FORTINET®

HOW DIGITAL TRANSFORMATION IS IMPACTING MANAGED SECURITY SERVICE PROVIDERS

And the Resulting Business Potential

WHITE PAPER

Many organizations are reinvigorating their businesses with digital transformation initiatives, yet some may find themselves overwhelmed by potential security and other risks before they can reap the benefits. Managed security service providers (MSSPs) have a tremendous opportunity to address these concerns by providing the expertise to help organizations navigate digital transformation securely and productively in a managed services market expected to grow rapidly over the next few years.

DIGITAL TRANSFORMATION HOLDS BOTH PROMISE AND PERIL

As a concept, "digital transformation" is not new, nor does it have a universally agreed-upon definition. Still, it is a useful shorthand to convey the extent of digital change affecting organizations in almost every industry around the world.

Digital transformation means much more than eliminating analog forms of data generation, manipulation, and transmission. It involves rethinking and optimizing every aspect of an organization's activities, from product and service design to interactions with customers, partners, employees, authorities, and the public at large.

The potential rewards of digital transformation are far-reaching. Here are just a few benefits:

- Improved customer insight, leading to innovation and improved revenue-generating services and products
- Streamlined supply chain processes, yielding savings across the organization
- Acceleration of business processes, enabling larger organizations to move with the agility of a startup
- Heightened customer engagement, boosting customer loyalty and advocacy

What is particularly important to understand is that digital transformation has no ultimate objective. There is no way to finish the job. A successful digital organization is one that maintains a dynamic equilibrium, with superior agility, responsiveness, and efficiency in meeting ever-changing needs.

The predominant concern with such a dynamic digital environment is the expansion of the attack surface. Digital transformation pushes data to the forefront. Data is constantly in motion and communicated between different tools (servers, storage, private, hybrid, and public cloud IoT, among others). This expanded attack surface provides cyber criminals with a much larger target of vulnerabilities, making the attack vectors considerably larger and more dynamic.

A successful digital organization is one that maintains a dynamic equilibrium, with superior **agility, responsiveness**, and **efficiency** in meeting ever-changing needs.

THIS IS WHERE MSSPs COME IN

Consequently, digital transformation goes hand in hand with increased cybersecurity efforts. According to Cybersecurity Ventures, global spending on cybersecurity products and services will exceed $1 trillion cumulatively from 2017 to 2021—and digital transformation is one of the key enablers of this growth.[1]

Due to the urgency of these security efforts and the shortage of advanced security skills, many organizations are turning to MSSPs. Whether it is a practice within an existing service provider business or a dedicated cybersecurity firm, an MSSP faces significant challenges in ensuring that its security solutions and services keep pace with its clients' digital transformation.

Those challenges, however, also present an opportunity for the MSSP to achieve competitive advantage in this growing market. To understand the optimal approach to security in the context of digital transformation, it is useful to evaluate the transformation along three dimensions: data, processes, and platforms.

$1 trillion
Cumulative global spending on cybersecurity products and services from 2017 to 2021

BIG DATA SWELLS DIGITAL FOOTPRINT

Data continues to expand in volume, variety, and velocity. According to IDC, the global datasphere[2] will grow to 163 zettabytes by 2025, nearly 10x the data generated up to 2016.[3] Unstructured data, such as video, audio, and images, is becoming easier to generate, transmit, and store. Moreover, a growing network of automated intelligent sensors and embedded devices is adding to the human-generated data stores. For example, IHS predicts that the Internet of Things (IoT) market will grow to 30.7 billion devices in 2020 and 75.4 billion in 2025.[4]

This growth in organizations' digital footprints makes it harder to rely on traditional security technology. As data is distributed across networks, organizations have an increasingly limited visibility of their attack surface, making it harder to assess and prioritize vulnerabilities.[5]

Moreover, as data volumes grow, adhering to security best practices, such as routine audits, becomes more difficult.[6]

CARRIERS ARE RAMPING UP FOR IoT. ARE CISOs READY?

The emerging 5G standard—to be completed in 2020—is expected to alleviate the bandwidth crunch associated with the burgeoning IoT and new web services. Before the floodgates open, CISOs need to have comprehensive, integrated security technology and processes in place, both to protect remotely collected data and to inoculate the organization against IoT-borne threats.

PROCESS SPRAWL MULTIPLIES ATTACK OPPORTUNITIES

As businesses and their supply chains grow, they have more processes to manage. This may be the consequence of expansion into new markets or new service areas. Or, it may be the result of regulatory or other legal requirements.

As digital technologies enable self-service anywhere at any time, more applications will be running around the clock. Additionally, employees who interact with customers and partners across time zones are lengthening their organizations' business days. Thus, their IT infrastructure is "always on," expanding the window of opportunity for attacks.

Finally, cost reduction, process efficiency, and improved customer satisfaction are motivating organizations to give more line-of-business workers, partners, and customers access to systems and data that were previously restricted to a few employees within the organization. This increases the risk of unscrupulous behavior, such as downloading and sharing restricted information. It also increases the points of entry for attackers.

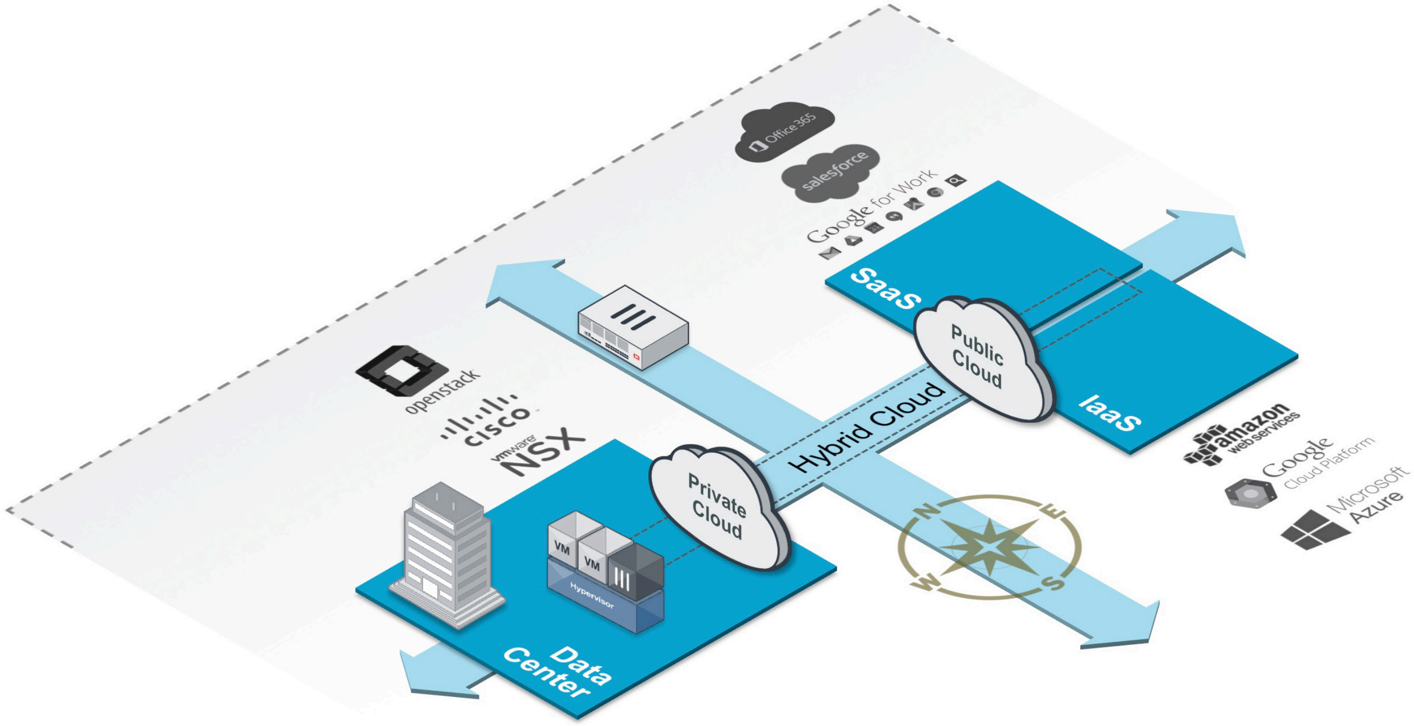
CLOUD PLATFORMS FURTHER EXPAND ATTACK SURFACE

Digitally transforming organizations need to be able to deploy applications quickly, scale them easily, and do so in a cost-competitive manner. Not surprisingly, cloud computing has become a pillar of digital transformation.

Software-defined servers, storage, and networks (SD-WAN) have enabled organizations and cloud service providers to provision server capacity and bandwidth on the fly, so workloads can run wherever it is most expedient and communications can be routed along the least-cost, highest-performance path. Although this is good news for the lines of business, it sends CISOs scrambling to track and protect increasingly fragmented, dispersed assets.

SECURITY RISKS INHERENT IN DIGITAL TRANSFORMATION:

- Growth in digital footprint
- Extended window of opportunity for attacks
- Expanded attack surface



THE COST SAVINGS AND EFFICIENCIES OF CLOUD COMPUTING ARE DIMINISHED BY INCREASED SECURITY RISKS

SECURITY: FROM DIGITAL TRANSFORMATION ROADBLOCK TO STRATEGIC ENABLER

It is easy to see how this multifaceted growth in threats, coupled with a sense of inadequacy in dealing with them, can be seen by some as an inhibitor to digital transformation. The rewards of digital business are huge, but the risks loom even larger. All the benefits that a company may gain through digital transformation—increased market share, business expansion, profitability, and customer loyalty—can be erased with a single data breach. In the case of government, infrastructure, and financial institutions, the losses can be economically devastating and even life-threatening.

In any case, the organization and its executives face legal and personal consequences if data or applications are compromised. Accountability has become a watchword for the C-suite. And security budgets have reflected this attitude. In Fortinet's recent *Global Security Survey*, more than 60 percent of respondents reported spending over 10 percent of their IT budgets on security.[7]

This is likely to grow. Each revelation of a massive data security breach spurs companies to further improve their security posture. However, it is becoming increasingly difficult for existing IT staff to meet this need. In a recent survey, ESG found that 46 percent of IT organizations have a problematic shortage of cybersecurity skills, impeding their ability to implement cybersecurity initiatives.[8] Frost & Sullivan puts this in a larger perspective, noting that there are 1 million unfilled IT security positions today, and that shortage is projected to reach 1.5 million globally by 2020.[9]

So, should organizations throttle back their digital transformation until the security issues can be addressed? Some, evidently, are inclined to do so. Research from Intralinks and the Cloud Security Alliance (CSA) cites data privacy and compliance worries as one of three crucial barriers to digital transformation.[10]

It doesn't have to be this way. As is often the case, the solution lies in a shift of perspective. Rather than view security as a fortress-building effort, it may be more useful to consider it as an insurance policy. This mindshift is key: When executives can say, "Yes, the threats are there, but we have the strategy to deal with them competently," digital transformation can move forward at a competitive pace.

MSSPS CAN LEAD THE WAY IN ENABLING DIGITAL TRANSFORMATION

Managed security services are already in high demand to help alleviate the security pressures that organizations are facing. A recent Forrester survey of companies with more than 500 employees found that half already engage an MSSP in some fashion, and 28 percent are planning on doing so in the next 12 months.[11]

MSSPs can build on their customers' trust to help them achieve the necessary mindshift to perceive security as a digital transformation enabler. Words will not suffice. MSSP product managers need to develop detailed security roadmaps based on integrated best-of-breed technologies that adapt to changing requirements. This will require reimagining the managed security service portfolio.

1.5 million

Projected global shortage in IT security skills by 2020 (Frost & Sullivan)

Among companies with more than **500** employees, half already engage an MSSP in some fashion; **28 percent** are planning on doing so in the next 12 months. (Forrester)

BEYOND NETWORK INFRASTRUCTURE: A SEAMLESS, END-TO-END SECURITY STRATEGY

For many MSSP customers, security technology is synonymous with network infrastructure, such as next-generation firewalls (NGFW). While these tools are crucial to a managed security service, MSSPs should also initiate solutions that address the inherent volatility of their digitally transforming organizations. These solutions should protect the expanding attack surface, deal with emerging threats, and detect and mitigate breaches (because they will occur), while concurrently enabling agility and transformation.

An MSSP should present these and other initiatives to clients in the context of a comprehensive network security strategy that includes event monitoring, device management, and incident response, and that addresses governance, risk, and compliance issues.

MONETIZATION OPPORTUNITIES

In theory, the security challenges and skills shortages in digitally transforming organizations should have clients beating a path to the doors of MSSPs. In practice, however, MSSPs will win and retain business only if they can demonstrate that they can deliver security services more competently and less expensively than clients can achieve on their own.

Product leaders at MSSPs who are responsible for architecting and managing the underlying security architecture of their security and network operations centers are under constant pressure to ensure they maintain legacy security-as-a-service offerings while evolving to and adding new, advanced network security services. One way is to build on a fully integrated security fabric that delivers transparent visibility across the attack surface and integrated and automated communications between each of the different pieces—both in terms of prevention, detection, and remediation. These must be deployed cost-effectively and be self-provisioned.

To meet the competence requirement, the individual service modules should be field-proven and credentialed, as should the skills of the MSSP consultants. And while service automation works to contain MSSP costs, the modular services lend themselves to bundling and differential pricing to suit different markets. This will help MSSPs derive a profitable revenue stream, while meeting the budgetary needs of each client.

CONCLUSION

MSSPs are in the enviable position of riding a bull market for cybersecurity services. Industry analysts are urging companies to get on the digital transformation bandwagon, even as they caution against the security pitfalls. As Gartner notes, “By 2020, 60 percent of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.”[12]

Most MSSPs are expected to capitalize on this trend, but not all will profit equally from it. The winners will be those that offer a flexible and comprehensive suite of foundational network security and security-as-a-service options that not only protect what exists but also adapt to emerging concerns.

AN MSSP’s SUITE OF ADVANCED SECURITY SERVICES SHOULD INCLUDE ALL OF THE FOLLOWING:

- NGFW application control
- Intrusion protection
- Antivirus protection
- Web filtering
- Web application security
- Mobile security
- Advanced threat detection, including sandboxing and threat intelligence
- Advanced threat management, including security information and event management—SIEM

“By 2020, 60 percent of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.”

—Gartner

[1] "Cybersecurity Market Report," Cybersecurity Ventures, December 2016.

[2] A conceptual "universe of data".

[3] "Total WW Data to Reach 163ZB by 2025," Storagenewsletter.com, May 2017.

[4] Louis Columbus, "Roundup Of Internet Of Things Forecasts And Market Estimates, 2016," Forbes.com, Nov. 27, 2016.

[5] Nick Ismail, "Staying ahead of the distributed cybercrime threat," Information Age, Sep. 8, 2017.

[6] Aleksandr Panchenko, "Nine Main Challenges in Big Data Security," Data Center Knowledge, Jan. 19, 2016.

[7] Patrice Perche, "Cybersecurity Needs to be Seen as a Strategic Issue, Not Just an IT Investment," Fortinet, Oct. 9, 2017.

[8] Doug Cahill, Tony Palmer, "CenturyLink Managed Security Services: Overcoming the Security Skills Gap," ESG, October 2016.

[9] Michael Suby, et al., "The 2015 (ISC)2 Global Information Security Workforce Study," Frost & Sullivan, 2015.

[10] Daren Glenister, "Collaboration in the Era of Digital Transformation: Barriers to Success," Intralinks, 2017.

[11] TC Doyle, "Enterprise Customers Turning in Droves to Managed Security Service Providers (MSSPs)," MSPmentor, June 8, 2016.

[12] "Gartner Says By 2020, 60 Percent of Digital Businesses Will Suffer Major Service Failures Due to the Inability of IT Security Teams to Manage Digital Risk," Gartner, June 6, 2016.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990