RESEARCH
Influence and insight through social media

December 2016

CISCO ONE SIMPLIFIES ENTERPRISE SECURITY IN THE DIGITAL ERA

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

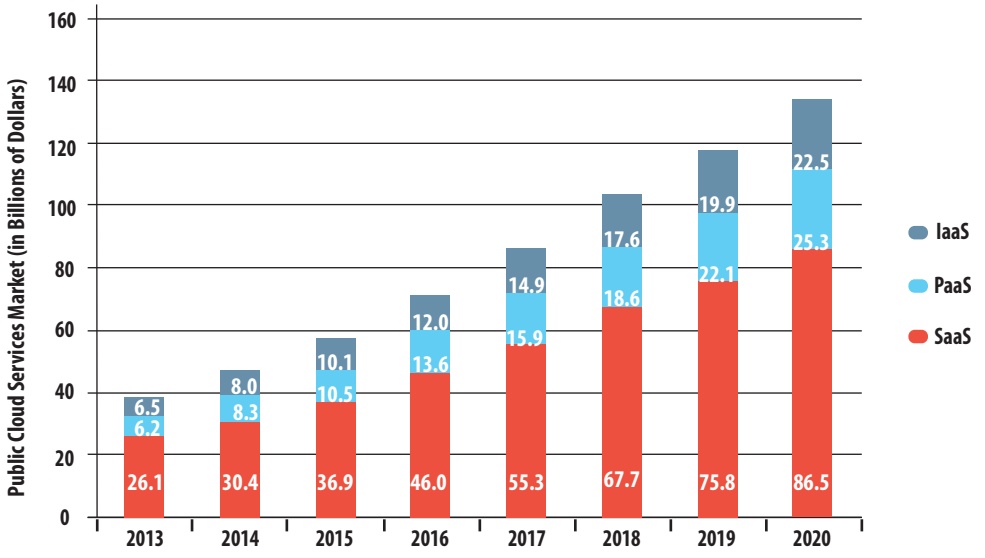
INTRODUCTION: DIGITAL ORGANIZATIONS NEED TO RETHINK SECURITY STRATEGIES

The world is becoming digital, requiring the IT environment to rapidly evolve to meet the needs of businesses. Networks have become software defined, applications have moved to the cloud, employees are using personal devices in the workplace and the Internet of Things (IoT) is gaining momentum. All of these technology shifts have increased an organization's ability to be dynamic and agile and to move with speed. However, the one part of the IT ecosystem that has yet to change is security. Below are the major changes to IT that are affecting security:

The perimeter is eroding. Historically, the enterprise was secured by deploying a firewall at the connection to the internet, which was the only point of entry into the company. Today, the rise of cloud computing (Exhibit 1), IoT and "bring your own device" (BYOD) has eroded the existing perimeter and created hundreds of new entry points. For example, the cloud enables lines of business to procure their own services directly. In fact, the ZK Research 2016 Network Purchase Intention Study found that 96% of organizations have cloud services that were not procured by the IT department, creating a blind spot for the security team. IoT creates more blind spots because the operational technology group deploys IoT endpoints. These trends have created several new entry points into the company; consequently, ZK Research estimates that the number of attack surfaces has grown by 10 times in the past five years.

The threat landscape is evolving. The ZK Research 2016 Security Survey found that 90% of security budgets are used just to protect the perimeter. However, only 20% of attacks are

Exhibit 1: The Rapid Growth in Cloud Services Creates New Security Challenges



ZK Research 2016 Global Cloud Forecast

ABOUT THE AUTHOR

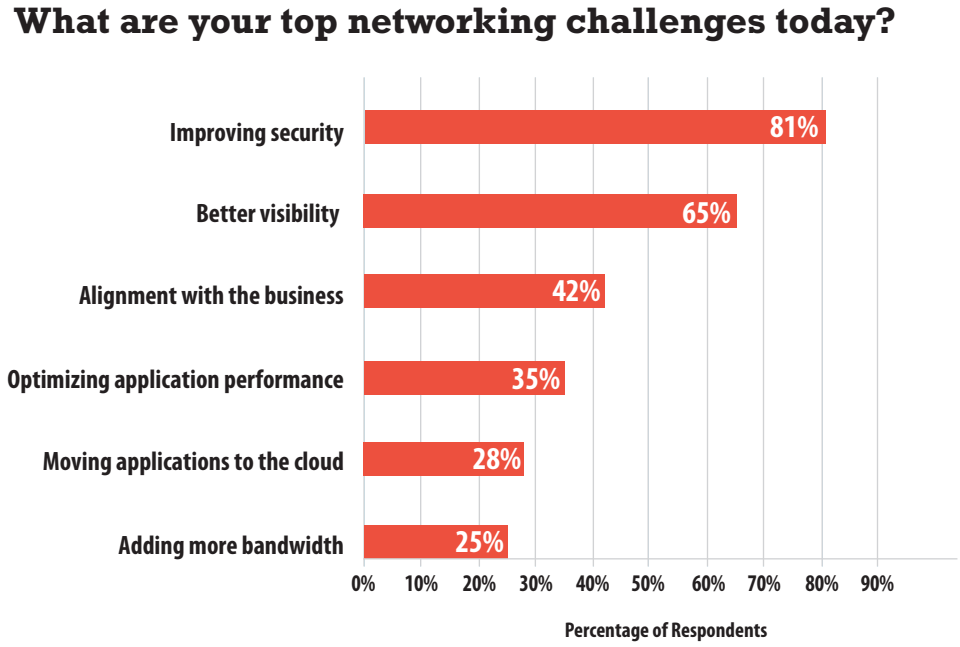
Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

focused at that point. Businesses need to focus on several new attack vulnerabilities such as phishing, network eavesdropping, mobile attacks and software bugs. Digital transformation has made cyberattacks much more lucrative, which means the threat landscape will continue to evolve at an exponential rate.

Security is becoming more complex. The growing number of attack surfaces combined with new, more sophisticated attacks has caused organizations to deploy more security point products in more locations. The ZK Research 2016 Security Survey found that large enterprises have deployed an average of 32 security vendors, with some companies deploying more than 100. Having more security tools does not necessarily equate to having better security, as this can lead to inconsistent security policies. In addition, ZK Research has found that it takes an average of more than 100 days to find a breach. Also, despite enterprises spending tens of billions of dollars on new products every year, security remains the top challenge for network managers today (Exhibit 2). Lastly, the large number of point products makes implementing new policies or even simple changes extremely slow and can create gaps in security, as multiple devices need to be configured and tested.

Businesses are aggressively marching down the digital path. Meanwhile, the current state of security is overly complicated, and security methods are too slow to meet today's needs. It's time for organizations of all sizes to rethink their security strategy and align it with the requirements of the digital era.

Exhibit 2: Security Remains the Top Challenge for Most Organizations



ZK Research 2016 Network Purchase Intention Study

SECTION II: UNDERSTANDING THE CISCO ONE SOFTWARE MODEL

Digital organizations are built on network-centric technologies such as IoT, cloud computing and mobility. Consequently, networks have grown in importance and have had to start delivering more functionality. This has driven up the complexity of buying, deploying and managing the software needed to run a network. However, the process of managing and procuring network software is plagued by several issues, including the following:

The process of ordering and managing software licenses for network devices is becoming more complex, making it difficult to ensure the right features are available in the appropriate places in the network.

Network software is upgraded typically at refresh, which can cause organizations to miss out on new opportunities.

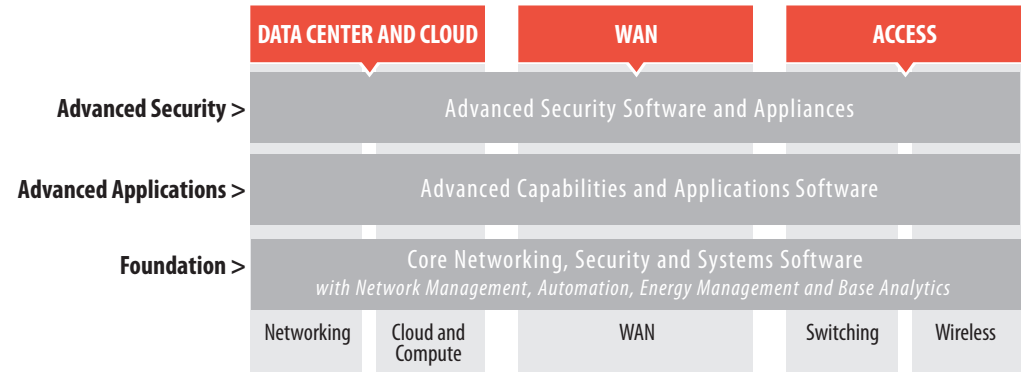
The periodic refresh of network infrastructure leads to lumpy spending patterns, making budgeting difficult.

Cisco ONE Software provides a simple and flexible way for customers to buy software for their data centers, wide-area networks (WANs) and access networks. This model decouples the acquisition of the software from that of the underlying hardware platforms.

Cisco ONE Software simplifies the process of network procurement and management by enabling customers to buy all the feature licenses in one package and then turn on what is required when needed. It offers greater value to customers through reduced complexity, investment protection, access to new capabilities and flexible buying models.

Cisco ONE Software is organized into three distinct domains: Data Center and Cloud, WAN and Access. Each is available in three different feature sets: Foundation, Advanced Applications

Exhibit 3: Cisco ONE Software Provides Breadth and Depth to Customers



Cisco, 2016

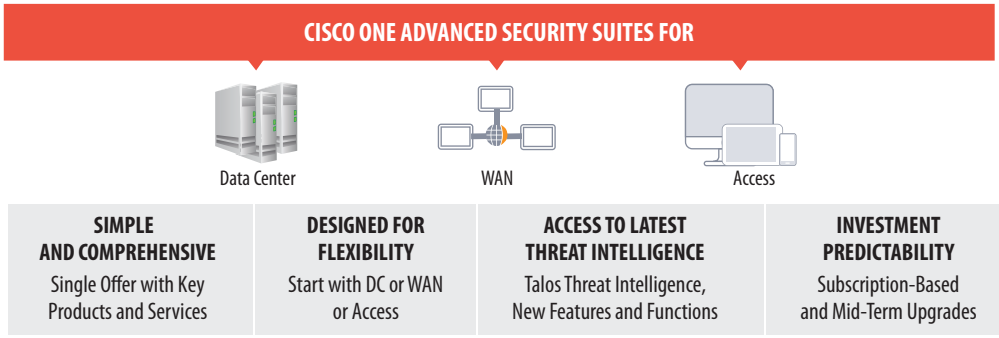
and Advanced Security (Exhibit 3). Details of Cisco ONE Software for the different domains can be found at *www.cisco.com/go/one*.

SECTION III: CISCO ONE ADVANCED SECURITY SOFTWARE

Cisco ONE Advanced Security (Exhibit 4) extends the value of Cisco ONE to advanced security. It makes it easier to fortify an organization's data center, WAN and access with simple, predefined suites of key security products and services in a single offer for each.

Customers that choose to purchase advanced security using Cisco ONE will realize the following benefits:

Exhibit 4: Cisco ONE Advanced Security Frameworks



ZK Research and Cisco, 2016

Simple and comprehensive suites: For each domain (Data Center, WAN and Access), Cisco ONE provides a single, predefined offer with key security products and services. For example, in the data center, the offer includes advanced malware protection, next-gen intrusion prevention, URL filtering and virtualized firewall and services.

Designed for flexibility: Customers may begin deployment in one specific domain. But the sum is greater than its parts when customers take a holistic approach to security by deploying Cisco ONE Advanced Security in all three domains. In addition, Cisco ONE supports both physical and virtual appliances (currently for access; forthcoming for data center and WAN).

Access to the latest threat intelligence: Customers have access to Cisco Talos, industry-leading threat intelligence that supports the functionalities in the various Cisco ONE offerings. Cisco ONE Advanced Security also offers access to new features and functions.

Investment predictability: All three offers are available as one-, three- or five-year software subscriptions. Subscriptions provide predictable cash flow. Customers can also

upgrade the subscription to a newer appliance mid-term and get credits for any unused term in their old subscription.

All three subscriptions include software support services that provide software updates and upgrades, access to technical support and new software capabilities.

This differentiates Cisco from other vendors, as it covers more places in the network (data center, WAN and access) and also provides depth of security—both inside and perimeter security.

To help customers realize the value of Cisco ONE Software faster, Cisco offers a set of professional services composed of the following components:

Quick Start services are customized to Cisco ONE to quickly integrate new capabilities into the business. Service engineers provide expert guidance and assistance throughout the process to lower risk while improving time to value. Quick Start activities include turning up new services, software installation, configuration, customization, task automation, migration, onboarding and testing.

Optimization services include adoption and change management to ensure customers achieve the desired transformation while driving business outcomes.

Most organizations focus on protecting the perimeter but often overlook internal data center security.

SECTION IV: CISCO ONE ADVANCED SECURITY FOR DATA CENTER

The data center is the lifeblood of most organizations. It's the place where all of the critical applications, data and intellectual property reside. Consequently, the data center is a main focal point for hackers. It can be a challenge to protect, as attacks can start directly in the data center, or it can be breached through a "back door" if a system that accesses the data center is unprotected. Most organizations focus on protecting the perimeter but often overlook internal data center security. Based on the following data points from the ZK Research 2016 Security Survey, it's clear that a greater focus on securing the data center is required:

Currently, 90% of security budgets are spent at the perimeter, but only 20% of breaches occur at that point.

The average time to find a breach in the data center is 100 days.

East–west traffic now accounts for 70% of data center traffic and is growing rapidly. East–west traffic bypasses the security placed in the core of the network.

53% of survey respondents turn security features off at the perimeter in favor of performance, leaving the data center even more exposed.

Exhibit 5: Cisco ONE Advanced Security for Data Center

SUBSCRIPTIONS	DETAILED LICENSES	HARDWARE (Sold Separately)
ASA 5585-X subscriptions*	ASA 5585-X Firepower (IPS, URL, AMP) Security Context	ASA 5585-X appliance
Firepower 4100/9300 subscriptions*	Firepower 9300/4100 Firepower Threat Defense (IPS, URL, AMP)	Firepower 9300/4100 appliance

*Subscriptions include both the software licenses and software support that provide benefits such as software and signature updates, credits for mid-term upgrades, and access to the latest threat intelligence and features.

Cisco, 2016

Cisco ONE Advanced Security for Data Center enables customers to handle security threats against the data center today:

It allows segmented policies through a virtualized firewall.

It helps with prevention and mitigation of known and unknown threats with next-gen intrusion prevention.

It helps with detection and blocking of stealth malware and zero-day attacks with advanced malware protection for the network.

It provides reputation- and category-based filtering of more than 280 million websites in at least 80 categories.

It equips you to defend your enterprise from both outside and inside, as an increasing number of attacks are originating from inside the organization.

Exhibit 5 shows the features included in Cisco ONE Advanced Security for Data Center.

SECTION V: CISCO ONE ADVANCED SECURITY FOR THE WAN AND EDGE

For many organizations, the branch is the business. ZK Research estimates that 84% of employees now reside in a branch office, making it the dominant place where work gets done and where customers are served. The rising number of branch resident employees has had a profound impact on the network due to the exponential growth in the number of devices resulting from the BYOD trend. The ZK Research 2016 Consumerization Survey found that 82% of organizations now have a formal BYOD plan in place, and branch workers are carrying an average of three devices per person. The use of consumer devices in the workplace has created new security risks,

and 75% of respondents in the ZK Research 2016 Security Survey cited mobile security as their top security challenge.

The other trend that has raised the security bar in branch offices is the growing use of cloud-based applications. To improve the performance of software as a service (SaaS), businesses are enabling workers to access the cloud directly from the branch instead of having to traverse the WAN first. The combination of consumer devices and cloud applications has increased the number of branch attack entry points by five times during the past year.

Branch security must evolve to keep pace with an increasingly digitized world. Businesses need to ensure branch security includes the following characteristics:

Secure remote access

Unified wired and wireless security

Data protected from tampering, unauthorized access and eavesdropping

Secure direct internet access

Cisco ONE Advanced Security: Threat Defense for WAN and Edge is a solution designed to enable advanced security in branch locations:

It offers highly secure remote access and client VPN.

It helps with prevention and mitigation of known and unknown threats with next-gen intrusion prevention.

It helps with detection and blocking of stealth malware and zero-day attacks with advanced malware protection for the network.

Exhibit 6: Cisco ONE Advanced Security: Threat Defense for WAN and Edge

SUBSCRIPTIONS	DETAILED LICENSES	REQUIRED HARDWARE (Sold Separately)
ASA 5500-X subscriptions*	ASA 5500-X Firepower (IPS, URL, AMP), AnyConnect Plus	ASA 5506, 5508, 5516, 5525, 5545, 5555 appliances

*Subscription includes both the software licenses and software support that provide benefits such as software and signature updates, credits for mid-term upgrades, and access to the latest threat intelligence and features.

Cisco, 2016

It provides reputation- and category-based filtering of more than 280 million websites in at least 80 categories.

Exhibit 6 shows the structure of Cisco ONE Advanced Security: Threat Defense for WAN and Edge.

Businesses need a simplified approach to securing the access edge.

SECTION VI: CISCO ONE ADVANCED SECURITY FOR ACCESS

The access edge of the enterprise network is becoming increasingly complex. The growth of consumer devices and cloud applications has created many blind spots that can lead to network breaches. Also, IoT is rapidly becoming the norm, and a wide range of new devices are being attached to the access edge including video surveillance cameras, LED lighting, HVAC systems and vertically specific equipment. The ZK Research 2016 Network Purchase Intention Study found that 70% of network managers have little to no confidence that they are aware of all the devices attached to the access edge.

Also, cybercriminals have focused their attention on the end user and applications through advanced malware such as advanced phishing campaigns. Once these threats enter the network, they remain hidden for several months while they gather information to eventually exfiltrate valuable data. Other interesting data points related to the access edge from the ZK Research 2016 Security Survey include the following:

90% of organizations have been breached—46% in the last year alone.

50% of businesses employ the use of mobile devices that are infected with malware.

The average time to find a breach at the access layer is 100 days.

96% of organizations are using applications that were not sanctioned by IT.

Workers use an average of four consumer applications as part of their daily job.

Businesses need a simplified approach to securing the access edge to enable workers to utilize the information they need at any time on any device from any location. Additionally, security teams need improved visibility to search for anomalous traffic that may indicate a breach.

Cisco ONE Advanced Security: Policy and Threat Defense for Access is designed to increase security while providing users with correct but simplified access. It offers the following:

Highly secure access based on identity and device, centralized identity- and context-based access from anywhere

Exhibit 7: Cisco ONE Advanced Security: Policy and Threat Defense for Access

SUBSCRIPTIONS	DETAILED LICENSES	REQUIRED HARDWARE (Sold Separately)
ISE and AnyConnect subscriptions*	ISE-Apex, ISE-Plus, AnyConnect Apex	ISE appliance

*Subscription includes both the software licenses and software support that provide benefits such as software and signature updates, credits for mid-term upgrades, and access to the latest threat intelligence and features.

Cisco, 2016

Visibility, compliance and mobile device management (MDM) support

VPN and highly secure endpoint with Cisco AnyConnect Apex

Exhibit 7 shows the structure of Cisco ONE Advanced Security: Policy and Threat Defense for Access.

SECTION VII: CONCLUSIONS AND RECOMMENDATIONS

The digital business era has arrived, and it has brought with it many new technologies such as IoT, cloud and mobility. These technologies have enabled organizations to be more dynamic and distributed, and they have raised efficiency and productivity to new heights. Companies that can make the rapid transition to becoming digital will be more profitable and gain a competitive advantage; those that can't will struggle to survive.

However, all of these new technologies come with a price—security has grown increasingly complex. The traditional security methods of focusing solely on the perimeter are no longer sufficient because the bulk of attacks are now bypassing the network edge. Security architectures must change, and an increased focus on the internal network is necessary—particularly the data center, branch and access edge, which are the new focal points for cybercriminals.

Cisco's threat-centric approach is ideally suited to meet these requirements. It turns the network into both a sensor and an enforcer, because it can quickly discover threats through network anomalies and then quarantine them before they can spread laterally and cause more damage.

In conjunction with the rollout of its advanced architecture, Cisco has simplified the purchase of security features in the data center, branch and access edge with its Cisco ONE Software. Customers that purchase security using Cisco ONE Software will realize the following benefits:

Domain-specific simple and comprehensive software suites

Flexibility to start at any place

Access to the latest threat intelligence and features

Investment predictability through subscription offers

Cisco ONE Software helps customers better secure their network by enabling businesses to purchase the right software capabilities to address their needs today, while offering investment protection for the future. Also, this is what differentiates Cisco from many other point product vendors, as Cisco ONE helps customers cover more places in the network and provide depth in security.

Migration to the Cisco ONE Software model should be the top priority for any company looking to improve its security posture. Consequently, ZK Research makes the following recommendations:

Rethink security in the digital era. Traditional security methodologies were developed in an era when IT had tight control over applications, endpoints and where users work. This is no longer the case; the control IT once had is now gone. Businesses need to adopt a threat-centric approach that leverages the network—a company's most ubiquitous asset—and that sees all traffic and can quickly identify breaches.

Minimize the number of security vendors. The ZK Research 2016 Security Survey found that businesses have an average of 32 security vendors in their environment. Working with this many vendors leads to an unmanageable environment with many blind spots, false positives and inconsistent information. The goal should be to minimize the number of security vendors to improve performance and simplify management. Although multiple vendors will likely be needed, companies should choose a main vendor with a large ecosystem of third parties to ensure seamless interoperability.

Customers should consider Cisco ONE Software for security. As demonstrated throughout this paper, Cisco ONE provides both cost and innovation advantages over traditional purchasing models. ZK Research believes Cisco ONE Software is the right security purchasing model for data center, WAN and access for the digital business era.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314