FORTINET

WHITE PAPER

Broken and Disconnected: A New Approach to Security Connections is Needed

Executive Summary

Digital transformation (DX) has brought new business capabilities to enterprises while simultaneously exposing new security risks. Network defenses that use a patchwork of disaggregated multivendor products are no longer effective within distributed network structures, where data often resides in various isolated environments and siloed applications. Information technology (IT) leaders must revisit security at an architectural level to address several critical problems—a lack of integrated and connected security tools, overly complex management, and a lack of automation.

In 2017, there were over **53,000 recorded security incidents** and **2,216 confirmed data breaches.**[1]

Hybrid IT describes a strategy for enterprise network management where an organization's **in-house IT team oversees some resources while cloud-based services manage others.**

Digital Transformation Creates New Security Challenges

Organizations recognize that they will not survive without embracing the business advantages offered by DX. Business leaders are pushing for rapid adoption of cloud-based initiatives, expanded use of Internet of Things (IoT) devices, and embracing more aspects of mobility to drive revenue and exploit data. This creates a highly diverse and disparate IT environment consisting of varied on-premises and cloud deployments, access points and devices, applications, and users.

But securing DX environments presents new challenges. Previous-generation security products are typically disconnected from one another. They reside in their own isolated silos, with limitations that include:

1. Different solutions that don't talk to each other and therefore can't see what's happening in other parts of the network to defend against broad attacks
2. Manual management processes that drain IT productivity
3. Degraded threat intelligence—slow and encumbered—that inhibits overall security effectiveness

Reasons Behind Security Architectural Disaggregation

There are numerous factors driving this disaggregated security architectural model:

1. **Hybrid IT Environments**
   The growth of cloud and industrialized services (aka operational technology [OT]) and the decline of traditional data-center outsourcing indicate a massive shift toward hybrid infrastructure services. Adoption of hybrid IT is one of the most aggressive DX trends. The vast majority of enterprises now run a mix of on-premises and cloud-based data-center environments, and cloud adoption not uniform with 80% of organizations expecting to combine private and public clouds by 2021.[2] Additionally, 83% of workloads will be processed in the cloud by 2020.[3]

   Hybrid IT environments reside in silos that are disconnected and thwart security transparency and centralized policy controls. This incurs more manual processes for already strapped cybersecurity teams. It also degrades organizational security postures by slowing threat-intelligence sharing, which is particularly problematic when threats are becoming more advanced and employ multiple attack vectors simultaneously.

2. **Digital Transformation Expands the Attack Surface**
   CIOs are charged with driving DX through widespread cloud adoption, incorporating IoT devices, and expanded mobility. While DX accelerates certain business operations and introduces new capabilities, it simultaneously increases risks. And organizations are now finding that their existing security infrastructures weren't designed to keep pace with these changes.

For example, DX distributes the reach of a network in ways that it no longer has a clearly defined and defensible boundary. Without these discernible boundaries, traditional security solutions simply cannot adapt fast enough to protect the network.

These vulnerabilities aren't going unnoticed by C-level leadership. Cybersecurity Ventures reports enterprise security budgets trending upward and predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively from 2017 to 2021.[4] But spending alone cannot correct the course of what's wrong. Leaders must simultaneously revisit their security strategy in lockstep with DX adoption to address several key problem areas at an architectural level.

Operations and protocol frequently change as a result of digital transformation. This causes connection breaks between security products and threat intelligence feeds. It even breaks connections, API security connections, and nonsecurity technologies.

3. A Lack of Integration Means Disconnection

A distributed network means that data resides in multiple places—in physical networks and in private, public, and hybrid clouds. Data must be protected regardless of its location—on-premises or in the cloud—and whether it is at rest or in motion. In the past, when a new vulnerability or attack vector appeared, organizations would simply add a new point security product to stop threats from penetrating the network at that point of entry. This stopgap strategy led many organizations to establish de facto security architectures, comprised of a patchwork ensemble of isolated security tools from multiple vendors scattered across the network infrastructure.

In addition to the patchwork of security products, DX is driving the adoption of disparate technology vendors and platforms. Examples include the cloud (Software-as-a-Service [SaaS] apps and Infrastructure-as-a-Service [IaaS]/Platform-as-a-Service [PaaS] cloud services such as AWS, Google, Azure, Oracle, and IBM), information technology service management (ITSM) tools, identity and authentication management services, and DevOps products and tools. Deployed at different times and in silos, these varied solutions do not talk to each other and create communication gaps. Additionally, many of these solutions do not connect with the disaggregated security infrastructure.

These integration limitations prevent transparent visibility and centralized controls across these disparate, multivendor environments. This makes it hard to identify and fix security gaps while creating extra work for an already stretched security team. When organizations must account for things like increasingly strict industry, governmental, and security compliance requirements, manual compilation of compliance tracking and reporting requirements increases both risk and staff burden.

4. Complexity

Complicating these issues even further is the fact that there are numerous dynamic entities within the network that impact security operations. Elastic workloads can fluctuate from small to large every time a workload moves. Operations and protocols constantly change in the DX world. This results in connection breaks between security products and threat-intelligence feeds. Frequent breaks also occur between API connections and nonsecurity technologies (cloud, ITSM, software-defined wide area networks [SD-WANs], and single-sign-on/identity management).

This tangle of problems forces IT leaders into a reactive security mode, where security policies are manually updated—a difficult and time-consuming undertaking. Disaggregated multivendor security requires staff to juggle separate consoles for tracking and managing operations of the different products and makes it hard to achieve unification of policy. Without clear visibility of traffic, it becomes extremely difficult to determine and track if security is keeping up with all the frequent changes in the network. Manual processes are not only burdensome to administrators—they also increase risk of unattended vulnerabilities and security gaps.

5. More Threats, Fewer Skills

Rapidly evolving threats grow in velocity, volume, and variety every day. A robust cyber crime ecosystem enables fast creation of new threat versions that increase their odds of success. For example, cryptojacking malware more than doubled in Q1 2018 over the previous quarter to impact 28% of companies surveyed in a recent report.[5] And the emergence of zero-day marketplaces is making it increasingly easy for black hats and hacktivists to buy the latest and greatest exploits.[6] It thus almost goes without saying that the severity of the current advanced threat landscape demands a security posture that is proactive and able to respond in virtual real time.

And while threats are getting more threatening, security IT leaders struggle to fill many skilled positions on their teams. Estimates run as high as 1 million unfilled cybersecurity jobs worldwide. More than 50% of IT leaders indicate that a shortage of cybersecurity staff has increased the workload on existing staff. Additionally, 35% have compromised on filling roles with the right skills and experience. All of this increases risk, with over half of organizations disclosing that they have experienced at least one cybersecurity event that can be tied back to lack of security training and staff resources.[7]

This situation creates a perfect storm of vulnerability. Security products don't connect to each other or with critical nonsecurity components. This makes more work for IT staffs to manage, but there aren't enough skilled people available to hire. And at the same time, threats are multiplying.

6. DevOps is Particularly Vulnerable

Companies are prioritizing DevOps—86% of respondents to a recent study reported DevOps as part of their future IT strategy.[9] But because security isn't integrated into DevOps, there are some farther-reaching business impacts to consider.

DevOps naturally depends on sharing highly sensitive intellectual property and confidential information such as API keys, SSH keys, and privileged account status. But that information often isn't secure. Because of its relative immaturity, DevOps security can be an afterthought. Less than half (46%) of respondents to a recent report say that security teams are integrated throughout the entire DevOps process. And three-quarters of organizations lack security for privileged DevOps accounts—if just one password or piece of data is stolen, it could have catastrophic consequences.[10]

Even when security is in place, problems remain. Protocols and operations in DevOps environments constantly change—breaking the connection with security, which must then be manually reconnected (as described previously). These slow manual processes create security gaps. When a dynamic object changes, the dynamic policy change should be reflected in the security policy without delay to minimize risk exposure.

But perhaps more importantly in the demanding world of DevOps, this increased latency also reduces agility, hampers time to market for new applications, raises total cost of ownership (TCO), and makes it difficult to achieve scale. Without integrated security (such as identity protections to manage access), DevOps will fail. This is precisely why IDC predicts that security-led development will be a primary focus for 90% of organizations by 2020.[12]

Security For DX Must Be Connected

According to a recent Forbes article, "Of the features deemed non-negotiable, organizations are looking for something that provides end-to-end security, both on-location and on-premises, with dynamic secure connectivity to multiple clouds. Not only is 'secure connectivity' needed and table-stakes—but so is securing the application, user, location and device."[13]

There will be **3.5 million unfilled cybersecurity jobs** by 2021, up from 1 million openings last year.[8]

DevOps and Automation

Organizations are turning to DevOps workflows to achieve transformative velocity and innovation, but they're not prepared or staffed to manage the security of these environments. Many organizations simply task the same DevOps practitioners—often who have no security experience—to protect these environments, in addition to the numerous other responsibilities they have to deliver. That's no longer sufficient, especially considering the increasing threat surface in DevOps workflows and the associated risks in managing the scripts, platforms and systems used in automated workflows.[11]

[1] "Verizon 2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[2] "IDC FutureScape: Worldwide IT Industry 2018 Predictions," IDC, October 31, 2017.

[3] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

[4] Steve Morgan, "2018 Cybersecurity Market Report," Cybersecurity Ventures, May 31, 2017.

[5] "Global Threat Landscape Report for Q1 2018," Fortinet, May 16, 2018.

[6] Ibid.

[7] Jon Oltsik, "Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)," ESG and ISSA, December 15, 2016.

[8] Steve Morgan, "Cybersecurity Jobs Report 2018-2021," Cybersecurity Ventures, May 31, 2017.

[9] "New Study Shows Cloud Adoption Boom is Fueling the Transformation of IT," SUSE, October 17, 2017.

[10] Brandon Vigliarolo, "Report: DevOps has gone mainstream, but DevOps security hasn't followed suit," TechRepublic, November 8, 2017.

[11] Elizabeth Lawler, "DevOps Security Watch: Three Trends to Track in 2018," CyberArk, February 14, 2018.

[12] "IDC FutureScape: Worldwide Developer and DevOps 2018 Predictions," IDC, October 2017.

[13] Kelly Ahuja, "Preparing The Network For A Multi-Cloud World," Forbes, January 4, 2018.

[14] "General Data Protection Regulation (GDPR)," Intersoft Consulting.

[15] "Art. 32 GDPR | Security of processing," Intersoft Consulting.

October 26, 2019 3:27 AM

58160-B-0-EN

D:\Fortinet\White Paper\Refresh- Problems Connected Education\wp-FA-broken-and-disconnected-a-new-approach-to-security-connections-is-needed