NETWORKS THAT KNOW SECURITY

EBOOK

SECURITY

Your ideas. Connected.

JUNIPER NETWORKS

Preface

In today's rapidly evolving world, the modern enterprise has the benefit of many technologies that were unheard of just 10 years ago – the cloud, for instance. However, with every new technology – cloud included – there are new security challenges. With huge numbers of users, devices and data deployed to take advantage of the latest technologies, the enterprise is becoming increasingly vulnerable to data loss, malicious attacks and network instability.

In the era of the cloud, the always-on workforce and high levels of digital literacy, your customers, prospects, staff and suppliers expect 24/7 network access and availability. However, 24/7 access is not enough; your data needs protection from any number of potential security breaches. These can happen when data is inside the cloud or when it is in transit. Multiple layers of protection are required to safeguard your information, within physical and virtual environments, from hackers and their various modes of attack. You need a multidimensional approach to minimize the risks you face.

Section 1

KNOW THE LAY OF THE LAND

"USA has a 23% share of the world's malicious computer activity. The highest rate of cybercrime among the world's top 20 countries."

BusinessWeek / Symantec

Today's cybercriminal is more prolific, elusive and unpredictable than ever before. They might be stealing your data, your intellectual property or your identity. They can penetrate your accounts, compromise your data or take down your site. Regardless, their reputation is enhanced and yours could be destroyed.

The channels used by such criminals are commonplace: online stores, forums, email, private chat, open chat rooms – the list goes on. The cybercriminal's reputation within these communities is a huge driver – for both the skilled and non-skilled hacker.

With the advent and popularity of anonymous crypto-currencies, such as Bitcoin, the basic economics lend themselves to more crime, not less. Yes, law enforcement is getting better – after all, bigger targets get more attention. However, media coverage of these high profile attacks can glamorize the practice and attract newcomers to this digital underworld.

The lesson is that our hyper-connected, smart, on-demand environment creates more black market opportunities for digital natives. And they are displaying more creativity and variation in their attacks.

Section 2

KNOW YOUR VULNERABILITIES

"Financially-motivated criminals will naturally seek out data that is easily converted to cash, such as bank information and payment cards, while espionage groups target internal corporate data and trade secrets."

Verizon, 2014 Data Breach Investigations Report

According to Forrester, 46% of businesses plan to increase their security budgets on network defenses during 2014. It's also reported that the focus will be on counter-threat measures, such as intelligence services, wireless security, next-generation firewalls and malware detection. (Source: Understand The State Of Network Security: 2013 To 2014, Forrester Research, Inc., January 6, 2014).

This form of tactical response is hardly surprising when the economics of cybercrime are becoming more and more lucrative for the "actors" involved. Indeed, a recent RAND report, released in association with Juniper Networks, suggests that cybercrime – in some instances – can be more profitable than the black market drug trade. With low barriers to entry, less personal risk and steeper rewards, there's an argument that the incentives to attack will always outpace the ability to defend.

That doomsday scenario could well come true for the unprepared, the under-invested and the misinformed enterprises that are held back by sub-par network, data center and cloud infrastructures. After all, these are the types of organizations that cybercriminals prey upon time and time again. If the economics stack up, why wouldn't they?

"Cyber black markets are a maturing, multi-billion-dollar economy, with robust infrastructure and social organization."

RAND Corporation, Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar

Multiple layers of security must continually be revisited by security professionals. The tendency is to focus on one or two areas for maximum strength, but this can lead to vulnerabilities on other levels. While there tends to be good control at the end point and perimeter firewall, where it's easiest to manage, elsewhere it's a different story.

In the so-called "soft" middle layer—within apps, the network and data center – businesses are often left vulnerable or inert by needless complexity – complexity that is caused by proprietary, legacy systems, tools, policies and non-standard protocols. All of this, of course, causes a real headache for IT security teams as they struggle with the manual labor of dealing with multiple signatures and patches. For the business as a whole, this has a direct bearing on the organization's ability to control costs while improving user productivity and speed of response. Hackers are not only stealing your data and intellectual property, they're stealing your time, your money, your ability to do business – even your reputation.

KNOW YOUR BIGGEST THREATS:

Insiders, hackers and ineffective security solutions

These combined internal and external factors are the core challenges facing the modern enterprise. Rarely do long-term threats to corporate security come from a single, manageable source.

Social, big data, mobility and cloud

These are the Gartner Nexus of Forces which are major future threats to enterprise security. The intersection between social and the business is a key vulnerability, as is data spawn.

End users and end points

These are cybercriminals' entry point to your organization. They will use hostile entities such as packets, URLs, devices, apps and users to find their way in, with email as the most common attack vector.

Ineffective traditional controls

Old-school slow, antivirus and vulnerability signature updates can be ineffective against the ever-changing attack methods of cyber criminals.

Section 3

KNOW YOUR OPPORTUNITIES

Passive defenses such as simply monitoring and/or blocking traffic are important, but are no longer enough. Instead, firms should be looking to deploy a strategy that disrupts the economic benefits of hacking. In short, hitting them where it hurts – in the pocket.

Enterprises that can impose an active defense utilizing proactive blocking techniques are well positioned to make hacking more expensive and time consuming for the intruder. And, in doing so, either deflecting their attentions away from your perimeter or nullifying their behavior entirely.

"Corporates need to look at the actual bang-for-the-buck they are receiving from their IT security systems. They also need to remove the old layers of technology and refresh their security."

Andrew Rose, Forrester Research's Principal Analyst, Security & Risk as quoted in "Forrester report says firms spend 21% of security budget on networks", SC Magazine, January 8, 2014

"The hacker market - once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety - has emerged as a playground of financially driven, highly organized and sophisticated groups."

Juniper Networks

Securing your data centers, edge, and cloud environments is an ongoing challenge. Your adversaries—cyber criminals, nation state attackers, hacktivists—continue to develop sophisticated, invasive techniques, resulting in a continually evolving threat landscape. Traditional firewalls focused on layer 3 and 4 inspection are not sufficient in today's threat environment. Next-gen firewalls are powerful, yet not designed to protect from the velocity and variety of new attacks. In today's world, your firewall must be able to take immediate action based on known or emerging intelligence. It must identify attacks accurately and act quickly.

With the shift to cloud architectures, traditional firewall administration becomes burdensome and fraught with human error due to the sheer complexity of distributed security. What's needed is a firewall that can adapt to emerging threats in near real time, in an automated and dynamic way.

Opportunities/ challenges As you build and manage a traditional or cloud data center, security is a fundamental element. Balancing the need for users to access applications with the need to protect your digital assets is no easy task. Consider some of the follow challenges:

Proprietary and Inflexible Security Platforms—While some firewall solutions leverage cloud-based threat intelligence1, the data involved is often proprietary, preconfigured on the firewall, and inflexible, not allowing you to select nor exert any control over the information provided.

Security Inefficacy—The market is saturated with sources claiming to offer threat intelligence, though most of the available data feeds are not immediately actionable. Your firewall, therefore, is unable to use those data feeds directly within policy, providing less than optimal protection.

Static Address Groups—Administrators typically rely on static address lists to apply inspection or blocking and must manually update the firewall policy every time any of these lists change. This is cumbersome and difficult to maintain.

Firewall Performance—Firewall services, such as IPS and application inspection, tend to lead to dramatic performance reductions. In particular, intelligence data feed entries can quickly add up to the thousands (if not more) on a single firewall device, causing performance issues that can lead to unnecessary upgrades. And, your firewall may not be utilizing threat intelligence in a way that maximizes the firewall's resources.

Decentralized Policy Management—As the number of firewalls increase across your network and you need consistent policies across the firewall estate, a reliable, centralized web-based management solution is critical.

This is just one example of the agility you can get from a high level of security intelligence. The ability to make security decisions on the fly, based on new information, will be a critical defensive weapon against cybercriminals. Knowing other dynamic security information such as updated command and control centers (to defend against botnets), up-to-the-second worm and virus signatures, or customized feeds focused on a company's vertical businesses can all be critical to protecting your business.

Pure-play vendors provide only one part of the solution, meaning businesses tend to have more than “one throat to choke” when it comes to security and networking. As firms ratchet services up and down across multiple environments with more speed than ever before, it’s important to be able to manage multiple security gateways and devices – such as firewalls, routers and switches – using a common platform.

The modern enterprise needs to grow its security as its network grows, ensuring that they have a scalable, next-generation firewall to defend its servers. A firewall that delivers without compromising business continuity. A firewall that can detect threats based on correlation of data using smart analytics. A firewall that can identify attackers and determine the nature of the threat.

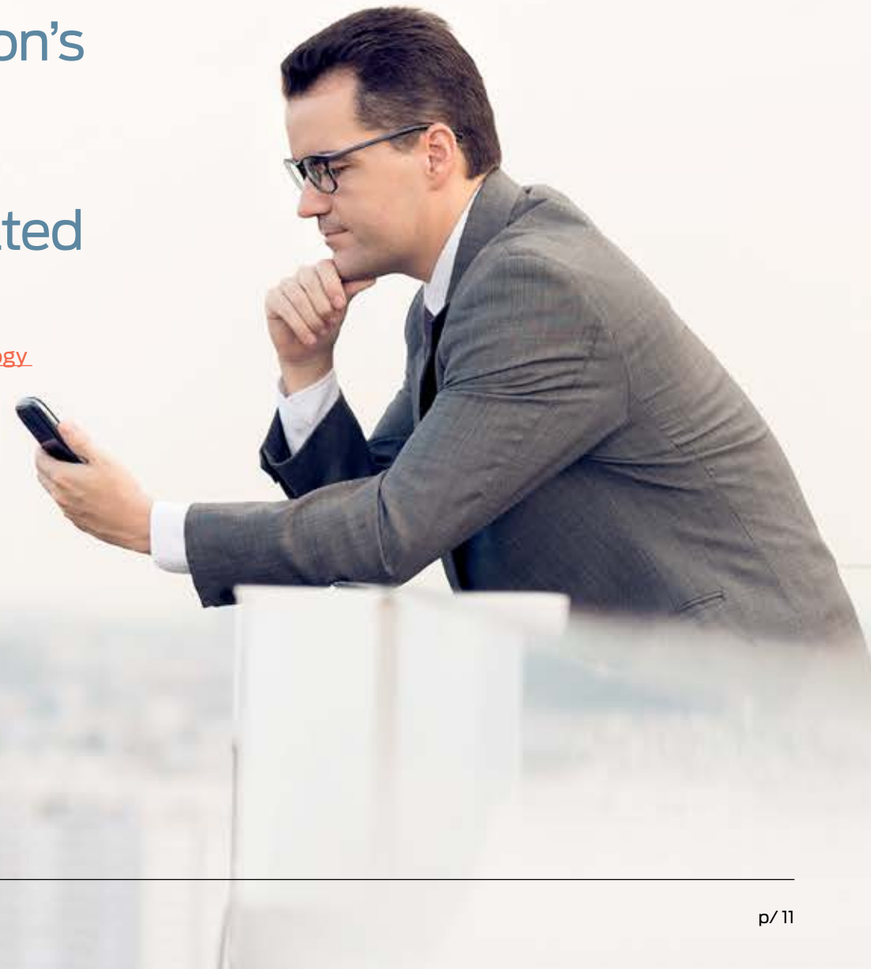
Most of all, firms that are serious about lowering costs and improving business agility need to better understand what their future needs are. Not just put up with a "make do and mend" mentality that holds the business back and opens the door to further security breaches and damaging downtime.

“Within the next year,

22%

of organization’s technology investments will be allocated to security.”

Network World, 2014 Technology Influencer Study



Section 4

KNOW YOUR CHECKLIST

What are the key attributes to look for when building a secure network?

- Reliable and secure hardware using open interfaces and standard protocols
- Ability to protect traffic at high speeds
- Programmable hardware that adapts to changes
- Ability to alter throughput, latency and connectivity
- Layered security in the network, firewall, and application
- Policy management for physical and virtual environments
- One operating system and language across security and network
- Network and security automation through APIs
- High resiliency due to separate data and control pane architecture
- Protection of traditional and virtual workloads
- Ability to add modules to expand security capacity and functionality without rip and replace

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

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