DELL Technologies

vmware

The State of Cybersecurity 2021

Security realities, IT priorities, and the road toward Zero Trust

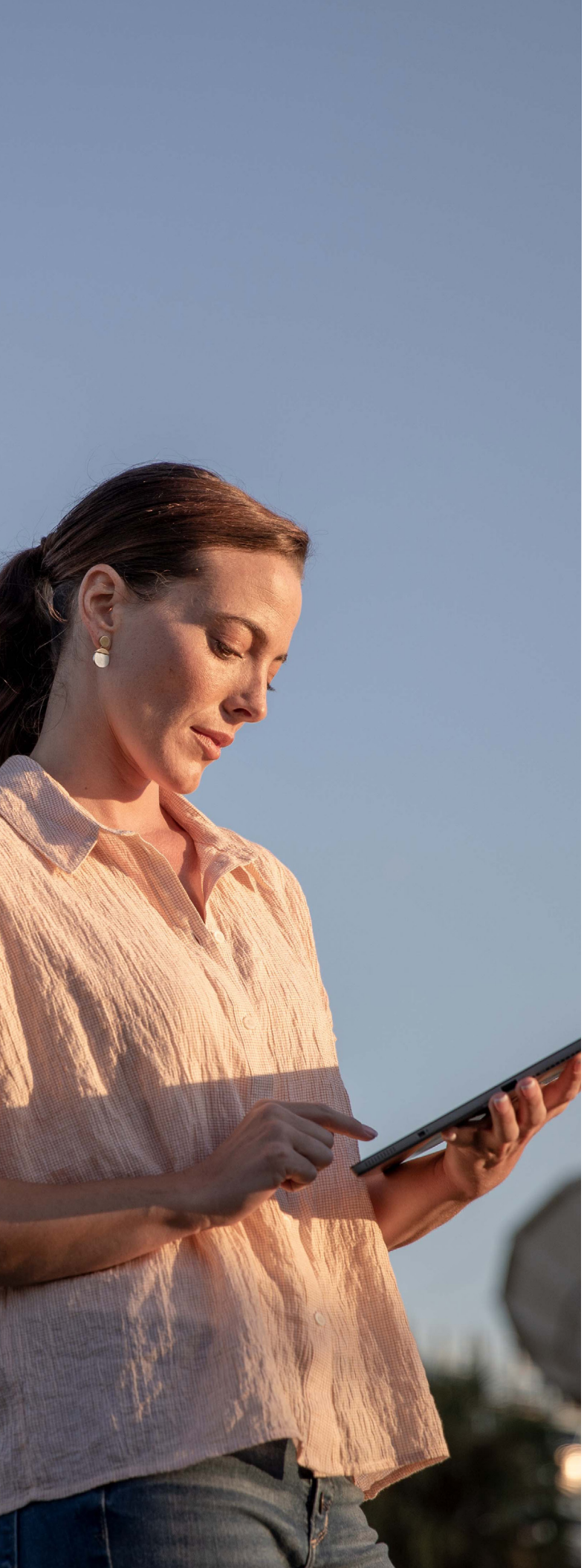


Table of contents

Introduction

Cybersecurity is always a moving target. In 2021, that movement was still driven in large part by the continuing effects of the COVID-19 pandemic. The acceleration of hybrid and remote work over the last two years means that more users than ever are located outside the traditional corporate firewall, often connecting over untrusted networks. In addition, more computing workloads are either on the public cloud or run on virtual machines which could be hosted anywhere.

With these changes in mind, we asked 452 cybersecurity decision makers at companies of all types and sizes about what changes they are making or planning within their IT security ecosystems over the next few years. Their responses provide insights into their cybersecurity needs and priorities at a broad level, and more practically at how they intend to adjust their security investments across six key aspects of IT:

Endpoints/ Devices | **Users** | **Connections** | **Applications/ Workloads** | **Operations**

Both hybrid / remote work environments and widely distributed computing resources have sparked ever greater interest in security based on Zero Trust principles, and that's reflected across each of these areas. These factors don't stand alone, however; the current security context also includes the need for:

- Flexible, automated, policy-driven security, rather a patchwork of ad-hoc decisions
- Greater portability, scalability, speed of deployment, and security for application workloads
- A risk-based approach to data protection
- Detection, response, and recovery capabilities to complement prevention strategies for security
- Improved user experience
- Greater efficiency in the face of a sustained cybersecurity workforce shortage

CHAPTER 1:

Getting to Zero Trust

Zero Trust security architecture means that access to resources is never based on simple one-time authentication or inherently trusted systems. Instead, it's conditioned on demonstrating and sustaining a pre-determined level of assurance or trust. That assurance is gained via a combination of security methods and tools such as authentication of both users and systems, multifactor authentication, and ongoing examination of factors such as systems' health and patch level. In order to actually put Zero Trust into action, organizations must be able to define trust levels, and enable the systems which allow that trust to be established.

WHAT IS ZERO TRUST?

A security model built on the following:

- Anything inside or outside the organization is not trusted by default
- Everything trying to establish a connection must gain / build trust
- Authentication and authorization must happen before trust can be built — and can be repeated to re-affirm trust

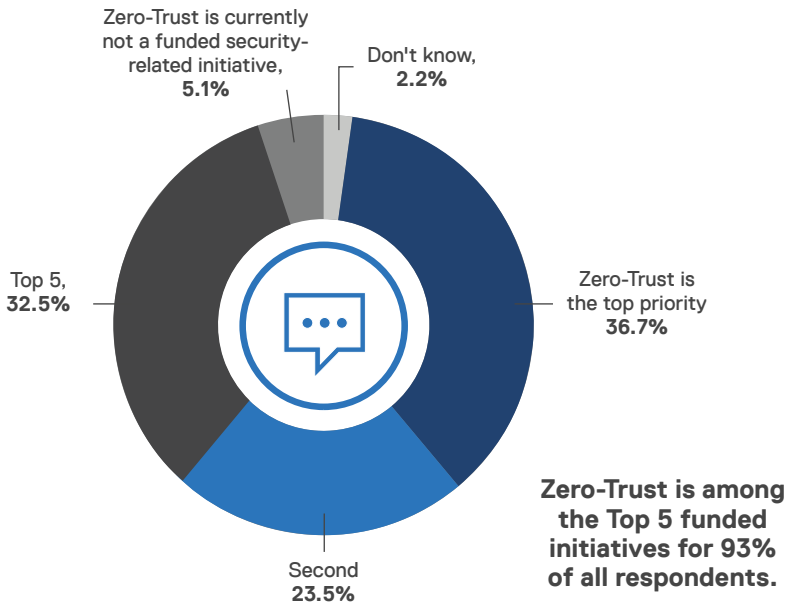
An architectural framework that is:

- **User-centric:** Everything starts and centers around the user acceding the service or resource
- **Service-oriented:** Makes it easier to create and consume reliable services with granular
- **Based on intrinsic security:** Every action is scrutinized in the context of its risk

Asked how long their Zero Trust initiatives would take to implement, participants reported a median time of between two and three years, with some expecting the effort to last five years or even longer. That broad range of timeframes reflects the fact that Zero Trust, like any large security goal or initiative, is a multi-part endeavor that requires planning and evolution. Realistically, implementing Zero-Trust is a multi-year journey to be approached in phases, with many possible starting points. Every organization has its own internal priorities, as well as its own existing security stance in each of the essential areas of trust, from endpoints to operations.

For companies that haven't already begun the journey to Zero Trust, however, that move isn't only in the future. Zero Trust security has already made the cut as a priority and a budget item for IT departments. In fact, for 93% of participants in our survey, it is among the top-five funded initiatives heading into the 2022 budget year. More telling is that for almost 60%, implementing Zero Trust solutions is actually in the top two priorities—and for more than one third (37%), it's the number-one priority.

ZERO TRUST AS A BUSINESS PRIORITY



Zero-Trust is among the Top 5 funded initiatives for 93% of all respondents.

ZERO-TRUST IN THE TOP 5

94%
IT (security)

88%
IT (non-security)

95%
Busniess leaders

85%
Technical experts

Given the variety of ways that organizations might start with deploying Zero Trust solutions, respondents were asked to define the order in which they planned to approach each of several areas. In this report, we describe trends in Zero Trust in order of the overall priorities they described, starting with data protection.

HOW CYBERSECURITY PROFESSIONALS RANKED THEIR SECURITY PRIORITIES

Priority/ Sequence	Endpoints/ Devices	Users	Connections	Applications/ Workloads	Data	Operations
1	62	84	64	50	105	87
2	75	75	86	69	81	66
3	73	81	77	82	69	70
4	85	76	72	84	69	66
5	70	62	81	83	60	96
6	87	74	72	84	68	67
	452	452	452	452	452	452

CHAPTER 2:

Applying Data Security

Given the onslaught of highly public, often costly malware attacks seen in recent years, it's not surprising that the top priority for the largest number of survey participants is the protection of data. Whatever systems surround that data's creation, protection, and use, safely storing and delivering the data itself is the purpose of any organization's IT infrastructure. Additionally, many national and state-level jurisdictions impose strict regulations on data handling, particularly when that data can be traced to identifiable individuals.

For each of the several areas in which organizations might implement Zero Trust technologies, we looked at the percentage of respondents expecting deployment over the next 12 months compared to the percent reporting current deployment. Looking through this lens at technologies and processes that relate to trusted data, the two areas of highest anticipated growth are **data governance** and **data classification**.

Data Governanace

Data Classification

A greater focus on these areas, particularly data governance, demonstrates an increasingly risk-based approach to data protection, compared to reactive solutions or coarse-grained lockdowns.

While governance—the process of making top-level decisions about data—may overshadow front-end data classification, classification is also key to deploying Zero Trust Architecture (ZTA). That nearly one third of respondents (29%) report near-term classification efforts shows increasing sophistication in the ways organizations think about data, starting with the question "Is this data worth protecting or not?"

Beyond that initial classification, governance helps address a litany of questions about proper data handling: Where is the data? Who has the data, who should have it, and how should it be protected?

All of these questions inform the issue at the core of good data governance: What is the organization's tolerance for risk? In the absence of a formal governance policy, data security decisions are nonetheless made constantly – but in an ad hoc manner, rather than based on business implications.

When considered in the context of ransomware, as well as other potentially destructive malware, it is eye-opening that one third of all respondents report that their organizations have deployed neither data backup and recovery nor data encryption. While this presents a potential danger, it can also be seen as a kind of low-hanging fruit. Implementing these basic tools would mean a substantial upgrade to their organizations' security posture. In contrast, the absence of backup, recovery and encryption tools may simply reflect personnel and budget shortfalls, rather than inattention or lack of interest.

On the whole, the results show a positive trend: that companies are moving toward adopting a policy of measured risk.

ZERO TRUST SECURITY INITIATIVES

	Currently Deployed:	Plan to deploy < 12 months	Plan to deploy > 12 months
Data Governance	48%	36%	9%
Data Backup and Recovery	69%	20%	9%
Data monitoring and filtering	54%	27%	12%
Database encryption	58%	26%	12%
Server encryption	62%	23%	12%
Endpoint encryption	60%	24%	12%
Data integrity	55%	28%	13%
Data classification	51%	29%	12%

CHAPTER 3:

Safeguarding Users

None of the hallmarks of Zero Trust security—adaptive and multifactor authentication, context awareness, risk-scoring, transparency to users—are completely novel, though their implementation has often been piecemeal and uneven.

With the sustained shift towards remote / hybrid work, a renewed focus on protecting users, and improving their experience, is an obvious priority for many organizations, coming in as the second-most important area to our respondents. By applying user-centric Zero-Trust tools in concert, and in combination with high-level policy approaches, both aims can be met.

Our survey revealed that the fastest-growing areas surrounding user trust are adaptive authentication, multi-factor authentication, and various approaches to password-less authentication. All of these fit neatly into the Zero Trust model by doing away with naively trusted login:password pairs in favor of richer authentication.

Changes in authentication also demonstrate an increased focus on improving the user experience, another especially important factor in the work-from-anywhere era. Users may now have to figure out more problems on the own, rather than with the help of an IT professional. Selectively easing access to less vital systems with heuristics and single sign-on means that users are less likely to waste time in authentication, or face password hurdles.

PROTECTING USERS WITH ZERO TRUST

	Currently Deployed	Plan to deploy < 12 months	Plan to deploy > 12 months
Policy decision point for automated, real-time access decisions	46%	26%	15%
Login behavior monitoring / analysis	48%	32%	12%
Multifactor authentication via hardware token	47%	30%	11%
Multifactor authentication via app	50%	30%	13%
Adaptive authentication	40%	32%	15%
Email + one-time link	38%	30%	14%
Email + “magic link”	30%	30%	15%
Password-less authentication	35%	27%	14%
Username / password	69%	21%	8%

CHAPTER 4:

Putting Operations Security in Place

At the level of actually operating an organization, approaches are available that don't readily map to protecting individual users or existing data. The implementation of **detection and response capabilities**, including **managed detection and response** solutions, shows the highest growth anticipated in the next 12 months in the trusted operations domain.

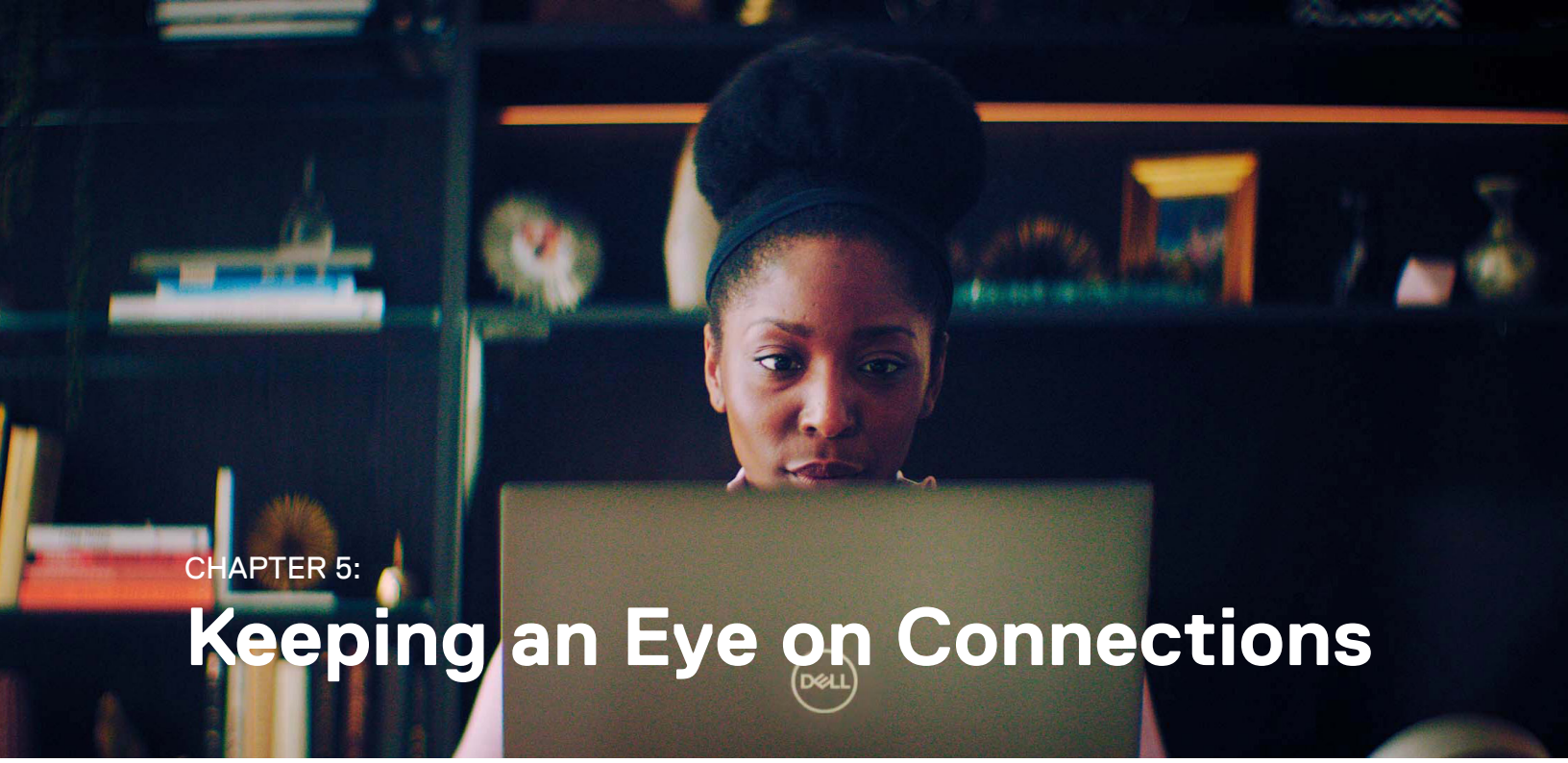
That security pros put so much attention in this area underscores that prevention alone is not sufficient; deeper security of the kind Zero Trust is intended to deliver requires conventional preventative measures, but also robust detection and response systems.

Determining the right level of risk tolerance hinges on understanding what threats face a system, and that is a large part of what such analytical systems deliver. When prevention and detection fail, as they inevitably will at times, both response and recovery systems are necessary for a complete security infrastructure.

The importance placed on technologies to advance security operations reflects the ongoing need to adapt to a sustained cybersecurity workforce shortage, which was a persistent challenge even before the current pandemic. To that end, among the strategies we see being employed is workforce automation in the form of AI tools, machine learning, and the use of managed services.

PROTECTING USERS WITH ZERO TRUST

	Currently Deployed	Plan to deploy < 12 months	Plan to deploy > 12 months
Advanced bot detection and mitigation	41%	26%	17%
Third-party threat intelligence	48%	26%	14%
Managed detection and response (MDR)	46%	31%	11%
Extended detection and response (XDR)	40%	31%	13%
Network detection and response (NDR)	54%	23%	15%
Endpoint detection and response (EDR)	54%	25%	13%
Security orchestration, automation, and response (SOAR)	41%	28%	14%
Security information and event management (SIEM)	50%	28%	13%
Log management	51%	26%	16%

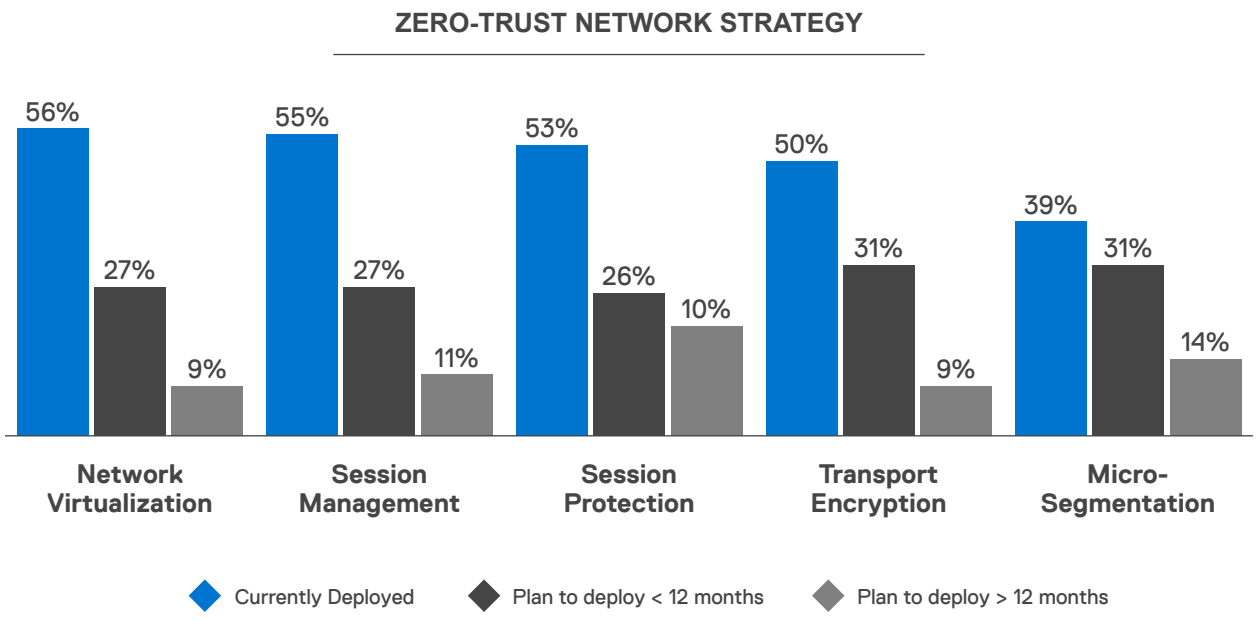


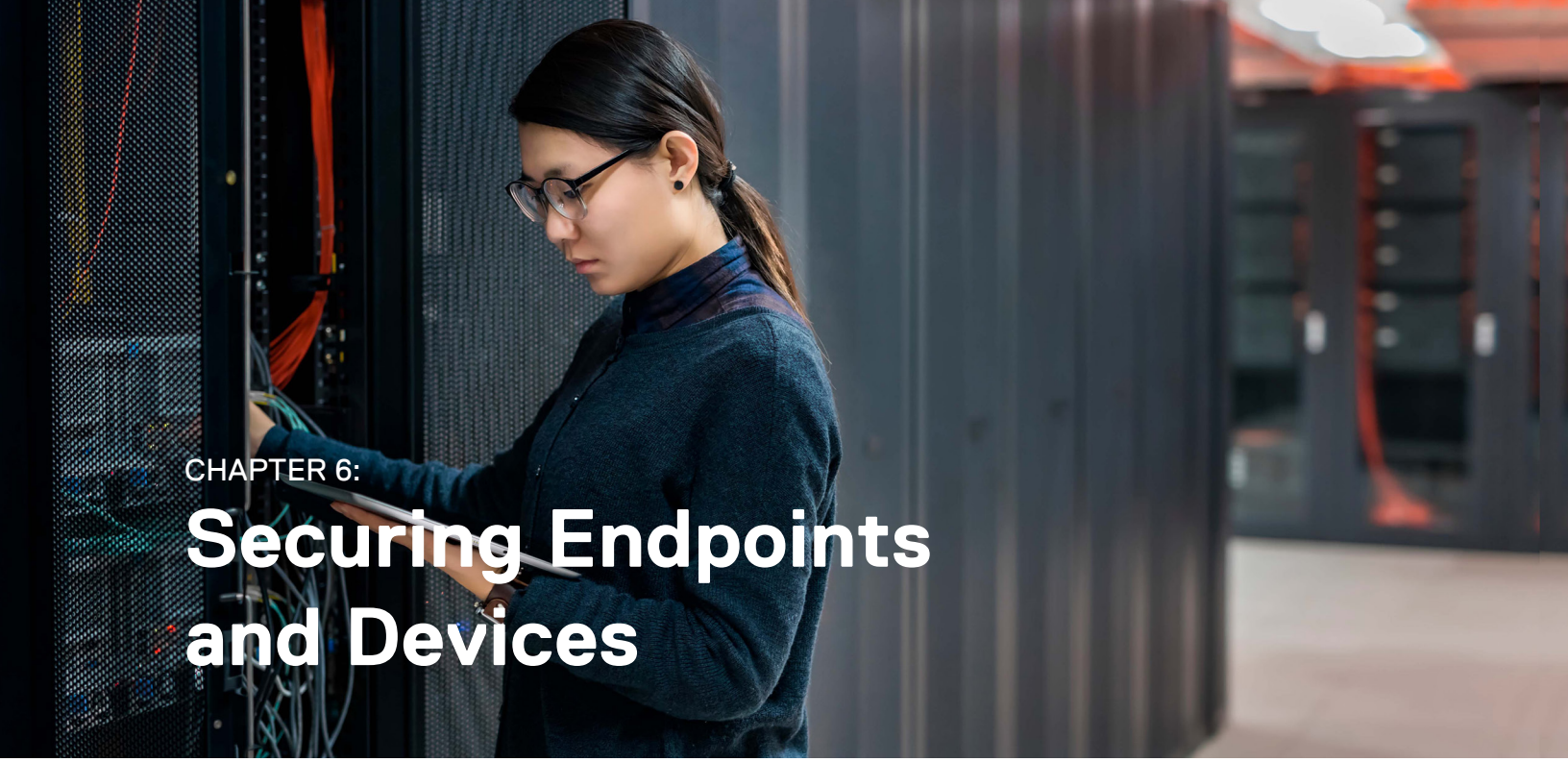
CHAPTER 5:

Keeping an Eye on Connections

Networks are defined by their connections, and are only as secure as those connections themselves. In the realm of trusted connections, security measures can allow IT to implement flexible, automated, policy-driven security policies.

What we see from survey participants is a continued movement away from one-size-fits-all approach towards a more granular, responsive approach to security. Micro-segmentation and transport encryption that ensure data flowing between network nodes are protected in transit are among solutions with the highest growth projected in the next year.





CHAPTER 6:

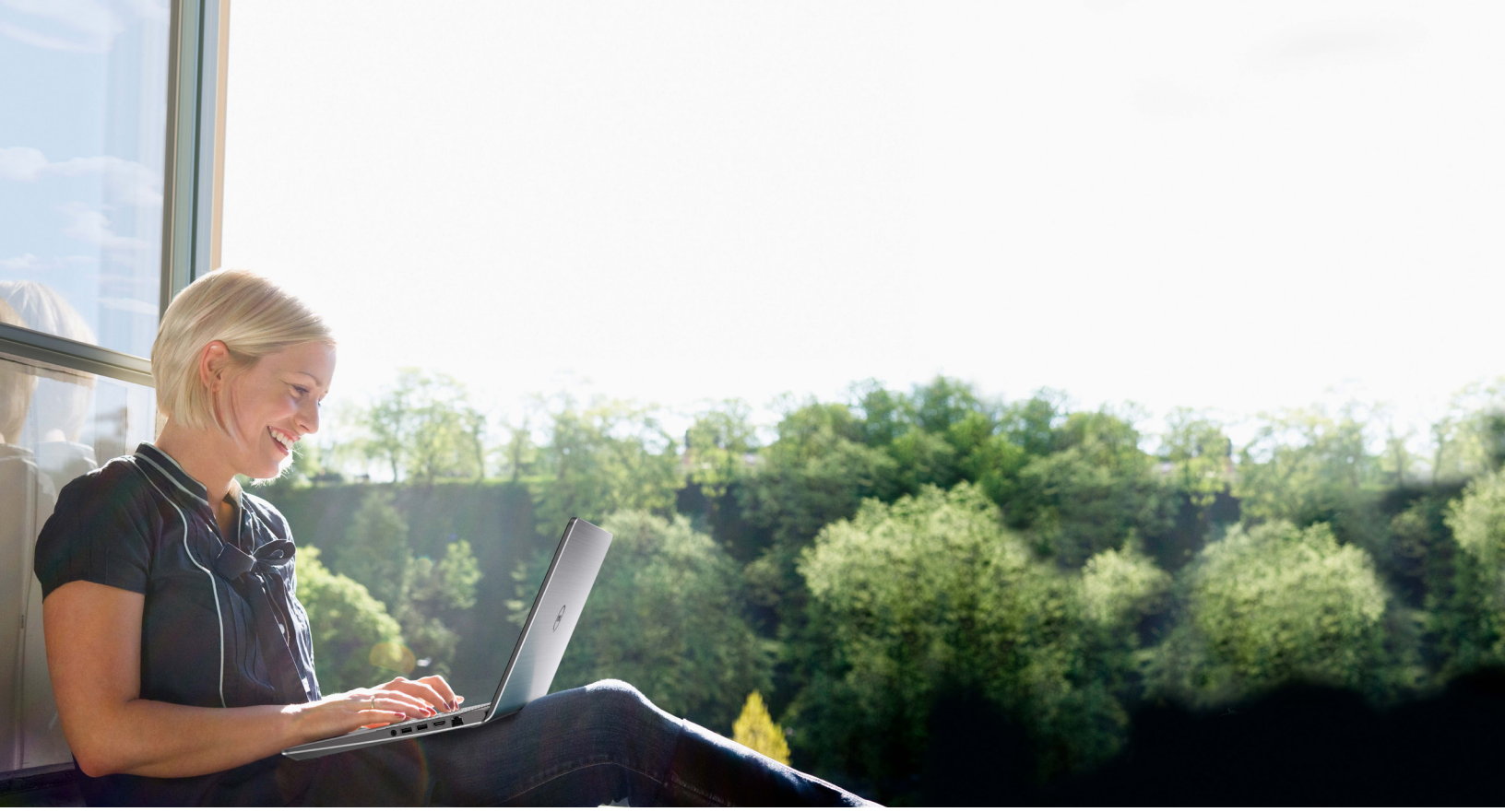
Securing Endpoints and Devices

For typical users of any IT system, endpoints and devices are its most visible, most tangible aspects. That's especially true in the current environment of working from remote locations or hybrid workplace environments. IT and security teams need to know what's going on within their network, and to know about unsafe behaviors, especially when users are no longer protected by a single known firewall and other controls in of a conventional workplace network.

For IT security teams, securing those endpoints should involve not just preemptive, preventative security measures that block known malware or prevent visiting unsafe web sites, but gaining visibility and insight into user behavior. A critical security question for IT staff managing distributed environments is "Do we know what users are doing?"

Our study found that the highest-growth areas anticipated for the next 12 months are in **enabling greater visibility of users and devices**, deploying **Virtual Desktop Infrastructure** (VDI), and **conditional access of devices** (based on both authentication and on each device's security posture).

Cybersecurity professionals will note that many of the concerns vital to securing endpoints and devices in an intentional Zero-Trust environment have long been goals of IT security, including: allowing only authorized access, keeping track of device inventory, and ensuring that devices on the network are well-patched, and compliant with corporate policy. Rather than simply good policy, in the context of Zero Trust these goals all become factors in determining the extent of trust in end-nodes on the network.



ZERO TRUST AT THE PERIPHERY

	Currently Deployed	Plan to deploy < 12 months	Plan to deploy > 12 months
Virtual Desktop Infrastructure (VDI)	48%	29%	14%
User behavior monitoring	44%	33%	14%
Endpoint security (e.g. Anti-Virus, Endpoint Detection and Response)	69%	20%	9%
Device protection (e.g. hardware-based security)	62%	24%	10%
Device authentication	56%	30%	10%
Device compliance (e.g. signature updates, patch levels, corporate policy compliance)	56%	30%	10%
Device inventory (e.g. visible, not visible to technical staff)	56%	27%	11%

CHAPTER 7:

Locking Down Applications and Workloads

Over the next 12 months, the most growth anticipated by the professionals we surveyed is in the areas of application isolation (encompassing virtualization, containers, and container orchestration) and standards-based single sign-on.

Unsurprisingly, these are both central to an ongoing movement towards improving the portability, scalability, speed of deployment, and security of application workloads in general.

Single-sign on is one result of an increasing focus on improving the user experience. Having to repeatedly log in across systems can not only be frustrating to users, but can also lead to unsafe security behaviors, such as writing down passwords for easy access – and possibly opening up a security hole as a result.

Both isolation techniques and consolidated login systems make apps more portable and more scalable for IT teams, and as applications change in scope or hosting environment, the convenience of a consistent user interface for authentication makes them faster to deploy, and more secure.

With an increasing number of apps living on the cloud or with local-application functionality being replaced by services, Web application firewalls are also notably rising in deployment, along with Cloud Access Security Brokers to regulate access to cloud services. Together, these approaches to security emphasize the increasing role of decentralization, and how important it is to go beyond traditional preventative, per-device security measures.

ISOLATION AND INTEGRATION WITH ZERO TRUST

	Currently Deployed	Plan to deploy < 12 months	Plan to deploy > 12 months
Web application firewalls	60%	22%	10%
Application integration (e.g., APIs)	54%	24%	12%
Application isolation / container orchestration (e.g., Kubernetes)	40%	30%	15%
Application isolation-containers (e.g. Docker)	39%	34%	15%
Application isolation – virtualization	46%	30%	14%
Cloud access security broker (CASB)	50%	27%	12%
Single sign-on (e.g. SAML, OAuth, OIDC, FIDO UAF)	44%	33%	12%

CHAPTER 8:

Applying Real-World Solutions

Implementing a Zero Trust architecture can be daunting. Not only does Zero Trust mean reconsidering nearly every part of your security infrastructure, it means choosing a starting point that makes the most business sense for your organization, and actually beginning a transformation that may take years to complete. Every organization presents a unique case, with its own risk tolerance, operational requirements, regulatory environment, userbase, data storage needs, and growth potential.

The good news is that each of the software solutions and behavioral shifts that together make a Zero Trust architecture possible also offer concrete advantages of their own. Deploying a cloud access security broker or implementing an app-based or token-based multi-factor authentication system can deliver greater ease of use and greater security, even if you don’t yet have the time, budget or expertise to comprehensively adopt Zero Trust.

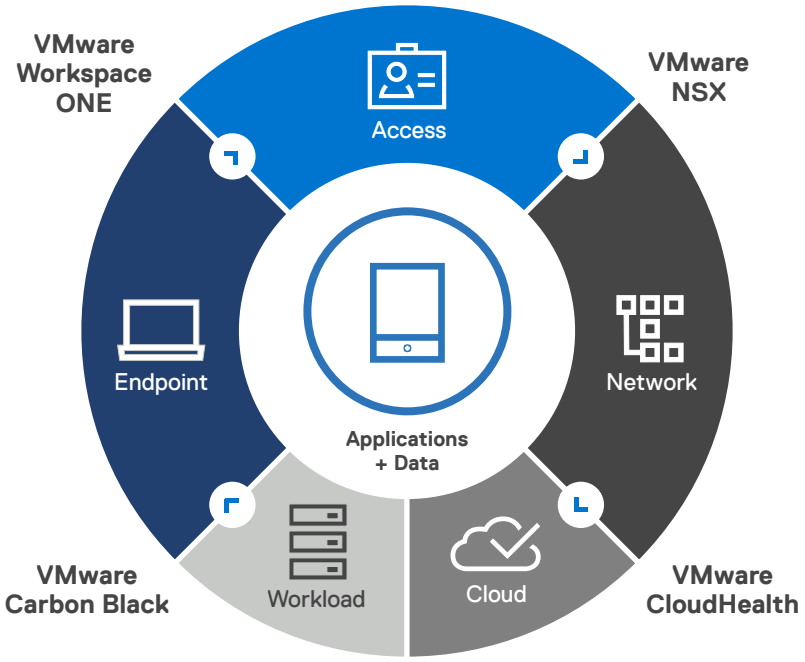
ZERO-TRUST SOLUTIONS FROM THE DELL AND VMWARE SECURITY PORTFOLIOS

Security Concern	Available Solution(s)
Data Safety	Dell SafeData VMware Workspace ONE UEM (Unified Endpoint Management) VMware Horizon 7 VMware NSX-T Data Center
User Security	VMware WorkspaceONE Access VMware WorkspaceONE Intelligence VMware WorkspaceONE Intelligent Hub VMware Horizon 7
Operations	VMware Carbon Black Cloud
Connection Security	VMware Horizon 7 NSX-T
Endpoint and Device Security	VMWare Carbon Black SecureWorks Taegis VMware Workspace ONE UEM
Applications and Workloads	VMware Horizon 7 VMware Workspace ONE UEM VMware Workspace ONE Access

Conclusion

The advantages of continuous authentication and security posture evaluation inherent to Zero Trust extend to every user, and every aspect of your data environment, from improved user experience to enhanced data security, user logon to workload orchestration.

With more than 20 years of experience providing secure virtual environments and IT systems, security has always been a top priority for VMware and Dell. Together, they offer a portfolio of products that work to protect users, data, and workloads, while helping companies avoid the high costs – both financial and reputational – that come with breaches of security.



Check how your IT security stacks up, and how VMware and Dell security tools can help with a no-cost cyber resiliency assessment.

Evaluate Your Cybersecurity Resiliency

DELL Technologies

About the survey

VMware commissioned Spiceworks Ziff Davis to conduct a survey in October 2021. This survey targeted cybersecurity professionals involved in their organizations' data center purchasing decisions, to understand current perceptions and investment priorities in cybersecurity. Survey results includes responses from 452 individuals from a broad range of company sizes, across industries including IT services, software creation, manufacturing, health care, and more.

vmware