IDC
ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Securing the Connected Enterprise Using Network-Based Security

March 2018

Adapted from *Bring Security to the Forefront of Digital Transformation* by Christina Richmond, et al., IDC #US42549117

Sponsored by CenturyLink

As organizations undergo technology changes influenced by digital transformation (DX), networks are becoming more exposed and vulnerable to security threats and attacks. Long gone are the days when an organization needed to protect only what was within the perimeter. Today, organizations are highly distributed, with applications and data being migrated to the cloud. A new era has arrived in which security is no longer concentrated in one specific area. Organizations must embrace these complexities and the security challenges that come with them. This IDC Technology Spotlight examines the importance and benefits of network-based security, trends in security, and the role that CenturyLink's network-based security solution plays in this market.

Introduction

As organizations become increasingly distributed and migrate applications and data to the cloud, networks are growing more critical. Unfortunately, as networks and endpoints expand, so do security vulnerabilities. The security environment is no longer static, so organizations must evolve to keep up with a rising number of threats that are harder to detect with traditional security solutions.

In the past, organizations traditionally addressed security from a perimeter-centric approach that was trusted and had boundaries. Today, this focus is inadequate due to the distributed nature of many organizations as well as the ongoing threat environment. Each connection introduces another point for attack or infection. Put another way: As the perimeter evolves, IT complexity and risk grow along with it. What this means for organizations is that:

- Security costs grow exponentially.
- Risks increase as a result of efficient hybrid WAN and cloud services.
- Personnel and budget to address security appropriately are lacking.
- DX initiatives also pressure security services.

DX is expected to scale dramatically in the coming years. In fact, IDC predicted that by the end of 2017, two-thirds of the CEOs of Global 2000 enterprises would have DX at the center of their corporate strategy. By 2020, 50% of the Global 2000 will see the majority of their business depending on their ability to create digitally enhanced products, services, and experiences. In response, many organizations are embracing a new way of doing business. However, without appropriate security built into development processes, the door is open to sophisticated, determined attackers. Digital security initiatives need to evaluate and mitigate new risks while ensuring privacy, confidentiality, integrity, and availability.

As adoption of DX and technologies such as cloud, big data and analytics, mobile, and social accelerates, new challenges arise related to where data resides, how data is accessed, and who owns security. With hybrid architectures and migration to the cloud, an organization's applications, data, and users increasingly are outside the CIO's traditional domain, yet CIOs are responsible for security, visibility, control, and compliance. As a result, IT organizations are turning to providers of managed security services (MSS) to deliver a wide span of security capabilities and consulting services, including predictive threat intelligence and advanced detection and analysis expertise. These services are necessary to overcome today's security challenges and to prepare organizations against future attacks. However, in the DX era, companies don't want to be "all in" for either on-premises managed security services or cloud security. Instead, they are seeking solutions that are on-premises in their datacenter, located within communication and network service providers, or hosted via multitenant security and cloud-based security either in a public cloud or on a SaaS/PaaS platform and managed/monitored in the cloud.

Network-based security is a long-standing approach that has gained significant importance in recent years. It provides the ability to see a threat early on and protect the organization before the network is hit.

Definitions

- **Digital transformation:** DX is a strategic business imperative at the enterprise level that is driving fundamental changes in how the enterprise operates, delivers services, and interacts with its customers and supply chains. It refers to the disruption and evolution of business models and processes through new technologies leveraging cloud, analytics, mobility, social media, and the Internet of Things (IoT).
- **Managed security services:** MSS is considered part of the worldwide security services market by IDC, which defines MSS as "the around-the-clock remote management or monitoring of IT security functions delivered via remote security operations centers (SOCs)."

Benefits of Network-Based Security

The security landscape is complex and challenging — and becoming more so as organizations move to a digital world. Therefore, organizations need to deal with many moving parts to defend and fight against the sophisticated cyberthreats and attacks of today. Organizations face new types of attacks such as those that combine advanced persistent threats and distributed denial-of-service (DDoS) attacks. They are finding it harder to detect these attacks and to protect their infrastructure and systems against them.

Fortunately, a network-based approach to security can provide the advanced protection needed. Such an approach offers more protection than traditional point security solutions against the rising tide of known and unknown threats. Network-based security solutions can reduce a threat before it reaches the organization's systems. For example, in the event of a DDoS attack, a network-based security solution can provide immediate protection by rerouting the malicious traffic coming into a scrubbing center and then having the legitimate traffic sent without any interruption. In addition, network-based services such as spam filtering can block users from connecting to bad URLs from malicious sites.

Network-based security solutions offer a set of complementary services to protect an organization from the inside out. These solutions are typically handled by a managed security services provider (MSSP) and include advanced protection and threat intelligence to help extend the defenses offered by traditional security solutions. Organizations that allow an MSSP to handle the management and monitoring of security services can realize greater synchronization of security policies across all applications and workloads. The uploading of new malware signatures can also be easily applied once new threats are determined by the MSSP. With network-based security, organizations can centralize security to block all known threats and identify and block unknown threats.

Utilizing a network-based service means there is less need for a premise-based firewall or intrusion detection and prevention systems (IDPS) or appliances. While some organizations may still need these appliances on-premises, a network-based service can work with the on-premises solution in a complementary fashion and provide even more effective protection. With network-based solutions, there is no need to invest in an appliance, therefore reducing any up-front costs. The organization is also relieved from any extra labor costs associated with managing a new appliance and thus can invest in other business initiatives.

Working with an MSSP also provides organizations with the expertise and resources needed to maintain a healthy security posture. MSSPs are well known for their expertise in security, and their staff typically have the capabilities to determine what new threats are emerging within specific industries. For example, the open source Mirai botnet was used to provide a DDoS attack against many large infrastructure entities. An MSSP has the expertise to spot these attacks faster than a typical organization and apply proper measures to protect against the attacks. In many instances, network-based services help identify threats faster within their life cycle and provide deep analysis of other potential security threats.

Trends in the MSSP Market

As organizations continue on their DX journey, the attacks and threats will become harder to keep up with and defend against. This evolving trend calls for organizations to adopt stronger security measures.

The security services market has been undergoing expansion and compression for several years. This trend will continue. To remain relevant, service providers must:

- Demonstrate threat intelligence/advanced detection and remediation capabilities
- Provide analytics
- Elevate the security conversation to a business differentiator by including the C-suite and boardroom
- Differentiate and invest in human resources

Companies seeking MSS should consider providers that can:

- Develop security for the entire life cycle
- Provide advanced security services such as intelligence/visibility, big data and analytics, incident response, forensics, and advanced detection methods
- Offer/improve customer portals by adding visualization, real-time updating, and customized reporting
- Investigate MSS research and development areas such as cloud evolution, threat intelligence, incident response, forensics, big data and analytics, and advanced detection techniques
- Acquire and retain talented professionals to help with security needs and challenges
- Improve efficiencies of the security spend (reduce cost)

Given the trends that exist today (too many threats, not enough budget or people, expanding perimeter), companies are looking to a trusted provider to offer extended security at all ingress and egress points of their architecture.

Considering CenturyLink

CenturyLink is a large U.S. telecom company that expanded its footprint by acquiring Level 3 in 2017. Today, the company provides a multilayered approach through network-based security solutions that consist of advanced capabilities; services such as DDoS mitigation, adaptive network security, and threat intelligence; and complementary services such as incident management and response and security log monitoring. CenturyLink operates a global network that allows it extensive visibility into security threats to better predict problems and quickly mitigate attacks. The company states that each day it monitors 1.3 billion security events, mitigates 120 DDoS attacks across its 11 globally distributed scrubbing centers, and monitors 99 billion netflow sessions. It also has 24 x 7 security operations centers located in North America, Europe, Asia/Pacific, and Latin America.

CenturyLink's network-based solutions are backed by the company's threat intelligence. CenturyLink applies advanced analytics to its network-based security services to detect unknown threats in the network. The company utilizes a team of experts, threat research labs, and the visibility provided by its global network to analyze and monitor traffic to provide threat data. With threat intelligence, the correlation of traffic against malicious communication is utilized with CenturyLink's proprietary analysis and data.

CenturyLink's Adaptive Network Security Service offers next-generation firewall protection via the cloud. It acts as a flexible and secure network gateway by offering broad security for coverage of distributed hybrid networks, datacenters, cloud deployment, branches, remote offices, and mobile workers. As a network-based solution, it also provides cost-effective, flexible, and reliable protection that will not impact performance.

CenturyLink's DDoS mitigation service provides customers with network routing, rate limiting, and filtering paired with a network-based detection and mitigation scrubbing center solution. The DDoS approach utilizes threat intelligence that is derived from its global infrastructure and data correlation to detect DDoS attacks across the network. The mitigation service is carrier agnostic and pulls the customer traffic through route redirection (BGP redirect or DNS redirect) onto the company's scrubbing centers for mitigation and cleansing. The customer's traffic is onboarded at the closest point of presence (POP) for faster mitigation service. The service can mitigate sophisticated attacks against volumetric and application layer attacks that form from Layers 3–7. In addition, advanced behavioral analytics are applied on the proxy service. Flexible customer deployment options are available "on demand" or as an "always on" solution and backed by time-to-mitigate service-level agreements (SLAs) for most known forms of attacks on the network.

CenturyLink Adaptive Threat Intelligence utilizes network visibility to provide global threat analytics and tracks two-way communications to identify attack patterns. It then automatically correlates and analyzes the threat data and prioritizes it for the customer's IP address space. If the sampled information matches a malicious IP, an alert is created and forwarded to the portal or customer security information and event management (SIEM) system. This feature allows customers to act on a data-driven, cyberthreat plan in near real time.

CenturyLink Security Log Monitoring provides 24 x 7 tracking of customer IT environments. The service receives logs from customer devices and applications including existing log management systems, SIEM systems, and on-premises, hosted, or cloud devices. It leverages a data analysis engine for sophisticated log ingestion and event correlation. Customers have the option to add incident management and response to investigate and respond to cyberthreats.

Challenges

CenturyLink is well known in the United States, but it has undergone several organizational changes as a result of its recent acquisition of Level 3. Both companies bring a breadth of knowledge and skills to the market, but integrating services and networks can be a challenge following an acquisition. Along with the challenge of integrating the security portfolio, matching the culture of two organizations and their customer bases can present hurdles as well. The support of and relationship with customers are key to success in the MSSP market, and CenturyLink will have to continue to provide customers with a seamless integration while undergoing operational changes following the Level 3 acquisition.

Conclusion

The security landscape is complex and challenging for organizations around the world. IDC recommends that enterprises consider a multilayered approach that will detect and respond to both unknown and known threats and alert the business. As security threats continue to grow and become more complicated, companies need to undertake a holistic, enterprisewide security posture that is proactive and predictive.

It's a daunting effort, however, to sustain the necessary level of threat intelligence and advanced analytics capabilities along with the skills to interpret and act on findings. In-house 24 x 7 security solutions are expensive, and security talent is scarce. As organizations debate "build versus buy," many are turning to MSSPs.

IDC believes that CenturyLink's network-based security services, which leverage the company's threat intelligence, global network visibility, and 24 x 7 customer service, can support an organization effectively as well as reduce costs associated with securing an organization's infrastructure. To the extent that CenturyLink can address the challenges described in this paper, the company has a significant opportunity for success.
