Software-Defined Secure Networks

Cybersecurity for Cloud-Grade Networks

Introduction

Cloud-Grade Networking builds on carrier-grade reach and reliability and enterprise-grade control and usability, bringing cloud-level agility and operational scale to networks everywhere. Cloud-Grade Networking essentially adds a new set of principles and capabilities to what the industry already knows, making networks less capital-intensive, more automated, and ultimately better suited for innovation, both on and within the network.

In many ways, Cloud-Grade Networking is an acknowledgement that the way networks are currently designed, built, and operated is changing. While these principles might have originated with the major cloud-scale properties, they are now transforming networks of all shapes and sizes, across all industry verticals.

What Is a Software-Defined Secure Network?

Software-Defined Secure Network (SDSN) describes a unified cybersecurity platform that transforms every network component into an enforcement point, making them an integral part of the security umbrella. Using the SDSN platform, security teams can manage centralized policy and control, surfacing threat intelligence across the whole of the infrastructure so that it can be analyzed in real time and enforced dynamically.

The SDSN platform adds security and software-defined control to a solution that is centralized in its administration and control but distributed in its enforcement, extending the principles of cloud security across the whole of the network.

If It’s Connected, It Can Be Infected

The days of simply securing the perimeter are over. Threats are everywhere—both inside and outside the perimeter. Every connected device is vulnerable, representing a potential threat. This includes devices such as servers with root kits, users, rogue actors and employees infected with malware, and even connected sensors that are part of the Internet of Things (IoT). If it is connected, it can be infected.

Understanding that every connected entity represents a risk, the notion of security changes from keeping the enemy out to quickly identifying, responding to, and containing threats—wherever they may be.

Security Sprawl

Cyber threats are expanding. As the number of attack surfaces increases, the risk goes up; as attackers become more sophisticated, threats become more complex. This has led companies to deploy a sprawling set of specialized security solutions. Some enterprises may have more than 50 discrete security products in the data center alone; large enterprises might have far more.

Unfortunately, there is no evidence that this approach—which naturally drives up costs—makes companies demonstrably safer. Cyber crime is expected to cause $2.1 trillion dollars in damage in 2019, triple the 2015 number. In 2017, it is expected that 1.1 billion identities will be exposed. In 2016, one in every 131 e-mails contained some form of malware. The reality is that, despite the overwhelming investment in security, threats are not being adequately addressed, and new ones are always emerging.

Unified Cybersecurity

The first step in deploying an SDSN platform is unifying the security complex. The biggest issue with security sprawl is not the cost of managing dozens or even thousands of discrete security products; rather, it is the debilitating complexity of a security landscape that features multiple points of policy control and potentially hundreds of thousands of enforcement points that don't share information, leaving gaps in protection.

The answer to scalable security is not to grow security teams linearly to keep pace with the number of specialized solutions being deployed. Rather policy, management, and visibility—augmented by automation and machine learning—must be centralized so that relatively small teams of skilled security professionals can effectively manage them. This helps contain costs, and also focuses the collective security expertise on a smaller administrative domain. For this to work in a distributed heterogeneous environment, policy enforcement and threat containment must work in a multivendor environment, allowing teams to manage many devices and threats from a "single pane of glass." An SDSN platform, built around open interfaces, allows this.

Further, a unified security approach requires that telemetry and data be shared. In a modern infrastructure, this information must be accessible from any device, running in any network or in any cloud. For the most part, this information already exists, but it is fractured—hidden in silos, with no way to correlate or illuminate crucial security status.

Automated Enforcement

Once policy is centralized, management is unified, and information is understood across the infrastructure, the SDSN platform automates enforcement based on existing threat conditions.

Systems can stream data—threat intelligence, network telemetry, events, and so on—to a collector for real-time analysis. With SDSN, this information is shared across solutions boundaries, enabling the discovery of threats that are only revealed by correlating data and events across disparate devices. Once detected, the centralized analysis engine can push policy changes that address the threat.

Augmenting this analysis engine with machine learning expands what is possible with the SDSN platform, enabling companies to build a strong, real-time, data-driven security posture that leverages devices from multiple vendors.

Distributed Containment

The final pillar of the SDSN platform is threat containment. In an SDSN environment, every node, from firewalls to switches, is a potential policy enforcement point. If a threat is detected, the SDSN platform uses the centralized controller to push policy down to the relevant devices.

Imagine, for example, a user unwittingly downloads malware or clicks on a weaponized link outside the office. When the user connects that laptop to the corporate network, the malware can spread. With a unified cybersecurity platform like SDSN, this threat would be contained and the offending endpoint would be quarantined and tracked—all seamlessly orchestrated with intelligent, automated threat containment.

Conclusion

By having every device participate in the enforcement scheme, the SDSN platform lets companies pinpoint the threat and right-size the remediation, ensuring that a threat is rapidly stopped and damage is minimized.

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