FORTINET

WHITE PAPER

Why Data Centers Lack Adequate Security to Ensure Business Continuity

Executive Overview

Business-critical applications are now hosted and consumed from increasingly distributed data centers that extend across hybrid IT infrastructures—from on-premises, to co-locations, to private and public clouds. And with this trend, digital data and workflows are proliferating across locations. This expands an organization's attack surface while reducing visibility and control. To address the increased risk, many businesses added point security solutions. But this fueled infrastructure complexity and created more manual workflows for overstretched network and security teams. This coalesces into an environment that degrades operational performance, reliability, and availability—thereby jeopardizing business continuity.

Enterprises with a hybrid strategy (combining public and private clouds) grew to 58% in 2019—up from 51% in 2018.[1]

How an Expanding Attack Surface Impacts Data Centers

As modern data centers become more distributed, vulnerable workflows and data are now spread across a hybrid IT infrastructure that includes on-premises, co-locations, and private and public clouds. This creates an expanding broad attack surface to defend. Adding point security products to address individual exposures or compliance requirements cannot cover the ever-expanding nature of this problem. As a result, network engineering and operations leaders face greater risks of a successful cyberattack, increasing odds of a network outage due to malicious activity or natural disasters, as well as growing costs and operational complexity.

Greater Risk

Security risks in the data center revolve around several issues:

Data centers extend to private and multiple public clouds

As distributed data centers include more and different cloud-based services, applications and data move around and across the hybrid infrastructure—from on-premises, to co-location, as well as to and between the different clouds. Traditional, silo-based security solutions lack the scalability and agility to meet the demands of this new hybrid environment. Network engineering and operations leaders are increasingly unable to manage risks and protect critical business applications and services (e.g., rapidly changing DevOps environments, hyper-growth ecommerce businesses) irrespective of location. In particular, their security strategies lack visibility into network traffic and assets, as well as sophisticated detection and protection against unknown and zero-day threats.

Malware encryption

Encrypted data recently hit an all-time high of over 72% of total network traffic—a nearly 20% increase year over year.[2] And last year, 28% of breaches involved malware,[3] which is often concealed and delivered using secure sockets layer (SSL) and transport layer security (TLS) encryption. Indeed, research shows that upwards of 60% of attacks use SSL or TLS encryption to hide malware.[4] Some examples include Zeus, TrickBot, and Dridex malware that records keystrokes to steal a user's valuable credentials, such as bank logins/passwords, to then cause financial damage.

Most firewalls significantly degrade network performance when inspection is turned on. To compensate, network engineering and operations leaders must either buy more firewalls or separate inspection appliances to help enforce inspection. These options increase capital costs (CapEx) while incurring greater operating expenses (OpEx) to manage the additional solutions. With these factors in mind, the difficult choice for many businesses is to either perform SSL and TLS encryption inspection by setting concerns for cost and performance aside or to increase risks by not inspecting SSL/TLS encrypted traffic at all. Other factors complicating a move to SSL and TLS inspection include issues of privacy and the perceived difficulty of managing certificates.

Lack of visibility and control

With 34% of breaches now attributed to trusted internal sources,[6] visibility and access control of the internal network becomes an imperative. Segmentation of users, devices, applications, and services can help prevent unauthorized access to sensitive content. However, traditional network-based segmentation lacks inherent mechanisms for content inspection; once within the perimeter, malware can spread laterally without obstruction.

Static trust does not reflect the true realities of human behavior, business needs, and productivity requirements. Trusted users can unknowingly become infected or have their credentials stolen as a source of data theft—not to mention occasions when a user might abuse access privileges to maliciously steal information. In addition, once-secured devices and applications can also become compromised. Unfortunately, most organizations lack comprehensive visibility and policy-based access controls to prevent attacks from within.

90% of organizations have experienced or expect to experience a network attack using SSL or TLS encryption.[5]

The vast majority (89%) of security leaders at large enterprises still struggle with visibility and insight into trusted data.[7]

Network Outages

Data-center resiliency and availability are critical to operational success. With data and workloads increasing—driven by adoption of things like Internet-of-Things (IoT) devices, big-data analytics, and artificial intelligence (AI)—enterprises need security that can keep pace with the growth and direction of their network traffic needs. By 2021, global IP traffic is expected to show a five-year compound annual growth rate (CAGR) of 26%, while interconnection bandwidth (for the private exchange of data between businesses) is expected to jump by 48%.[8]

This scale of digital growth greatly increases the opportunity for a significant network outage causing serious damage to the business. The average infrastructure failure can cost $100,000 an hour and a critical application failure can cost $500,000 to $1 million per hour.[9]

The likelihood of a critical infrastructure failure occurring also increases in the event of malicious cyberattacks and natural disasters. Potential impacts include operational disruption or downtime, poor user experience, degradation in brand reputation, data theft, and lost revenue. Earthquakes, floods, and fires can cause critical services outages for data centers via fiber cuts, power failures, or cooling system outages. Non-natural disaster issues such as heavy-equipment accidents and other human errors can cause similar problems.

Cost and Operational Complexity

As the attack surface expands, many companies use point solutions to plug the gaps in their defenses one at a time. This approach is not only inefficient and costly but it greatly increases infrastructure complexity—which reduces security effectiveness even further.

Proliferation of point security products is a serious issue: the average enterprise uses 75 different security solutions, many of which address a single vulnerability or compliance requirement.[10] More than three-quarters (77%) of organizations rely on nonintegrated point security solutions to some degree within their organization, leaving networks vulnerable to cyberattacks.[11] Specifically, as these disparate products typically cannot share threat intelligence or coordinate responses across an increasingly dispersed hybrid IT infrastructure, response times to security events elongate, thereby increasing the chances that critical systems will be compromised and disrupted or that valuable data will be stolen.

Proliferation of point security solutions also creates a need for more manual workflows. Manual processes inhibit security scalability and agility, while resulting in inconsistent security policies from on-premises to the different cloud environments. Manual workflows for compliance tracking, auditing, and reporting compound this problem further. And as industry standards and privacy law requirements grow more complex year over year, lack of security automation in these areas places an undue burden on limited staff resources while increasing the risk of regulatory penalties due to human errors.

Evolving Data-Center Security

As data centers become more distributed across a hybrid IT infrastructure, an organization's attack surface expands greatly. Disaggregated security strategies are unable to keep up with the growing risks, increasing the chance of network outages, not to mention the cost and complexity of maintaining a disjointed security architecture in the face of sprawling threat exposure.

Network engineering and operations leaders should reevaluate their current means of securing their modern data centers. The following are a few of the questions they need to ask:

- Does the solution increase security visibility across all security elements?
- Does it inspect all network traffic—encrypted and unencrypted?
- Can it provide advanced threat detection and prevention, irrespective of the location of digital assets?
- Does it support high availability and resiliency using N+1 redundancy clustering to ensure seamless, virtual real-time failover in the event of a natural disaster or malicious attack?
- Does it support intent-based segmentation that applies dynamic trust for users, devices, and applications?
- Does it operate as part of an integrated security architecture with automated threat-intelligence sharing and responses across all deployed security elements?

The shortage of cybersecurity professionals has grown to nearly 3 million unfilled positions worldwide.[12]

[1] "RightScale 2019 State of the Cloud Report from Flexera Identifies Cloud Adoption Trends," RightScale/Flexera, February 27, 2019.

[2] John Maddison, "Encrypted Traffic Reaches A New Threshold," Network Computing, November 28, 2018.

[3] "2019 Data Breach Investigations Report," Verizon, April 2019.

[4] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[5] Ibid.

[6] "2019 Data Breach Investigations Report," Verizon, April 2019.

[7] "Why poor visibility is hampering cybersecurity," Help Net Security, June 24, 2019.

[8] Tom Coughlin, "Bandwidth Growth Drives Storage Demand," Forbes, September 24, 2018.

[9] Kevin O'Connor, "Is Your Disaster Recovery Plan Up to Date?," CIO, April 18, 2016.

[10] Kacy Zurkus, "Defense in depth: stop spending, start consolidating," CSO Online, March 14, 2016.

[11] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges"," Fortinet, May 23, 2019.

[12] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 18, 2018.

FORTINET

www.fortinet.com

July 26, 2019 9:16 PM

452531-0-0-EN

D:\Fortinet\Work\2019\July\072619\Task 2- wp fortigate\wp-fortigate-eseries-network-leader