them to harbor complex document-based malware unnoticed. One sophisticated attack called Operation Aurora, for example, exploits a browser vulnerability to compromise client PCs and gain access to local and remote file systems. Similar exploits of enterprise connected mobile smartphones are surely on the horizon.

Six of the ten most common vulnerabilities found were in Microsoft products. Roughly fifty percent of all exploits take advantage of vulnerabilities in Adobe programs.

—Source: Kaspersky Labs, "Information Security Threats in the First Quarter of 2010"

As targets become more decentralized, security teams face a host of critical challenges:

- Limited resources and exploding complexity. In the past, where a security engineer may have been responsible for the management of a handful of physical servers, now that same individual may be responsible for thousands of physical and virtualized machines. Further, as attacks focus on clients, these numbers grow even more daunting. For every server in an enterprise, there may be hundreds of end user devices. Attackers typically go after the easiest targets. However, though the focus of attacks has shifted over the years—moving from networks, to servers, to desktops, and now to mobile devices—security teams can't afford to ignore any potential risk area.
- Diverse user profiles and policies. When compared to securing servers—which typically have a limited set of policies, protocols, and applications—securing clients is an entirely different matter. Where in the past, a single, company-furnished desktop was the norm, now a single employee may use a smartphone, laptop, and home desktop for a broad range of business tasks. Where in the past, there may have been a handful of user profiles, now the combinations of applications, devices, and usage scenarios are virtually limitless. As a result, centralized, corporate, security-driven policies and standards are increasingly difficult to enforce. For example, while it may be practical and cost-effective to encrypt sensitive assets on a corporate server-based content management application, encrypting those same assets as they are stored and used by disparate end user devices is far more complex and costly.
- Device and OS proliferation. Security teams must contend with an array of platforms—including mobile devices running Symbian, Android, Blackberry, and Apple's iOS, as well as desktops and laptops running the Mac OS and several flavors of Microsoft Windows and Linux. This diversity has pros and cons from a security standpoint. In the past, it was the homogeneous nature of the enterprise computing environment that helped attacks widely succeed. In other words, one attack could potentially inflict damage on virtually every PC in an enterprise. Having a diverse set of clients means that a smaller set of devices may be susceptible to any given attack. However, for the security teams responsible for securing these diverse client platforms, this proliferation of devices and operating systems makes the process of enforcing security policies and implementing security technologies and upgrades much more complex.
- Inadequate security on mobile devices. While laptops typically have mature, effective security mechanisms installed, smartphones and tablets typically don't have any security safeguards in place. Further, the use of roaming mobile devices means that static, network-centric security policies no longer suffice.

Between 2009 and 2010, there was a reported increase in mobile device threats of 250%.

—Source: Juniper Junos Pulse Mobile Security Suite virus definition database

The Enterprise's Strategic Security Imperatives

In today's highly distributed cloud and virtualized environments, network performance and security are critical for business performance and continuity. If an enterprise's network is susceptible to distributed DoS attacks, it poses potentially existential business risk to the business and all of its stakeholders. For many enterprises, a network outage may not only compromise email communications, but employee access to SaaS-based CRM applications and an IaaS hosted ERP system, reseller access to online ordering and fulfillment applications, an outsourced call center's access to customer purchase histories, and much more. Consequently, network scalability and reliability are vital security and business mandates.

To adapt to these new realities, enterprises need to fundamentally transform their security approaches. Now more than ever, a defense in depth approach is required. No single technology, whether encryption, firewalls, application security, or intrusion prevention can effectively guard all of an enterprise's assets. To guard today's dynamic IT environments against the new threat paradigms such as APTs and sophisticated crimeware, organizations need broad coordination across all networking and security functions.

Security Functions

Given their multilayer, quickly evolving and dynamic IT infrastructures, and the many security threats in play, enterprises need an integrated platform that offers a centralized means to view and manage all vital security functions, including firewalls, VPNs, intrusion prevention systems (IPS), and antivirus scanners. The more comprehensive a platform, the more ably it supports consistency in administration, policy enforcement, event management, and more. Further, as threats evolve, security platforms must easily accommodate new security services and protections delivered through open standards, so that they can be quickly integrated with new sensors and security capabilities as exploits become known.

Multilayer Intelligence

Security teams need to take a cohesive, centralized approach that encompasses the client, network, server, and other elements within the IT infrastructure. All of these layers need to be integrated in order to ensure optimal performance and security. Further, trying to manage all of these efforts in a disparate, ad hoc fashion results in administrative complexity and high operational and capital expenditures, and reduces the robustness of the network. Thus, integrating the management of these disparate elements makes business sense as well.

To achieve these objectives, security teams need:

- Enterprise security controls that transcend the data center and protect at the client level
- IPS integration deep into the network operating system that delivers high-performance, unassailable protection at the network edge, network core, branch office, hypervisor, and more
- Application-level awareness and control to enforce security policies that are application (not port) centric
- Technologies that identify threats to the virtual infrastructure to provide visibility into traffic between VMs to ensure the security of all virtual devices

Diverse Element Support

Security should be applied across the broadest range of devices, including disparate laptop and mobile device operating systems, and should be integrated with security at the server and network level. By employing more security measures centrally rather than at the device level, an organization can simultaneously streamline and improve policy enforcement. The less security that is managed on the actual device, the less susceptible it is to attack.

Juniper Networks—Complete Solutions for Dynamic Threats and Environments

With its “new network” security solutions, expertise, and vision, Juniper Networks is uniquely equipped to support an enterprise’s near-term and long-term security objectives. Juniper offers a truly unified platform for networking and security. To support an enterprise’s defense-in-depth initiatives, Juniper delivers a comprehensive security architecture that encompasses clients, servers, networks, storage systems, and virtual environments. In addition to its investments in each of these areas, Juniper offers open interfaces and platforms that allow customers and partners to integrate and innovate with its products.

Juniper offers the following integrated, comprehensive capabilities:

- Pervasive security that integrates IPS capabilities into the network operating system, making it available everywhere—at the network edge, network core, branch office, and more
- Software development kits and support for open standards, such as Interface to Metadata Access Point (IF-MAP) that enable broad integration and rapid addition of new sensors and capabilities
- Mobile security, featuring unified, comprehensive support of a host of mobile platforms and operating systems, including Symbian, Blackberry, Apple iOS, and more.
- Virtualization support, delivering scalable, end-to-end security services across the device, network, application, and hypervisor

Juniper Solutions

Juniper security solutions are built upon Juniper Networks® SRX Series Services Gateways, which provide the essential capabilities necessary to connect, secure, and manage enterprise and service provider networks. By consolidating switching, routing, and security services into a single device, organizations can economically create new applications and services, secure connectivity, and deliver quality end user experiences. All SRX Series Services Gateways are powered by the industry renowned Juniper Networks Junos® operating system, which provides superior availability, performance, and infrastructure protection, while reducing total cost of ownership.

AppSecure

AppSecure is a suite of next-generation security capabilities for SRX Series gateways. AppSecure employs advanced application identification and classification to deliver greater visibility, control, and protection over the network. Working in conjunction with the other security services of the SRX Series, AppSecure provides a deep understanding of application behaviors and weaknesses to prevent application-borne threats that are otherwise difficult to detect, let alone stop. AppSecure has the intelligence required to distinguish among the volume of traffic that now tunnels through HTTP.

Unified Access Control

Juniper Networks Unified Access Control is a standards-based, scalable network access control solution that reduces network threat exposure and mitigates risks. UAC protects networks by guarding mission critical applications and sensitive data, identity enabling network security, and providing comprehensive control, visibility, and monitoring.

Junos Pulse Client

Juniper Networks Junos Pulse is an integrated, multiservice network client that provides dynamic connectivity, security, and application acceleration through mobile or non-mobile devices, including smartphones, while requiring little or no user interaction. Junos Pulse leverages identity and location awareness, and seamlessly migrates from one access method and policy to another based on device location. With Junos Pulse, enterprises can support the disparate devices and operating systems now in use—so that they can optimize end user productivity, regardless of location, while at the same time strengthening security.

SSL VPN

Juniper Networks SA Series SSL VPN Appliances secure employee and partner remote access with market-leading platforms, as well as capabilities for accelerating applications and dynamically downloading anti-spyware.

The Juniper Advantage

Juniper offers today's enterprises a host of unparalleled advantages:

- **Continuous, complete security.** Through its integrated intelligence of networking and security, Juniper enables customers to strengthen security—from the data center to all clients, and all points in between.
- **Strengthened network performance.** By integrating network and security intelligence in a unified fashion, businesses can optimize security, network performance, and thus business performance. Juniper enables customers to combine intelligence from networks, applications, and access control to make quality of service (QoS) and security refinements.
- **Agility to respond to changing business and security needs.** Through its open standards support and dynamic, pervasive network and security intelligence, Juniper enables customers to stay in front of evolving security threats, while retaining the agility they need to adapt to evolving cloud services and business opportunities.

Conclusion

Enterprise security teams need to contend with threats from increasingly sophisticated and well funded cybercriminals, while the very infrastructure they are chartered with protecting goes through fundamental paradigm shifts. To address these challenges and secure “the new network,” organizations need capabilities that ensure persistent security, while enabling continued evolution in IT. Juniper uniquely addresses these needs, delivering a comprehensive, unified security architecture that encompasses devices, servers, networks, storage systems, and virtual environments.

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.

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

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

Copyright 2011 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.