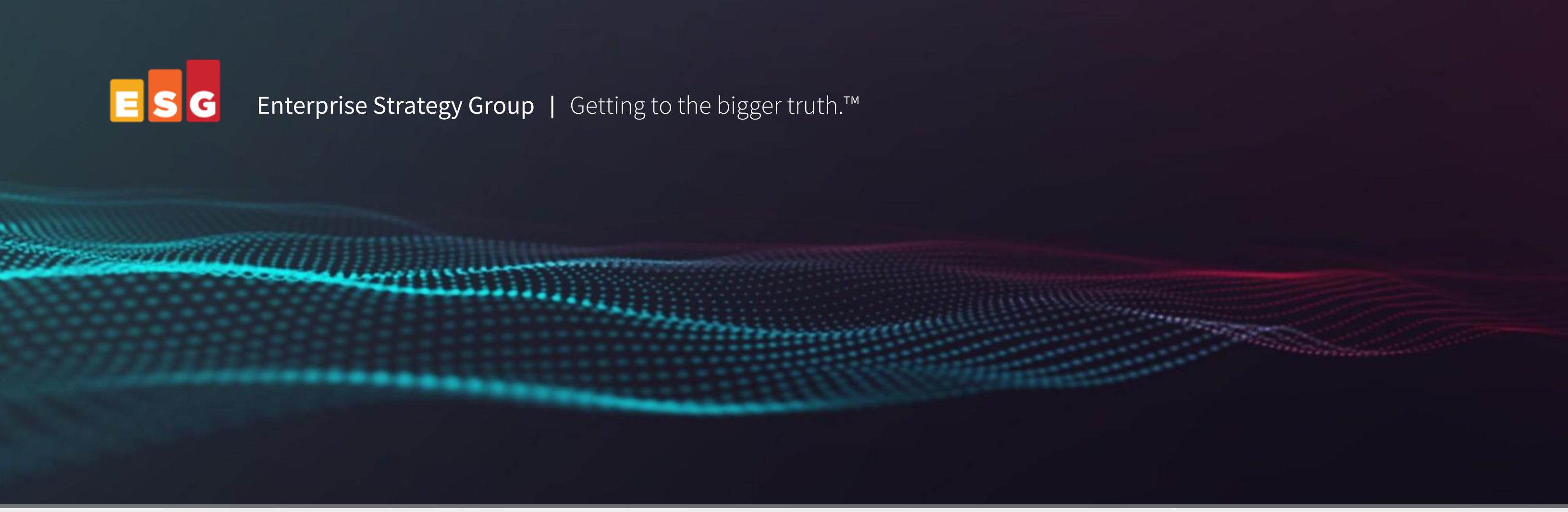


Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

New Priorities for IT Operations: Be Ready for Whatever Comes Next

A Pragmatic Roadmap to IT Sustainability with Tanium

By Doug Cahill, ESG Senior Analyst

March 2021

This ESG White Paper was commissioned by Tanium and is distributed under license from ESG.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Navigating the Challenges of 2020

Operationalizing Remote Work

The COVID-19 pandemic caused a rapid transition to work-from-home (WFH) in early spring 2020, with distributed workforces challenging IT infrastructures not designed to support such volumes of remote employees. As a result, the priority of IT operations teams was to keep the lights on and the business going. The rush to operationalize remote work did not afford the time to conduct the usual level of due diligence associated with a range of issues: scaling VPN infrastructure, tightening access/authentication policies and process, vetting personal devices not configured to corporate standards, assessing home network vulnerabilities, leveraging insecure collaboration software, and expanding cloud usage.

> **The rush to operationalize remote work did not afford the time to conduct the usual level of due diligence associated with a range of issues.**

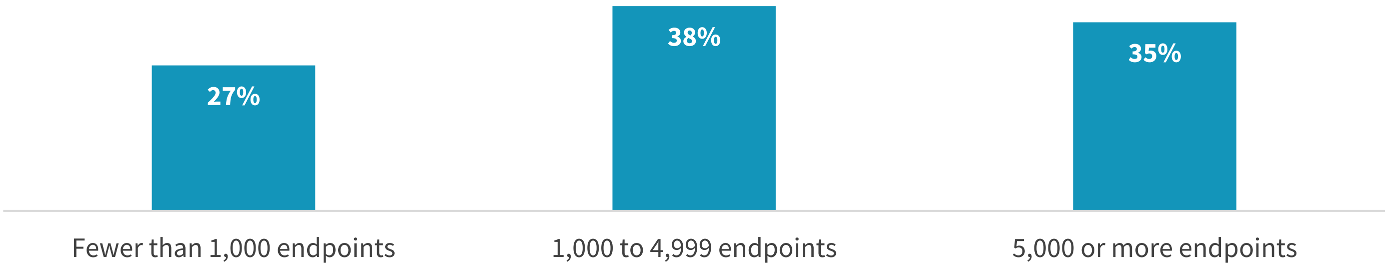
Of note, and as highlighted by ESG research, 35% of organizations reported that one of their biggest challenges supporting the increase in remote workers accessing data center resources was that it was straining their network infrastructure.[1] This indicates that the existing VPN infrastructure had difficulty meeting the increased requirement for remote access. The solution? A separate ESG research study found that 51% of respondents were already employing or planning to employ software-defined perimeters (SDP) for full-scale replacement of their VPN solutions for remote access.[2]

The shift to remote work also exposed the inadequacies of point solutions and poor IT practices. Respondents indicated that they face challenges and costs related to managing multiple disparate tools, including fifty-one percent who said increased organizational complexity, the top response, had a negative impact on their business.[3]

Additionally, while knowledge workers already were multi-device users, remote work further increased the number of devices being used to access corporate resources. To this point, 35% of ESG research respondents noted their organizations supported 5,000 or more endpoint computing devices (see Figure 1)[4].

Figure 1. Endpoint Devices IT Supports

Approximately how many total endpoint computing devices (i.e., desktop/laptop PCs, thin clients, tablets, smartphones, kiosks, etc.) does your IT organization currently support? (Percent of respondents, N=354)



Source: Enterprise Strategy Group

[1] ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021. All ESG research references and charts in this white paper have been taken from this research report, unless otherwise noted.
[2] Source: ESG Research Report, *Transitioning Network Security Controls to the Cloud*, August 2020.
[3] Ibid.
[4] ESG Master Survey Results, *Enabling Digital Workspace Strategies with VDI and DaaS*, August 2020.

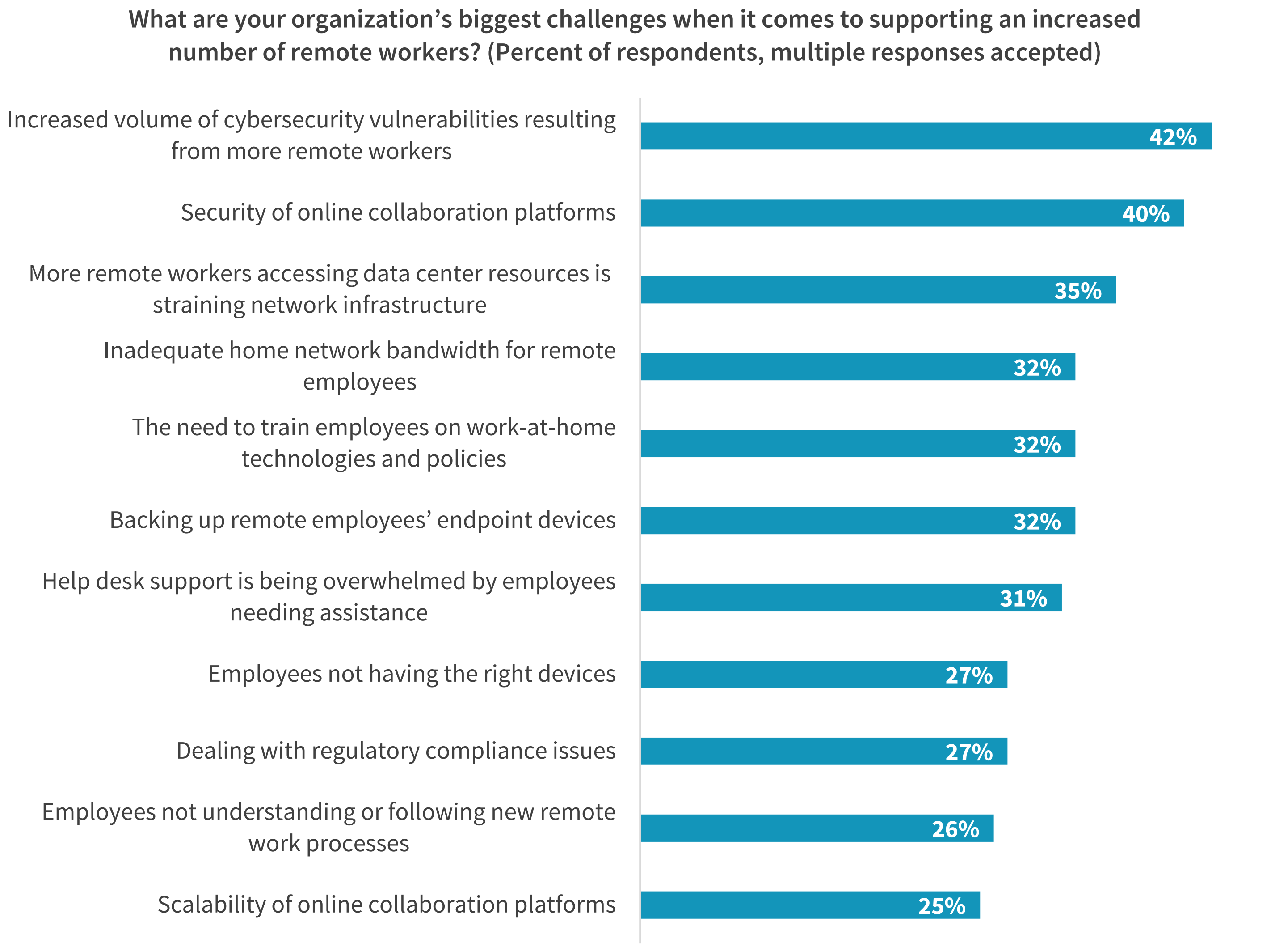
© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Remote work also necessitated accelerating digital transformation (DX) initiatives to support direct-to-cloud access patterns, further taxing IT resources. As IT operations teams regroup and plan for the future, they need to be ready for whatever comes next with a pragmatic approach to IT sustainability. Preparing for the unknown entails discerning which DX investments best can help to reduce IT complexity, improve security postures, and streamline cloud migration through adoption of a platform that enables scalability, visibility, and manageability.

Securing Remote Work

The increase in remote work brought with it yet more cybersecurity issues. For example, 42% of respondents cited an increased volume of vulnerabilities due to an expanded attack surface comprising new devices and home networks. Furthermore, an increase in cloud-based collaboration platforms created new opportunities for cyber adversaries. According to an ESG survey, 40% of organizations had significant concerns about the security of collaboration platforms for their remote workforce (see Figure 2). The fact that an organization's portfolio of cloud-based collaboration applications is sourced from multiple cloud service providers adds risk and complexity.

Figure 2. Cybersecurity Continues to Be the Top Pain Point for WFH



Source: Enterprise Strategy Group

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Determining Priorities and Next Steps

The New Normal of the Hybrid Workplace

While some uncertainties have carried over to 2021, WFH isn't one of them. ESG research revealed that 44% of organizations prefer to keep as many employees as possible working remotely as long as possible, and 48% are okay with WFH for the foreseeable future but would prefer to get most or all employees back into the office eventually. The new normal will consist of remote, on-premises, and hybrid workforces. With remote work operationalized, IT teams now have breathing room to think more strategically to evaluate recent decisions and determine what needs to be done to update and align processes and infrastructure without additional disruption. This approach sets new priorities centered on stability and sustainability.

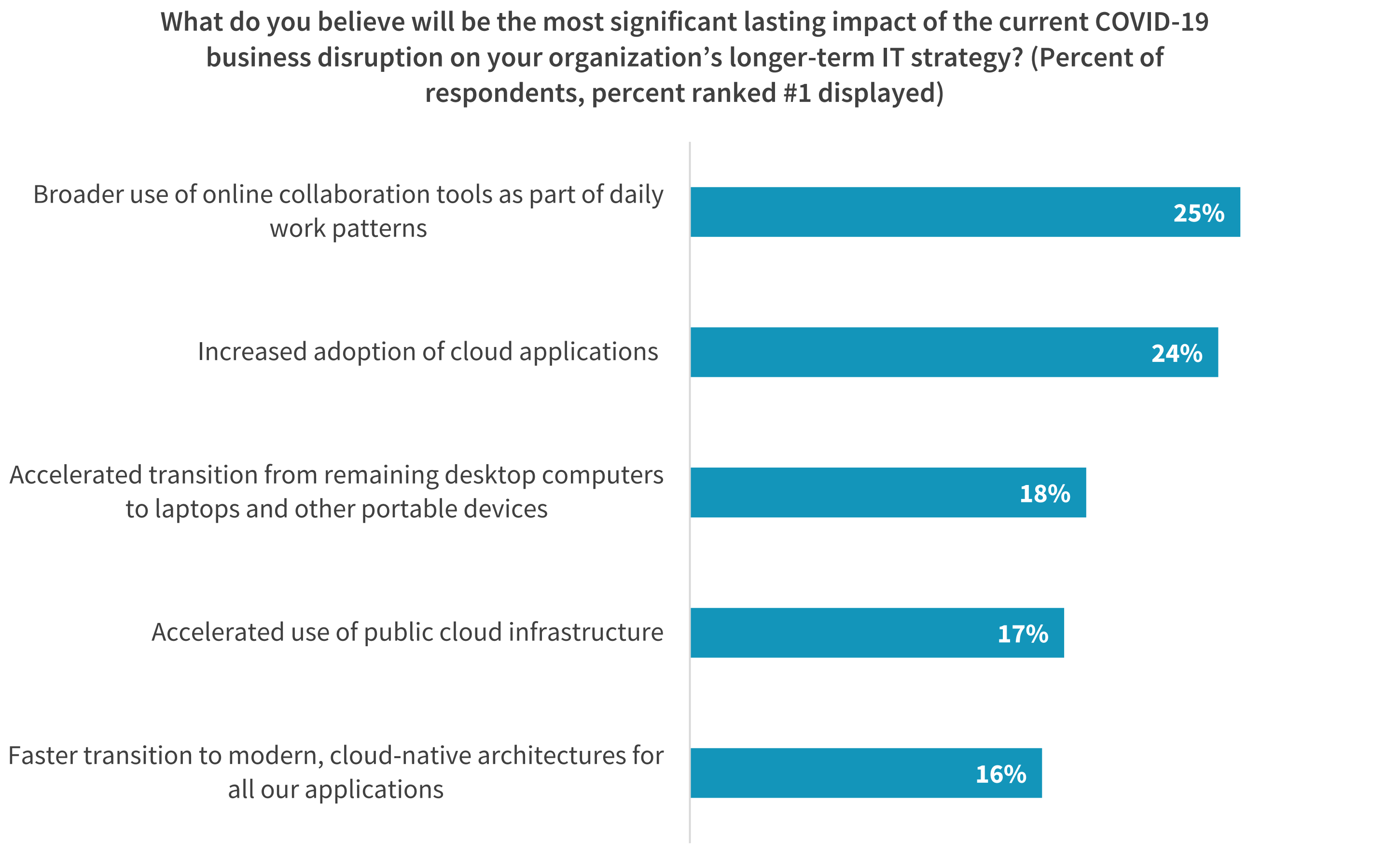
With remote work operationalized, IT teams now have breathing room to think more strategically.

IT operations teams are mulling over how to modernize IT to enable the new normal. ESG research revealed trends and challenges that will influence purchasing decisions and point to what work looks like in 2021. Such modernization clearly will include further reliance on cloud-based applications, both SaaS and those that have been internally developed. This means an expanded use of SaaS applications headlined by online collaboration tools (see Figure 3). In fact, respondents to a separate ESG research survey shared that end-user access averaged 17 applications per day.[5]

[5] ESG Master Survey Results, *Enabling Digital Workspace Strategies with VDI and DaaS*, August 2020

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 3. The Lasting Impact of COVID-19 on IT Strategies



Source: Enterprise Strategy Group

Securing a mix of technologies is a clear priority for today's digital leaders. Nearly half of organizations surveyed by ESG reported that fortifying cybersecurity is a top priority driving IT spending at their organizations in 2021. This is an expected finding given the aforementioned cybersecurity challenges resulting from the increase in remote work. Solving cybersecurity challenges depends on the ability of IT operations teams to do their jobs both efficiently and effectively. At the same time, hybrid workplace environments continue to increase IT complexity. Improving cybersecurity depends on solving other common IT conditions:

- Lack of enterprise-wide visibility, poor centralized control, and inconsistent policy enforcement—a problematic trifecta that increases cyber risk.

- Endpoint device management to assure that employees are using properly configured and, thus, secure devices. This is achieved by running updated operating systems, full disk encryption, personal firewalls, automated patching, current antivirus software, and more. Indeed, ESG research revealed that more than one-third (35%) of organizations in North America believe that the increase in both the number and type of endpoint devices they must support is one of the key drivers of heightened IT complexity.

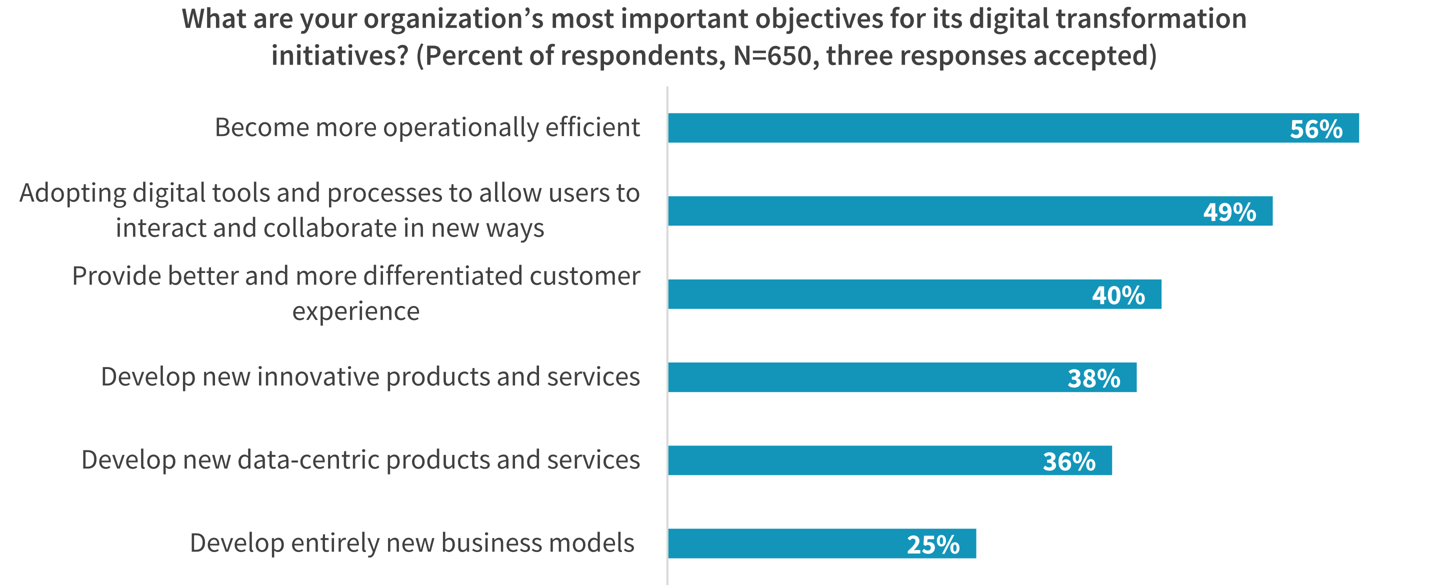
- A plethora of disparate IT tools that cause staff to spend precious time reconciling information that may or may not be actionable.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Digital Transformation Has Become a Strategic Imperative

An expansion of cloud consumption is part and parcel of digital transformation initiatives. To this point, organizations pursue DX in different ways, of course, but 45% of organizations have a cloud-first strategy for deploying new applications. Developing cloud-native applications saves time and money; eliminates forklifting, re-platforming, and refactoring; and assures scalability. These business benefits support the most important DX objective for more than half of the respondents to ESG's 2021 technology spending intentions survey: operational efficiency (see Figure 4).

Figure 4. Operational Efficiency is Top Objective for Digital Transformation



Source: Enterprise Strategy Group

To support realizing greater operational efficiency vis-à-vis DX initiatives, IT operations teams will need to consider inefficiencies of siloed tools and processes that hinder their ability to enable and secure a hybrid workplace. This issue portends adoption of technology platforms, including those that manage disparate devices. None of these challenges and trends exist in a vacuum. Solutions that put organizations on the high road are those that address multiple pain points and deliver positive outcomes across multiple areas of the business.

Routes to IT Sustainability

As IT leaders develop their roadmaps, they recognize the emergence of imperatives for 2021 and beyond:

Converge to Platforms

To gain operational efficiencies, many organizations now seek to alleviate point tool fatigue with a platform approach and the integration this provides. When it comes to cybersecurity—an area often characterized by the use of a significant number of point tools—92% of organizations agree that a cybersecurity product's ability to integrate with others is an important consideration of their security product procurement criteria. In fact, more than three-quarters of the respondents from the same ESG research study note that their organizations are actively consolidating the number of cybersecurity vendors with whom they conduct business. Why? Fifty-one percent cited gaining greater operational efficiencies realized by their security and IT teams as a top value of doing so. [6]

[6] ESG Research Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment*, March 2020.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Leverage Automation for Agility

Integrated, automated tools and processes that span on-premises, distributed, and cloud environments can bridge skills gaps, accelerate transformation, allow the business to become more agile, and bolster security posture/architecture. As a result, organizations can:

- Unite operations and security teams by providing a single set of data that streamlines IT operations, which improves decision-making related to technology changes and enables agile project teams as a core tenet of modern application development.
- Improve scale without the management and cost considerations of secondary servers required by traditional tools.
- Reduce IT complexity related to diverse workforces and data management logistics for remote, on-premises, and hybrid workforces.

Embrace the Move to Cloud

The self-service nature of SaaS applications that offer fast time to value clearly supports the agility imperative of DX initiatives while enabling workflows that create new business opportunities. In addition to agility, other benefits accrue from leveraging public clouds, refactoring legacy applications, and shifting to cloud-native application development. Fully embracing such moves to the cloud should entail the following considerations for organizations of all sizes:

- Continuous visibility. A focus on visibility centered on asset discovery inclusive of devices, software, and services from which risk assessments can be made and policies created. For application development projects, an inventory should include hardware and software assets and how they are used to help identify which applications to migrate. As cloud-native environments are dynamic, the discovery of assets needs to be continuous.
- Scalability and performance. Cloud-native applications are elastic to dynamic load requirements and more easily deployable at the edge, minimizing latency for direct-to-cloud use cases.
- Integrated security. Modern methodologies, such as DevOps, can introduce best practices like

Spotlight on Tanium

Tanium offers an endpoint management platform that integrates management as well as risk and security capabilities into existing infrastructure, applications, and processes across end-user, cloud, and server endpoints. This approach simplifies IT operations, digital transformation, and cloud migration. Flexible deployment models include cloud delivered as a service and on-premises customer-managed options. Through a single view, IT teams operate with the visibility and control they need to:

- Discover, inventory, and manage assets.
- Monitor asset health with tools that automate software management, patching, performance monitoring, and configuration management.
- Enhance protection by scanning assets, detecting threats, and remediating risk and misconfigurations.
- Integrate tools such as CMDB, ITSM, and SAM.
- Improve alignment of security and IT operations teams to promote collaboration and foster a shared mission.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

vulnerability management, configuration management, auditing, and more at each stage of the application lifecycle.

Close Security Vulnerabilities Across the Attack Surface

Three-quarters of respondents to ESG's 2021 technology spending intentions survey believe their organizations are more complex than they were two years ago. Asked why their IT environments have become more complex beyond the impact of remote work, 32% cited an increase in the number and type of endpoint devices as one of the reasons. As such, modern, unified vulnerability and configuration management tools must provide the visibility and control needed to secure the complicated heterogeneous mix of devices, locations, applications, and infrastructure. Essential capabilities for closing security vulnerabilities include:

- Continuous monitoring and asset discovery, real-time information about misconfigurations and potential threats, and remediation tools, all within a single agent and console.
- Flexibility to adapt to many requirements to support compliance with internal and external standards. Reducing the attack surface is required by regulations, such as PCI DSS and HIPAA, as well as newer data privacy regulations, including CCPA. Fortunately, industry frameworks provided by the Center for Internet Security (CIS) and NIST offer guidelines and best practices.
- Automated patch management and software management.
- Integrations with the stack of technologies employed by IT, security, and DevOps teams to leverage investments.

The Bigger Truth

Last year IT teams did what was necessary to keep the business operating under difficult conditions. With the pandemic yielding a hybrid workplace for the foreseeable future, IT teams are accelerating digital transformation initiatives as they better understand how to stabilize, optimize, and sustain remote, on-premises, and hybrid workforces.

Modernizing by converging to platforms, leveraging automation for agility, embracing the move to cloud, and closing security vulnerabilities offer clear benefits for both business and IT leaders who will be better equipped to:

- Assess the business' risk posture to inform technology and operational decisions.
- Strengthen cybersecurity programs without impeding knowledge worker productivity.
- Maintain superior IT hygiene as a foundational best practice.
- Increase business agility with cloud-delivered, as-a-service solutions.

Many of the objectives discussed in this report have been to date mutually exclusive: greater agility and efficiency, insight, manageability, and a reduction in the attack surface to manage risk. A cultural shift to collaboration between IT operations and security operations is paramount to demystifying such a perspective and yielding an outcome of moving fast, safely, and with assurance. Organizations pursuing these benefits will want to consider technology partners who provide solutions that enhance and secure their DX journey.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com ✉ contact@esg-global.com ☎ 508.482.0188

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.