FORTINET

WHITE PAPER

Developing a Digital Innovation Security Strategy

Introduction

In today's marketplace, increasing competitiveness, meeting shifting consumer demands, and making staff more efficient and productive require enterprises to be continually evolving. Such changes run the gamut from upgrading or supporting end-user and Internet-of-Things (IoT) devices, to building fast and interactive applications, to moving entire ecosystems to multi-cloud environments. And enabling such change requires the constant selection, deployment, and replacement of a wide range of technologies.

A term currently being used to define this groundswell of change is digital innovation (DI). And for many organizations, DI is not only an opportunity but also a constant source of stress and expense. Part of the problem is the intangible nature of what is driving DI. The digital marketplace's constant state of flux makes it challenging to allocate budgets or establish a consistent strategy for success. In today's competitive economy, the only constant is change. But how do you plan and budget for something like that?

"Operating a business in today's digital marketplace includes risks that are just as sophisticated and agile as the networks being targeted. This means that securing an enterprise network demands more than just having the latest and the greatest security devices in place."

To get out in front of this, it is essential to first realize that digital innovation isn't really about technology. It is about using digital technology to solve traditional business problems in a new way. These include: How can my organization be more competitive and profitable? How can we better respond to the demands of our consumers and clients? How can we work more efficiently and productively? These are questions business leaders have been asking for centuries. DI is simply the modern process of leveraging technology to reimagine how business is done, and at a speed never before required.

The Challenge of Securing DI

It is also crucial to remember that technology is a two-edged sword. Whatever technology enables through digital innovation—agility, flexibility, scalability—can also bring disruption, the full effects of which are often only realized after the fact. With every new technology also come new cyber threats that can cause harm to businesses.

The reality is, operating a business in today's digital marketplace includes risks that are just as sophisticated and agile as the networks being targeted. This means that securing an enterprise network demands more than just having the latest and the greatest security devices in place.

One of the biggest challenges organizations face from a security perspective is that new technologies and frameworks such as software-defined wide-area networking (SD-WAN) and secure access service edge (SASE) have pushed well beyond the limits of the traditional security solutions organizations already have in place. Yesterday's collection of siloed or poorly integrated security tools, purchased as one-off solutions from a variety of vendors, can have serious implications when applied to today's distributed and dynamic network environments. Vendor and device sprawl creates visibility, control, and threat detection and response challenges for many organizations that have only been made worse by adopting DI without assessing the limits of their existing security infrastructure.

Getting to the Heart of the Matter

Over the past few years, we've seen wave after wave of new technology being promoted—public cloud and multi-cloud, IoT, big data, hyperscale data centers, and most recently, SD-WAN and SASE. Each was announced with all the accompanying hype. While each of these technologies enables organizations to compete more effectively, they can also be a major disruptive force to the enterprises that embrace them. So before any organization dives in, the critical questions to ask are, "What are these disruptions?" and "What are their consequences?"

Of course, many disruptions are just part of any normal business or technology transition. However, whenever there's a change there is also a more sinister aspect to consider because some of them can directly impact the security posture of the enterprise.

The first challenge is in understanding which is which. This requires listening, filtering, categorizing, and then taking appropriate actions. The process begins by asking the right questions, which is easier said than done.

3 Critical Questions When Considering a DI Solution

To simplify the process of selecting and preparing to adopt DI solutions, here is a list of questions every executive should be asking. They look at the operational impact, compliance, and security concerns that should be part of any exploration into adopting new DI technologies or services.

Answering these questions not only helps organizations better understand how and to what degree a new technology might disrupt their organization, but they can also shift the paradigm away from an ad hoc development approach to a rational strategy that ensures that your organization can remain competitive while minimizing disruption. They can also help ensure that organizations are strategically selecting and deploying the right technologies for their environment.

1. How will this new DI solution impact existing operations?

- **Assessing operational disruption**
  - How much time and effort will be required to incorporate this new technology into the IT workflow?
  - How much time and effort will be required to bring staff up to speed on this new technology?
  - What resources are required to deploy, manage, and optimize this new technology or ecosystem? If we use existing resources, what existing projects and efforts will be dropped or receive less attention?
- **Addressing migration concerns**
  - With a "cloud priority" edict from the executive suite, do all or just some of our applications need to be migrated? What about data or infrastructure? What are the parameters?
  - Do we have the resources we need to plan, design, secure, implement, operate, and optimize this new technology or network environment through its life cycle?
  - Do all cloud platforms work the same? How do we navigate issues when they don't? Can data, policies, workflows, and applications move seamlessly between my existing physical resources and all of the various cloud environments being implemented?
  - Can security policies be enforced consistently across different environments? What about workflows and applications that have to pass between different cloud environments?
  - How can we nondisruptively migrate hundreds of remote sites using outmoded technology such as multiprotocol label switching (MPLS) to implement new technology such as SD-WAN?
- **Supporting additional technologies**
  - Do my teams have the right skill sets and experience needed for the technology? For example, do our DevOps teams have the right security skills to ensure cloud environments and applications are properly configured and protected?
  - If not, where do we get the right training or personnel?
  - Can artificial intelligence and other nonhuman advancements help carry the operational load?
  - How do I integrate a managed service?

2. How will this new technology impact regulatory and industry compliance?

- **Meeting compliance requirements**
  - Are configurations able to be applied consistently? How can we know if a configuration is out of compliance?
  - Is intellectual property and customer personally identifiable information (PII) being appropriately protected? Can we see and track data across multiple environments?
  - How do we apply specific regulatory requirements to new technologies or network environments?

- **New technology often means new suppliers**
  - What level of trust do I extend to outside organizations and personnel?
  - How do I integrate new suppliers and vendors into existing practices and procedures?
  - How do I ensure that individuals and devices only have access to the tools and resources they need to do their jobs?
  - What is our plan in the event of supply chain disruption?

3. Will security be an enabler or a barrier to success?

- **Performance and scalability are key**
  - Will our existing security solutions be able to operate fast enough, and scale up and out sufficiently to keep up with the demands of this new solution?
  - How do we ensure that security is being consistently applied and enforced across different technologies and environments?
  - Can policies be centrally managed and orchestrated? Can we maintain our single view across our network? Can solutions deployed in different environments see and talk to each other to ensure consistent control and unified threat response?
- **Extending trust to new technologies and environments**
  - Can new cloud platforms be trusted? What about transport systems? How do we monitor and track traffic and data across a distributed environment to ensure consistent visibility, security, and policy enforcement?
  - Who has the ultimate responsibility for protecting my data? Where is the dividing line between my cloud provider and my organization? Who do I go to when things go wrong?
  - How can I be sure that the tools being used by my DevOps team are secure? How do I validate the security of tools, processes, environments, code, and applications?
  - How do I know that a product will work the way the vendor has promised it will? What about tools deployed in different environments?
- **Does this new technology increase or decrease cyber vulnerabilities?**
  - Will the network be more vulnerable to cyberattacks?
  - Are the right levels of security in place?
  - Is security being enforced consistently across the network?
  - Are workflows and applications being secured along their entire transaction chain?
  - How can security levels be measured or evaluated?
- **Defining a plan to address potential vulnerabilities**
  - Insecure IoT devices
  - Misconfigured websites
  - Compromised passwords
  - Infected devices
  - Misconfigured access control
  - Insecure internet links
  - Cloud-enabled Shadow IT

A Culture of Security—From the C-suite to the Remote Worker

The uphill battle of changing security's perception in the executive suite starts with raising awareness and correlating security's value to the business objectives of the technology. Security can be a difficult concept to sell because when it is doing its job well, nothing happens.

We've all heard that security is "everyone's job," right? Engaging everyone in an organization starts by understanding and addressing the key concerns for each member of the C-suite. Issues like brand and reputation, profitability and stock value, customer confidence, competitive advantages, regulatory and industry compliance, and employee morale all need to be part of the security conversation—both in determining what, how, and where resources need to be protected, and what sorts of solutions are needed to achieve these objectives.

But the executive suite isn't the only place where security's value needs to be highlighted. Since most enterprise IT organizations are functionally organized, cybersecurity is typically handled by the network security team, which is distinct from (some would say siloed from, or even at odds with) the other IT teams. This organizational structure once made sense, but in the era of digital innovation, IT teams need to rethink how projects are planned, and where and when the security team gets engaged in the process.

Let's use SD-WAN as an example. SD-WAN is a networking solution; therefore, the network team should manage it. But the application, DevOps, and security teams are also implicated. They should not just be consulted after an SD-WAN solution is selected, but they also need to be involved in the initial planning stages of the project. The last thing any organization wants is to choose a solution that meets the networking needs of the company, but that then requires significant cost and overhead to implement an inadequate overlay security solution. Bringing these other teams into the initial discussion is not to undermine the networking's team ownership of the project, but for each team to bring their specific perspective to the project, especially the security perspective.

There is also a third aspect of raising awareness of the value of security, and that's within the workforce. In today's enterprise, most employees are equipped with technology—most often supplied by the enterprise, but also their own through bring-your-own-device (BYOD) policies. The problem is that while that technology can be protected using advanced security solutions such as endpoint protection platform (EPP) and endpoint detection and response (EDR), there is still a significant gap in end-user awareness of the consequences of making a poor security decision.

All too often, the employee is the weakest link in the security chain, with endpoint malware and phishing attacks still comprising the vast majority of network breaches. But with commitment from the enterprise, they can be transformed into the first line of defense. Training and internal email phishing campaigns are just two tactics that an enterprise can use to raise awareness, but it can't be a "one and done" effort. Cyber-awareness training must be ongoing and regular. It needs to be engaging, making users feel like they are playing a critical role as part of the security team. And any internal phishing or hacker campaigns should be as realistic as possible and designed for employees to become victimized. Employees who become "victims" shouldn't be penalized but converted into advocates to the rest of the workforce.

Most importantly, effective security requires ongoing reinforcement from the executive level on down. It needs to be part of every discussion, from sales to shipping. Changing the perception of security, and helping individuals realize its value, can only be achieved when all three spheres—executive, IT, and workforce—are addressed and convinced and working together.

Your Opportunity for Change

It's at this point that a more in-depth discussion about security technology—including conversations about vendors and products—can take place. Every debate needs to be a discussion about how to protect the organization better while achieving business objectives, especially when being enabled by new technology. Security doesn't just support and protect digital innovation. It allows it to function as a robust and critical element of every organization's digital strategy. Innovation without security is simply unbridled risk. And that sort of risk doesn't help anybody.

Federating security across an expanding infrastructure, and reducing the challenges of a vendor-heavy environment, require a new security strategy formulated around the key principles of performance, interoperability, and scalability. It needs to combine flexible form factors with centralized controls to ensure that the same policies and protocols are being deployed and enforced everywhere across the network. Likewise, open application programming interfaces (APIs) and common standards mean that disparate security solutions can be integrated together. That also makes it possible to even weave security into the network itself, ensuring that it can dynamically adapt to rapidly evolving environments in real time.

Of course, implementing this sort of security strategy may require radically rethinking your existing security strategy. But performance, scale, flexibility, and interoperability are foundational requirements for organizations looking to protect their DI projects. And it will allow security to seamlessly adapt to the new innovations that will be deployed tomorrow, without having to redesign your security infrastructure or add an additional layer of complexity.

August 11, 2020 2:43 AM

734154-0-0-EN

D:\Fortinet\White Paper\Grey White Paper\GREY - Enterprise Messaging\wp-FA-developing-a-security-strategy-for-ongoing-digital-innovation-8112020