Here, There, and Everywhere

A New Security Paradigm

Regardless of the business you are in, digital transformation is one of the biggest stories of the last decade. With the explosive growth of the Internet has come new ways of connecting consumers to producers, companies to suppliers, citizens to governments, and everyone to information. This trend has accelerated with the introduction of smartphones, geo-localization, and integrated applications creating frictionless interactions. The brutal disappearance of major companies who didn't adapt to this new world has created a compelling board-level incentive for every organization to move rapidly into true digital mode.

The success of the online world has resulted in the parallel creation of a new industrial sector dependent on the digital economy: cyber criminality. As digital assets have become more valuable, they have also become more tempting targets. A database containing millions of credit card numbers can be worth a lot in the wrong hands. So can industrial plans, product specifications, and sales figures. And a new twist has reared its ugly head with the advent of untraceable payment systems like bitcoin: blackmail using ransomware.

The days are long gone when lone hackers working in bedrooms and garages wrote viruses and broke into computers just for the fun of it. Organized crime syndicates are now monetizing attacks, breaches, and even the tools that hackers need to commit their break-ins.

IT's Impossible Digital Conundrum

As an IT professional, you are in the midst of a whirlwind of competing pressures from internal and external stakeholders. You are expected to provide the environments and platforms that generate the dynamism and agility to pursue new commercial opportunities, enable new revenue streams, and build new collaborations, paving the way for creative, disruptive business models. You are constantly faced with pressure to make business flow smoothly in all areas: applications, connectivity, ease of use, and openness. But at the same time you are responsible for ensuring that it all happens securely. Management, regulators, and customers agree: no data breaches allowed.

Considering that every year hundreds of millions of new pieces of malware are seen, and with new horror stories appearing every week, it can sometimes seem like cybercriminals have the upper hand these days. And they have so many different tools: viruses, worms, trojans, spoofing, phishing, spear phishing, just to name a few. And they can unleash them in so many ways: infected websites, e-mails, images, social media, social hacking, USB sticks, advanced persistent threats, and compromised personal devices. How do you cope? If you "lock down" everything online, you run the risk of choking off the very speed, agility, openness, and dynamism that your organization is looking for in its digital transformation.

Many methods are now used to protect digital assets. Traditionally, firewalls were the first line of defense. We put them at the entrance to the network. The so-called perimeter defense. Outside were the marauding hordes of hackers; inside was safe and trusted, just like a medieval castle. Then we added intrusion detection. And intrusion protection. Not to forget antivirus. When client/server models gave way to large data centers housing our applications and databases, we put the firewalls in front of the data center, where our key assets now resided. And the traditional firewall was transformed into the next-generation firewall, with more sophisticated functions and the ability to deal with application-layer threats.

We are deploying an ever-growing number of defensive tools, yet breaches continue to make the headlines. Two important reasons are that each of these tools focuses on a different aspect of the security conundrum, and they are all local weapons. They sit at particular points in the network: in front of the data center, at the internet access point, in the branch. They deal only with the threats that reach them. And only with those that they can already identify.

As data centers are increasingly virtualized, applications and databases are spread across dozens or hundreds of virtual machines in thousands of physical servers, often in geographically diverse data centers. And extending into the cloud. Or clouds. Where is the perimeter now? It is everywhere. And nowhere.

So where do you put your security? And how do you keep it from impeding your business?

A Better Approach

At Juniper Networks, we believe that fighting modern cyber threats calls for a completely different perspective. It requires a realistic view of the threat environment, with an eye on using security to enable business opportunities. You need a smart, de-risked way to enable digital transformation for your organization—one that embraces the opportunity to make your infrastructure a business driver without an ever-present shadow of reputational damage and regulatory censure. The right security architecture allows IT to say yes to the business rather than no, but responsibly.

Let's be realistic: you can't keep all threats out of your network. You can always be the victim of an infected USB stick, or a successful phishing attack. It isn't good enough to merely keep out the vast majority of known threats. You also have to identify new ones, and do something about any that do get in.

Clearly, specialized security devices have an important role to play in your security posture, but we view them as part of a comprehensive security architecture that fights threats throughout the one conduit that all attacks rely on: the network.

Juniper Networks believes that the old paradigm of relying on firewalls and other specialized security devices is inadequate for the new business environment. Instead, the network itself should detect and protect against attacks.

Think of how the human body protects itself against disease. The membranes in your nose and mouth trap many microbes before you breathe them in or swallow them. Your skin is a perimeter barrier to disease, just like a firewall. These are necessary, and useful. But your ultimate protection is your immune system, which flows throughout your body, detects threats (viruses and bacteria) wherever they enter, and automatically masses its resources to fight them. Not only that: it is constantly learning about and adapting to new threats.

The Network Is the Firewall

In the same way, you can’t rely on traditional perimeter security for your business; you have to protect everything, everywhere, because attacks can come from anywhere. But you can still be protected, if the network is the firewall.

Making this work involves a number of different aspects to managing the recognition and mitigation of threats and attacks.

First, you must have visibility of your entire network. This means a single policy enforcement and management domain for all network and security devices: switches, routers, firewalls, and everything else. Whether they are physical or virtual. In this way, for example, if you detect an infected workstation or virtual machine, you can disable its switch port, quarantine the device, prevent the malware from spreading, and update firewall rules to prevent the malware from communicating with its control server. All at lightning speed, of course.

Additionally, you want to implement centralized policy that dynamically learns and adapts, using open standards and protocols to instantly modify the network and security elements. And it must be able to receive threat information from a variety of sources to have the widest possible visibility into attacks, helping you stay ahead of the bad guys.

Finally, leverage the scale of the cloud to provide your policy controller with the greatest possible amount of threat intelligence. Sophisticated tools with open interfaces allow you to pool information, share intelligence, and cross-reference knowledge to optimize your understanding of threats. This enables fast identification, mitigation, and remediation of malware, ransomware, and other unwelcome intrusions. Such tools can also be used to extract suspicious files—which might indicate zero-day or advanced attacks—to be sent to the cloud for deep inspection, sandboxing, and sophisticated analysis.

Traditional perimeter defenses are no longer enough, because the perimeter has become elastic: it expands and contracts with the dynamic demands of digital business. The solution is in the network itself.

Conclusion

You didn’t set out to build a network —you set out to create a safe, reliable, and fast business environment for your organization’s digital transformation. To help you be successful, Juniper Networks believes in building networks that have security embedded in their foundations. Secure networks that embrace openness in support of collaboration, but which can automatically identify, isolate, and eliminate threats before they do any damage. So you don’t have to compromise your peace of mind, your brand, your compliance, or your customers’ trust as your organization enacts its digital transformation strategy.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
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