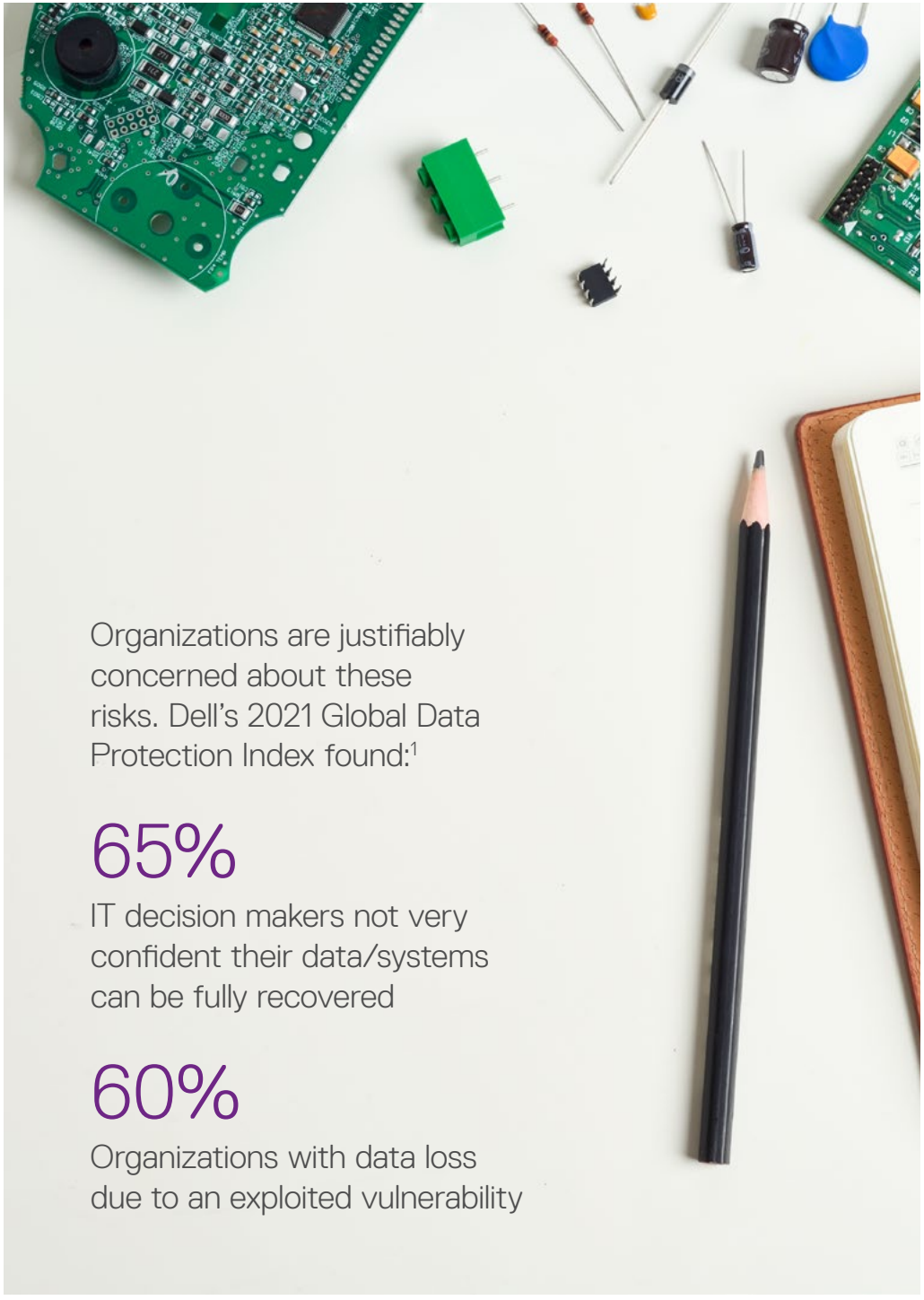

DELL Technologies
Fortify your enterprise with modern security
Protect your enterprise with a holistic strategy.



Organizations are justifiably concerned about these risks. Dell's 2021 Global Data Protection Index found:[1]

65%

IT decision makers not very confident their data/systems can be fully recovered

60%

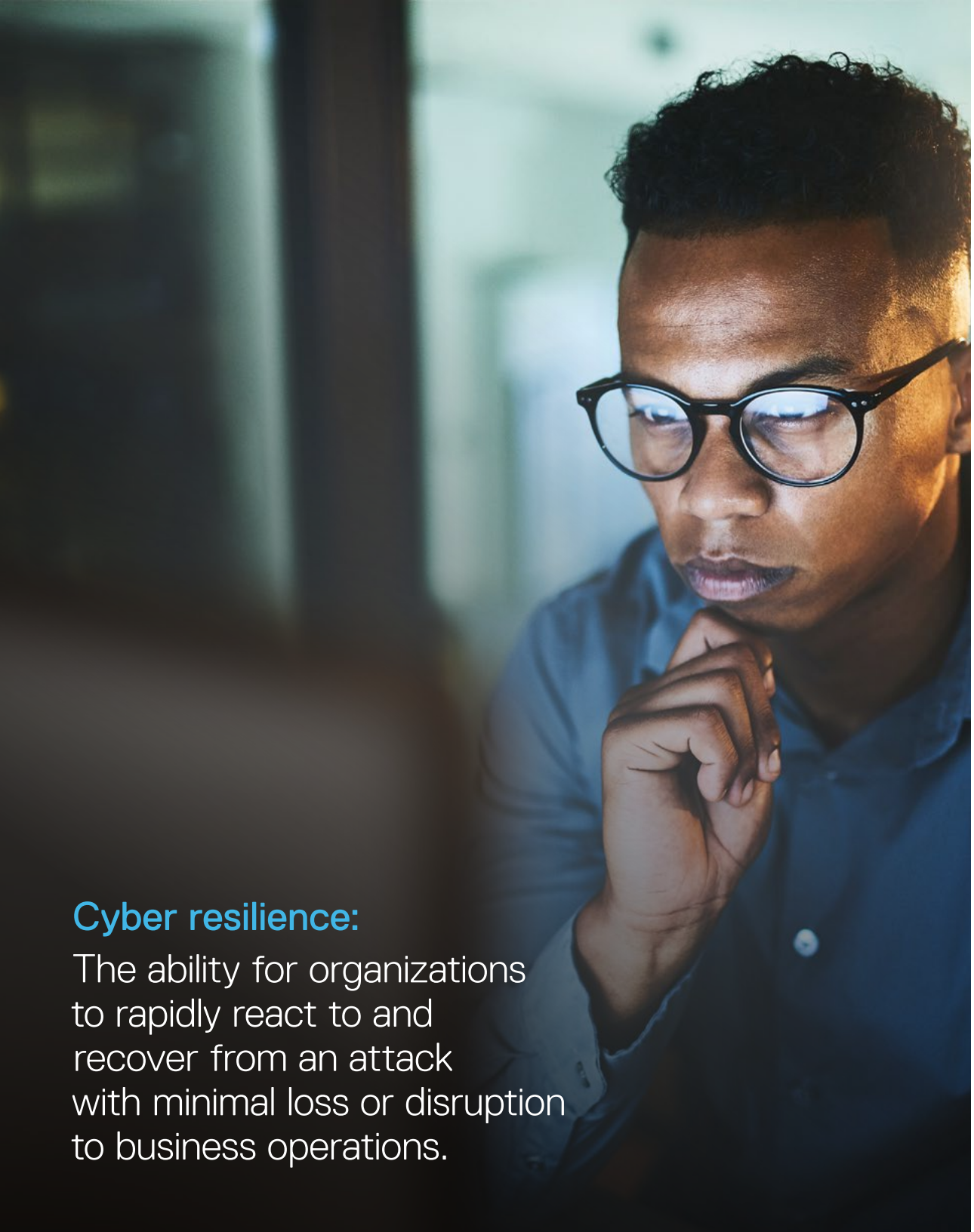
Organizations with data loss due to an exploited vulnerability

Rapid digital innovation introduces new security challenges.

Digital transformation is dramatically changing the way organizations work. While the shift began before the pandemic, the transition to remote work, multi-cloud environments, harnessing data at the edge and IT as a service has accelerated the process.

This rapid transformation presents a golden opportunity for organizations that harness the power of data, but **it also creates abundant security challenges**. Expanding perimeters are distributed, virtual, in multiple clouds and moving massive amounts of data. Inadequate security **creates new attack surfaces and vulnerabilities.** The sheer amount of data alone presents a growing challenge: **Organizations are now managing 10x the data they were just five years ago**, almost 15 petabytes on average now.[1]

Meeting these challenges means securing data, applications and devices. That, in turn, calls for a mature approach that leverages innovative technologies for scale and intelligence, aligns around the business rather than the threats, is proactive in recovery planning and defends the organization as a whole, rather than in pieces and parts.



Cyber resilience:

The ability for organizations to rapidly react to and recover from an attack with minimal loss or disruption to business operations.

Fortify with modern security: Dell's holistic approach.

While threat detection and prevention remain the first line of defense, Dell believes today's security challenges require going beyond the outdated notion that every potential threat can be stopped. As the number of high-profile cybersecurity breaches grows weekly (if not daily), organizations must now plan for WHEN rather than IF attacks will occur. This mindset shift can increase cyber resiliency.

Dell is ideally positioned as a trusted partner to help organizations design, build and manage their security transformation with:

- Advanced capabilities that intelligently scale
- A holistic presence throughout your IT infrastructure
- Technology expertise gained from decades as a leading global technology provider

Dell's holistic security approach can help your organization move toward a zero-trust architecture and effectively address today's most pressing threats.

The three pillars of Dell's modern security approach

To address the current and emerging threat landscape, Dell creates a powerful security foundation with these three pillars:

1. Protect data and systems

Modernize the organization's security approach utilizing a cohesive suite of advanced tools complemented by intrinsic features in hardware and processes from a provider with a holistic presence across the entire IT ecosystem. This requires carefully choosing security partners—virtually no one goes at this alone.

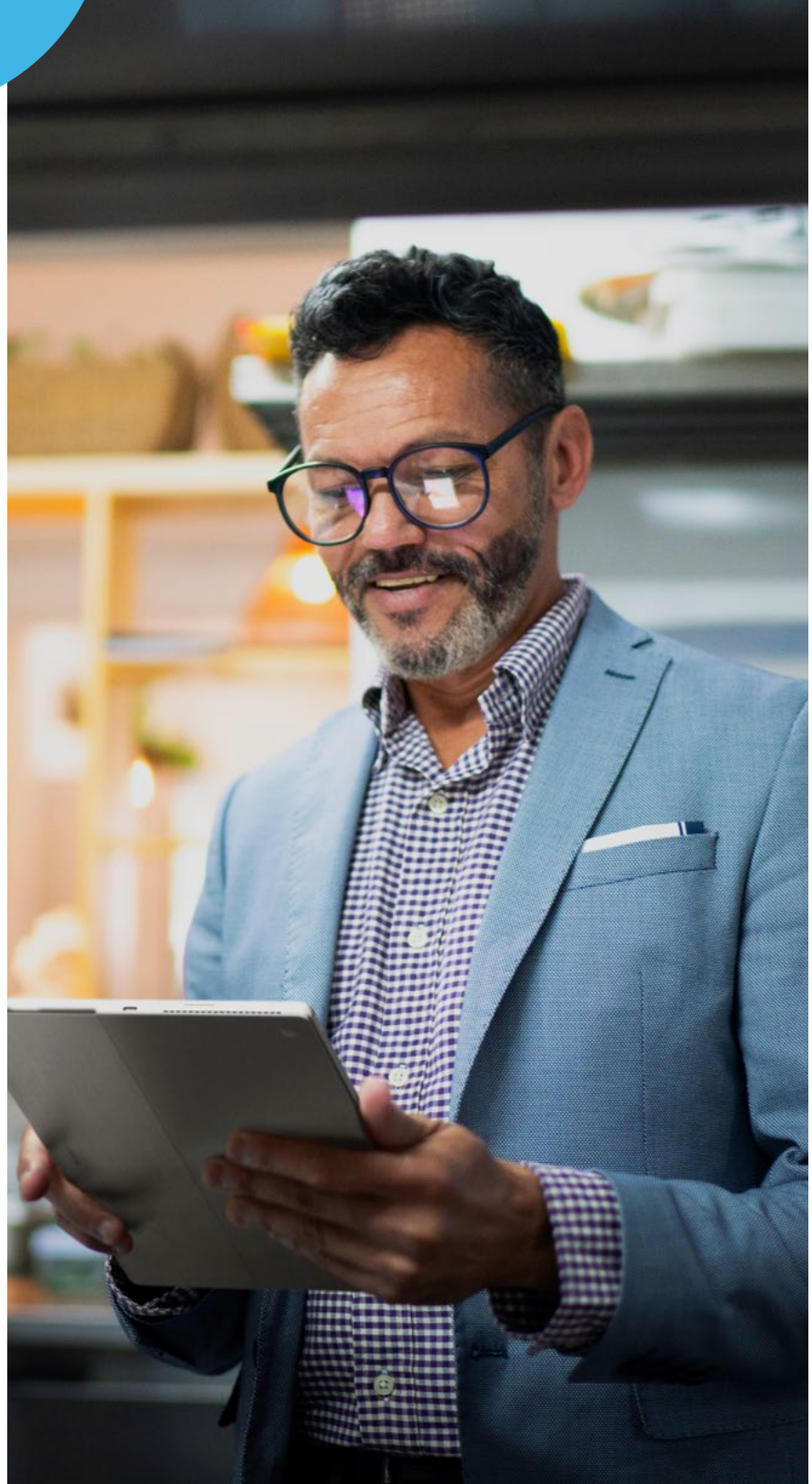
2. Enhance cyber resiliency

Organizations must understand their current level of resiliency for defending their data and preparing for business continuity and availability in the face of attacks.

3. Overcome security complexity

Simplify and automate security operations to enable scale, provide insights and extend resources through service partnerships.

Another important emerging doctrine in the cybersecurity arena is zero trust, which means that users and devices, even when already *within* an ecosystem, should not be trusted by default. Instead, all users and devices require continual and redundant verification. Zero-trust architectures also rely on strong data encryption and keeping systems isolated as needed to contain threats.



Know where your cybersecurity stands.

Know where it needs to get.

Your organization depends on always-accessible, always-safe data—from application servers to multi-cloud to your virtual desktop infrastructure (VDI). With confidence in the security of every element in your technology infrastructure, your organization can minimize costly downtime and stay focused on innovation and growth.

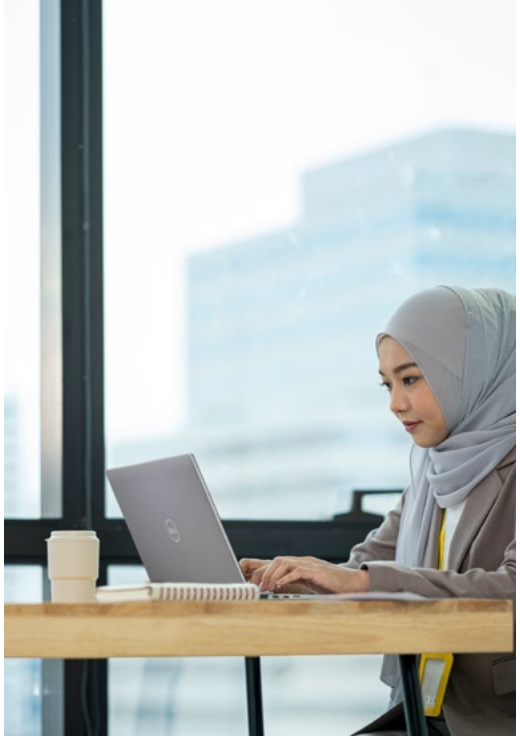
Use these checklists to assess the current state of your cybersecurity readiness. When you know your organization's strengths and vulnerabilities, you know the best next steps for comprehensive data security across your full IT ecosystem.

Protect data and systems checklist

Enhance cyber resiliency checklist

Overcome security complexity checklist

Modern Cyber Security for Enhanced IT Resiliency



Pillar one: Protect critical data and systems.

Fortifying your organization with modern security requires rethinking how you protect data and systems. Dell delivers significant incremental value with intrinsic security features and a holistic presence across the ecosystem.

Intrinsic security

Dell starts with devices and processes designed for security as a baseline. If **intrinsic security features** already exist in the hardware, the firmware and the security control points, the architectural foundation is ahead of the game. Intrinsic security also automates foundational security elements, reducing or even eliminating the need for human involvement and intervention.

Dell delivers incremental value with **intrinsic security** features built into its platforms and internal processes. As a global leader in IT technology for decades, Dell has had many years to drive intelligent innovation for security deep into our product designs and processes. Our customers utilize our hardened devices and processes for an intrinsic advantage.

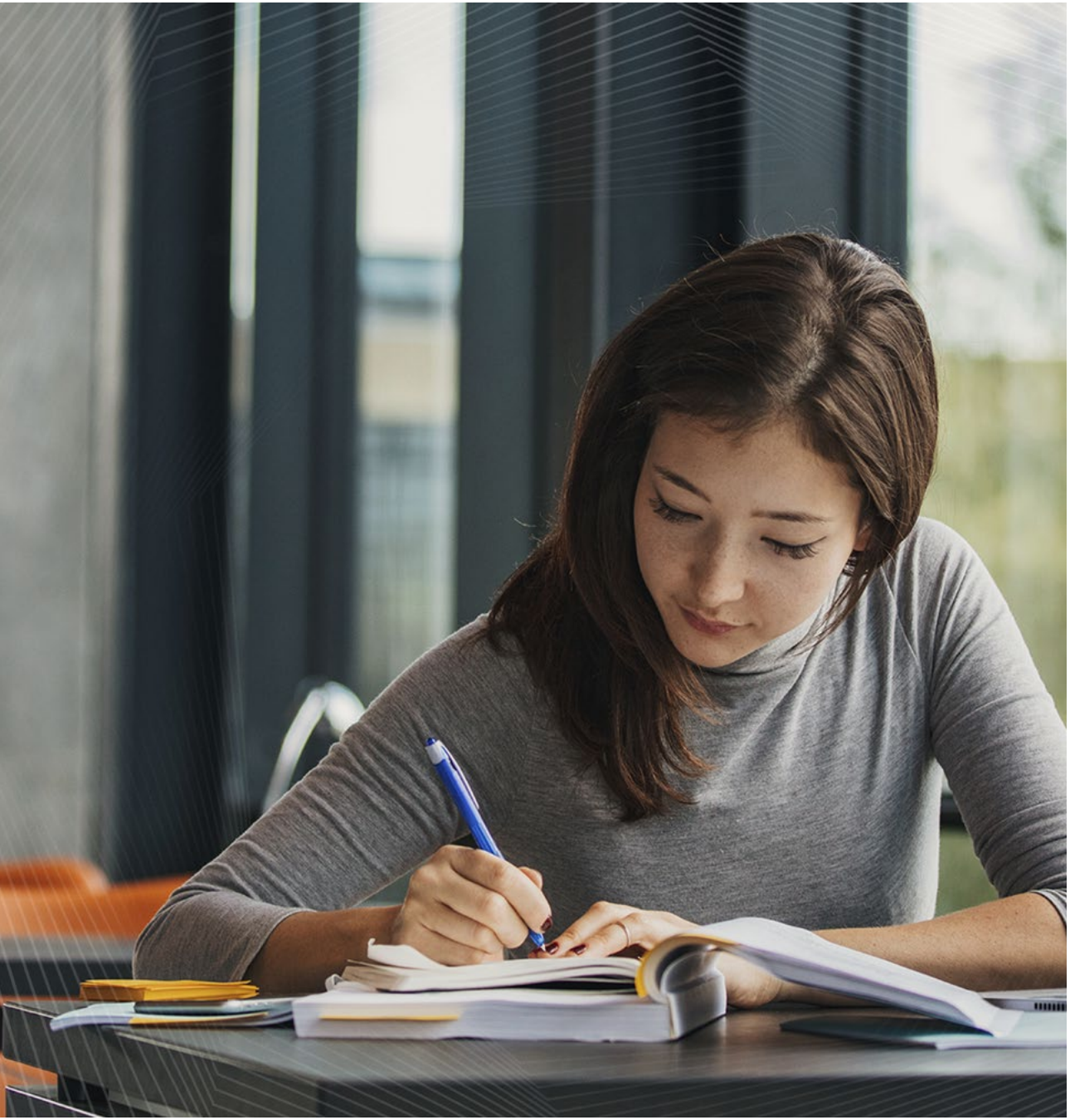
Endpoint data protection – Dell Trusted Devices

Dell Trusted Devices is a collection of features and offerings that help make Dell the industry's most secure commercial personal computers.[2] Dell Trusted Devices feature embedded technology that protects the device at the BIOS level. Only Dell maintains a protected firmware image and user access credentials off host on a dedicated security chip, hidden from malware that may steal access credentials or hijack the firmware.

Dell SafeData, part of the Dell Trusted Devices feature stack, helps protect data with:

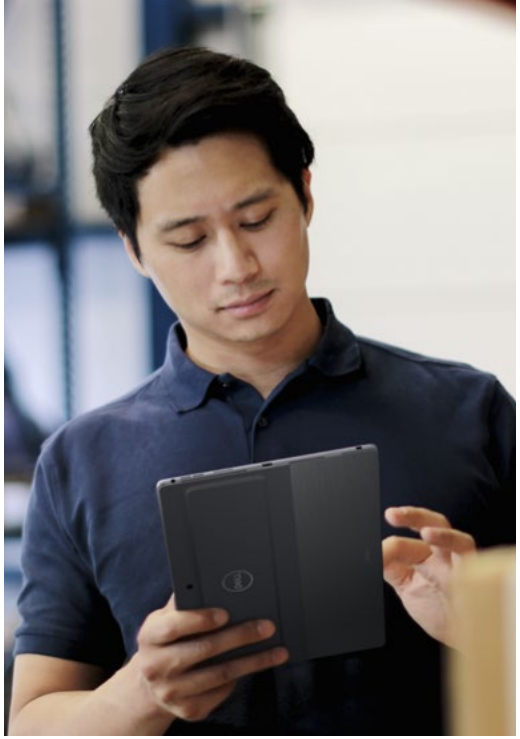
Netskope is a cloud-delivered security platform aligned with Gartner's secure access service edge (SASE) framework that includes network and data security controls for the modern enterprise. Includes zero-trust network access (ZTNA).

Absolute Persistence® technology is embedded in the firmware of Dell laptops and desktops. This technology provides a continuous, tamper-proof connection between devices and data on or off network and self-healing applications (such as VMware Carbon Black and Netskope). The connection is managed via the cloud-based Absolute console.



Dell Managed Detection and Response: The endpoint security portfolio, Dell Technologies Managed Detection and Response, powered by Secureworks® Taegis™ XDR, is a fully managed, end-to-end, *24/7 service that monitors, detects, investigates and responds to threats across the entire IT environment.*

Finally, **APEX Backup Services** is a software-as-a-service (SaaS)-based data protection platform that offers secure, scalable and cost-effective backup, retention, compliance and recovery for SaaS apps, endpoint devices and workloads running in the cloud on-premises.



Dell's secure supply chain program aligns to and, in places, exceeds US government-promoted best practices and standards, and we're constantly improving.

Extending security across your full IT infrastructure

Servers

Our Dell PowerEdge servers are designed and built with a cyber-resilient architecture that aims to have security built in at every phase of the server lifecycle. Key components include:

Hardware root of trust. A cryptographic key that Dell embeds into product silicon during hardware production to ensure that the BIOS cannot be tampered with.

Signed firmware, drift detection and BIOS recovery. Built-in data and system protection, reliable detection and monitoring and solutions for rapid recovery should an issue ever arise. A PowerEdge purchaser is not just buying a server, they're also getting a comprehensive, security-oriented feature set that is intrinsic to the product itself.

Storage

The operating system code in Dell's storage appliances has been hardened to help ensure that all sensitive data remains secure.

These platforms include features such as *multi-factor authentication, role-based access controls and data at rest or in-flight encryption, among others.*

For **key management,** we offer in-house solutions like CloudLink, options to integrate with a customer's existing key management and the flexibility to use a local key management store.

Secure Development Lifecycle and Supply Chain Security

Intrinsic security goes beyond technological features built into our products. Dell also manages internal processes designed to ensure the highest level of security for the products that reach our customers.

Dell Secure Development Lifecycle defines security controls for hardware and software development and is governed by an internal team. This team collaborates through several industry standard bodies to ensure best practices. Dell's suppliers also agree to a set of requirements with Dell to help ensure security throughout the sourcing cycle.

Dell Supply Chain Security ensures that the security, integrity, quality and resilience of our products remains intact. Dell has implemented cutting-edge programs across the full spectrum of supply chain risk—from our threat-informed product designs, to training our tens of thousands of developers on secure development practices, to securing our factories, to logistics security programs, all the way through to post-delivery support and services.

Holistic security capabilities

As a core-to-edge-to-cloud IT provider, Dell has a holistic vantage point for security and can offer solutions across the IT spectrum—**an integrated approach not many providers can claim.**

Dell's vision for security is that it should be holistic, intelligent and scalable, spanning the entire enterprise with consistent objectives and policy applications. Our security solutions cover infrastructure, the cloud (public, private and multi-cloud), applications (including mission-critical legacy) and new cloud-native apps and devices.

The power of Dell's intrinsic security solutions can be summarized this way: *With these features built in, there's less need to bolt on third-party security products that come with differing protocols and consoles, each requiring people to learn and to manage those systems.*

Protect data and systems checklist

From remote laptops and desktops to cloud and on-premises servers and storage, your organization depends on every IT infrastructure element to stay productive and innovate. But each device, network endpoint and system can introduce opportunities for intended or unintended systems breaches that leave your data vulnerable. Answer these questions to determine if your data is secure across your full IT ecosystem:

YES	NO	
☐	☐	**Is your overall security posture based on a zero-trust architecture?**
☐	☐	Does your organization's security capability cover the end-to-end IT ecosystem, including devices, applications and systems?
☐	☐	Does your organization manage one security policy that applies to both internal and external providers?
☐	☐	Has your organization assessed and addressed risks in its IT supply chain, accounting for security, integrity, quality and resilience?
☐	☐	Can your organization track devices/endpoints and lock or wipe them in the case of theft or unauthorized use?
☐	☐	Do your vendors (or internal DevOps) have appropriate measures in place to protect the process by which new products, features and services are developed (secure development lifecycle)?
☐	☐	Has your organization assessed the new and potentially greater risks posed by increased remote work?
☐	☐	Are endpoint security measures in place both above and below the OS?
☐	☐	Thinking holistically, is your current security capability bolted on or built in? Siloed or unified? Threat centric or context centric?
☐	☐	Are personnel and physical security technologies and processes in place? Are they routinely reviewed and updated?

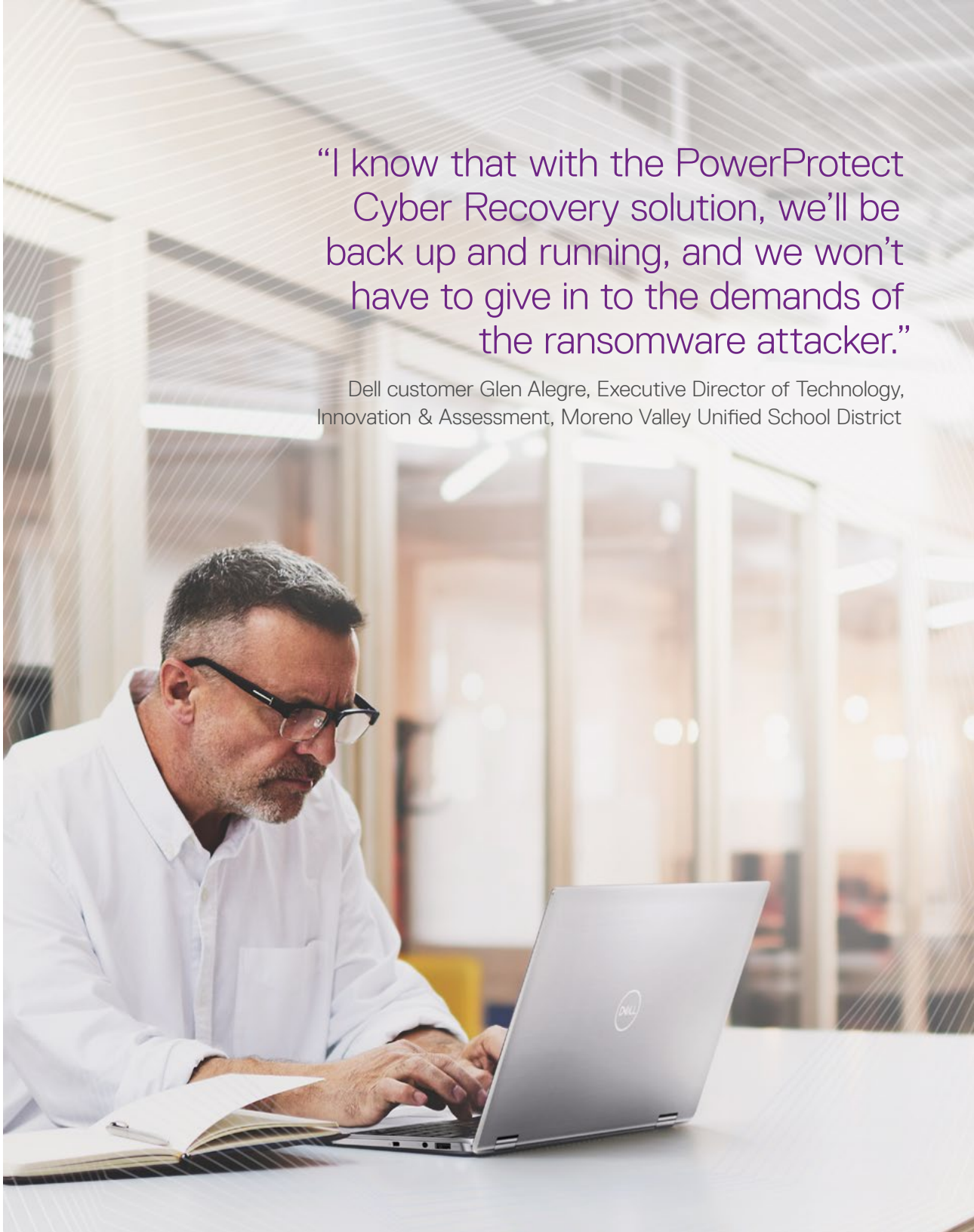
Pillar two: Enhance cyber resiliency.

Another key element in fortifying with modern security is enhanced cyber resiliency. No matter how good your cybersecurity protection may be, it is unlikely to prevent every potential threat. Organizations must assume that they will be the victim of a successful cyber attack at some point.

They shouldn't, however, accept catastrophic loss as a result. The key is to be **prepared** to recover as quickly as possible and minimize the impact to business operations. Attack preparation means less financial impact, reduced disruption to customers and, *most importantly, the peace of mind that comes from knowing your organization can recover quickly.*

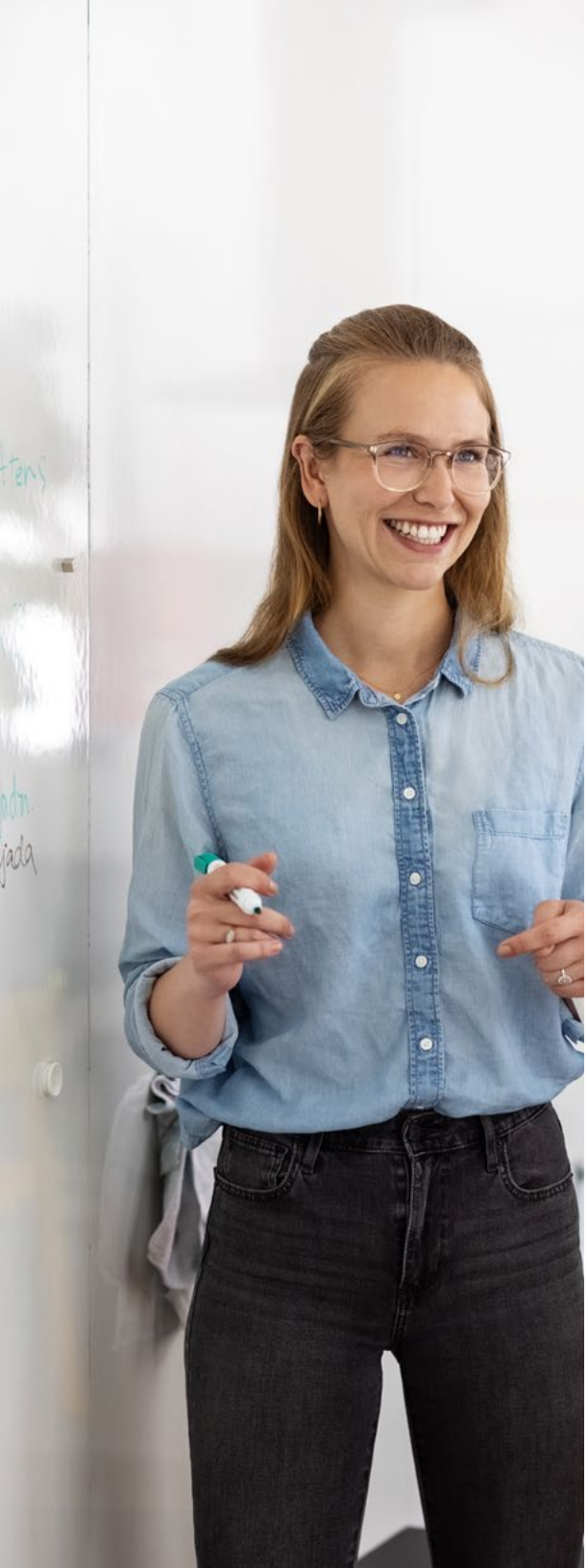
Resiliency is not a single technology, but an outcome, and it is achieved through the combination of planning, discipline and integrated technologies that manage detection, protection, response and recovery across an ecosystem.

Dell offers holistic technology solutions and services designed to help any organization achieve greater cyber resiliency and to help customers define strategies to get back up and running *before* an attack disrupts their operations.



"I know that with the PowerProtect Cyber Recovery solution, we'll be back up and running, and we won't have to give in to the demands of the ransomware attacker."

Dell customer Glen Alegre, Executive Director of Technology, Innovation & Assessment, Moreno Valley Unified School District



Dell's holistic portfolio of cyber protection solutions

Cyber recovery and resiliency solutions

APEX Cyber Recovery Services
A fully managed solution that isolates critical data to defend against cyberattacks and ransomware. This solution simplifies recovery operations and speeds recovery after a cyber attack by having Dell manage day-to-day cyber recovery vault operations and assist with recovery activities.

PowerProtect Cyber Recovery
A cyber-resiliency solution endorsed by Sheltered Harbor that isolates data immutably in an air-gapped secure data vault, enabling recovery of known-good data to help restore normal operations after a ransomware or cyber attack.

CyberSense
An incremental analytics tool that works with PowerProtect Cyber Recovery by scanning backup images in the secure vault for indications of a ransomware attack and generating an alert if suspicious activity is found.

PowerScale Cyber Protection powered by Superna
Enables real-time auditing, proactive detection and automated data recovery from ransomware attacks on unstructured file data residing on PowerScale and Isilon platforms.

Cyber recovery consulting and managed business resiliency services

Business impact analysis
Assess and validate business resiliency program maturity and the impact of downtime through our unique methodology.

Cyber recovery solution and services
Enable recovery with a strategy that ties together people, process and industry-leading technology to enable recovery of business processes after a cyber attack.

Incident response and recovery
A team of cyber recovery specialists offer a custom solution if an organization experiences a breach.

Enhance cyber resiliency checklist

Blocking cyber threats is an essential component of any data security plan, but if you stop at prevention—your data **is not** fully secure. You must also include cyber-resilience solutions and strategies to recover and protect data, and minimize data loss and costly downtime, should a breach ever occur. Answers these questions to determine the cyber resilience of your organization:

YES	NO	
☐	☐	**Is your overall security posture based on a zero-trust architecture?**
☐	☐	Are your existing data protection methods sufficient to cope with today's malware and ransomware threats? (Dell Technologies internal studies suggest that over 60% of organizations are concerned about this risk.*)
☐	☐	Does your organization practice the 3-2-1 backup methodology?
☐	☐	Are recovery plans routinely tested?
☐	☐	Has your organization ascertained the amount of time its operations would be disrupted in the event of a cyber attack? Is it weeks, days or minutes?
☐	☐	Does your organization base its security model on the notion of continually blocking/preventing as many threats as possible, or that an attack is ultimately inevitable?
☐	☐	Has your organization implemented systems and processes that focus on minimizing the operational disruption and/or financial impact that an attack may cause?
☐	☐	Has your organization implemented an air-gapped data vault where "known-good" data is stored?
☐	☐	What type of threat detection capabilities do you have in place? Are they managed internally or by a third party?
☐	☐	Does your organization utilize AI-based pattern anomaly detection?
☐	☐	Is end-to-end data encryption in place?
☐	☐	What is the organization's backup and system snapshot process?

Pillar three: Overcome cybersecurity complexity.

Organizations that use multiple data protection vendors experience a 4X greater estimated annual cost of data loss compared with those using a single vendor.[3] Complexity is the enemy of security, and so the final step in fortifying with modern security is to overcome security complexity.

Security operations teams are managing security solutions for endpoints, servers, networks, storage and cloud. As such, inefficiencies that contribute to risk and costs can mount quickly, resulting in the level of protection—or the productivity of technology—being compromised. Usually both.

Yes, we still depend on advanced tools to defend ourselves, but there is also an increasing recognition that **we simply add layer upon layer of security tools** as we adopt new technologies. The maintenance complexity quickly becomes unmanageable and adds risk.

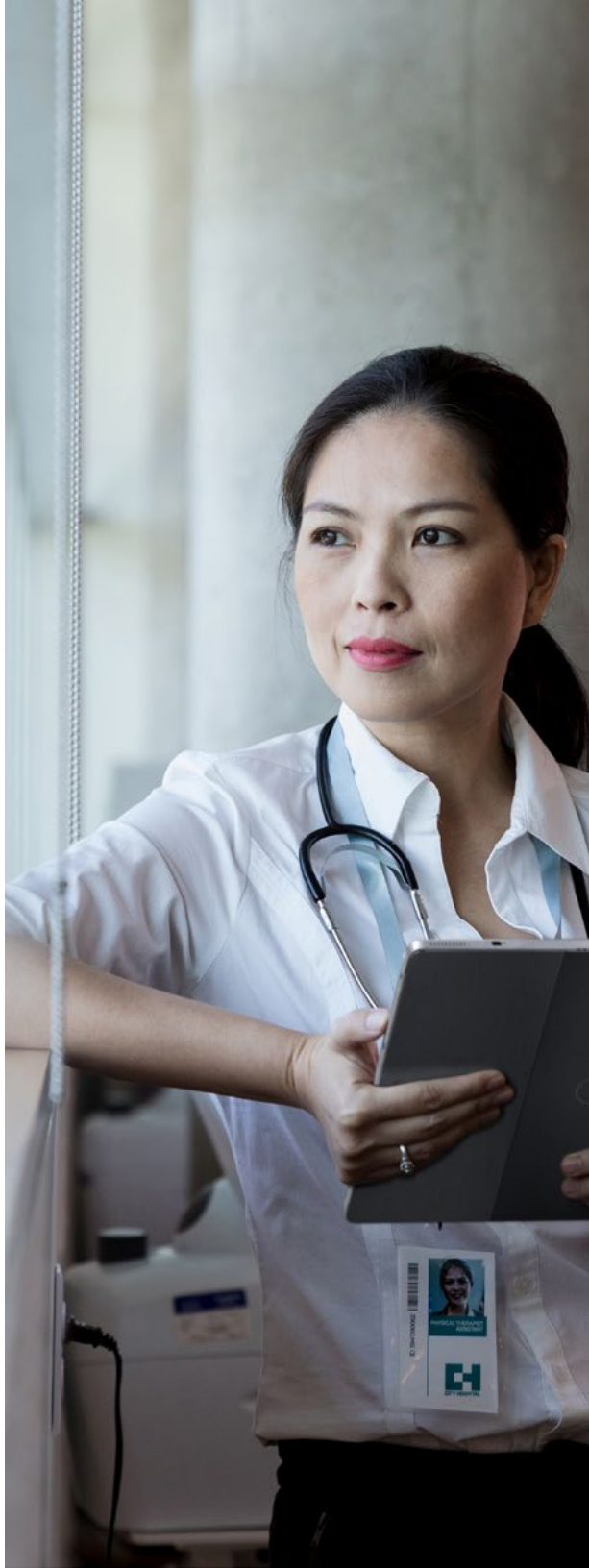
Organizations need better ways to scale. Dell's approach provides:

Intrinsically secure products
These help offload some of the basic security demands from humans to the devices, providing a foundational advantage.

Automation, intelligence and consolidation
Dell offers the unique advantage of consolidated tools and vendors, especially given the power of our partnership with VMware and more.

Intelligent innovation
Dell infuses artificial intelligence (AI) and machine learning (ML) into our security tools. For example, Cloud IQ is AIOps for intelligent infrastructure. CloudIQ combines proactive monitoring, automated notifications and recommendations, ML and predictive analytics to help reduce risk for Dell infrastructure systems.

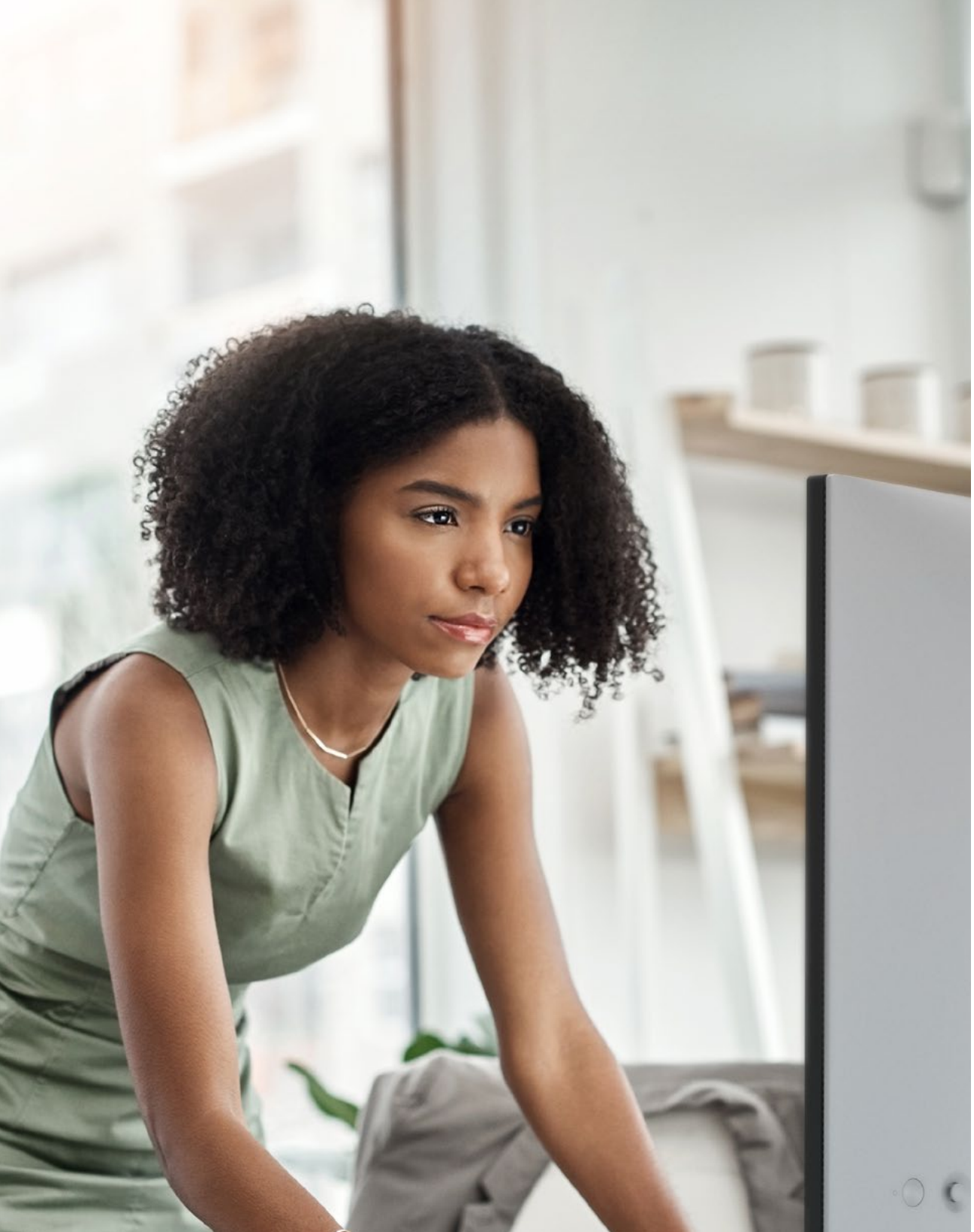
Partnering as a trusted advisor
Turning to Dell's professional security services is a proven way to extend constrained resources and reduce complexity. You also gain access to Dell's team of certified security experts, who use the latest AI-based capabilities to strengthen your security posture and address the most pressing threats with confidence.



Overcome security complexity checklist

Complexity is the enemy of security. When your Security Operations Team is managing security solutions for endpoints, servers, networks, storage, and cloud, the risks, costs, and inefficiencies can mount quickly. You can't afford to simply add layer upon layer of security tools or the maintenance that comes with them. Answer these questions to determine if security complexity is making your data and systems vulnerable:

YES	NO	
☐	☐	**Is your overall security posture based on a zero-trust architecture?**
☐	☐	What is your current security spend, both on internal and external (third-party) capabilities?
☐	☐	Does your organization routinely analyze its internal and third-party security providers to ensure effectiveness and value?
☐	☐	Has your organization ensured the appropriate level of redundancy in its security capability? Have extraneous or low-value elements been eliminated?
☐	☐	Has your organization taken advantage of potential synergies by rationalizing the number of security vendors?
☐	☐	Have you hired an outside expert to assess your overall security posture and propose enhancements?
☐	☐	If your organization is using multiple data protection vendors, have you determined the potential higher cost of data loss versus that of a single vendor? (Dell studies indicate that the cost can be as much as four times as high in a multi-vendor scenario.)
☐	☐	Does your organization utilize any automation or orchestration tools to help with either detection and/or recovery?



Strengthen your organization's security posture.

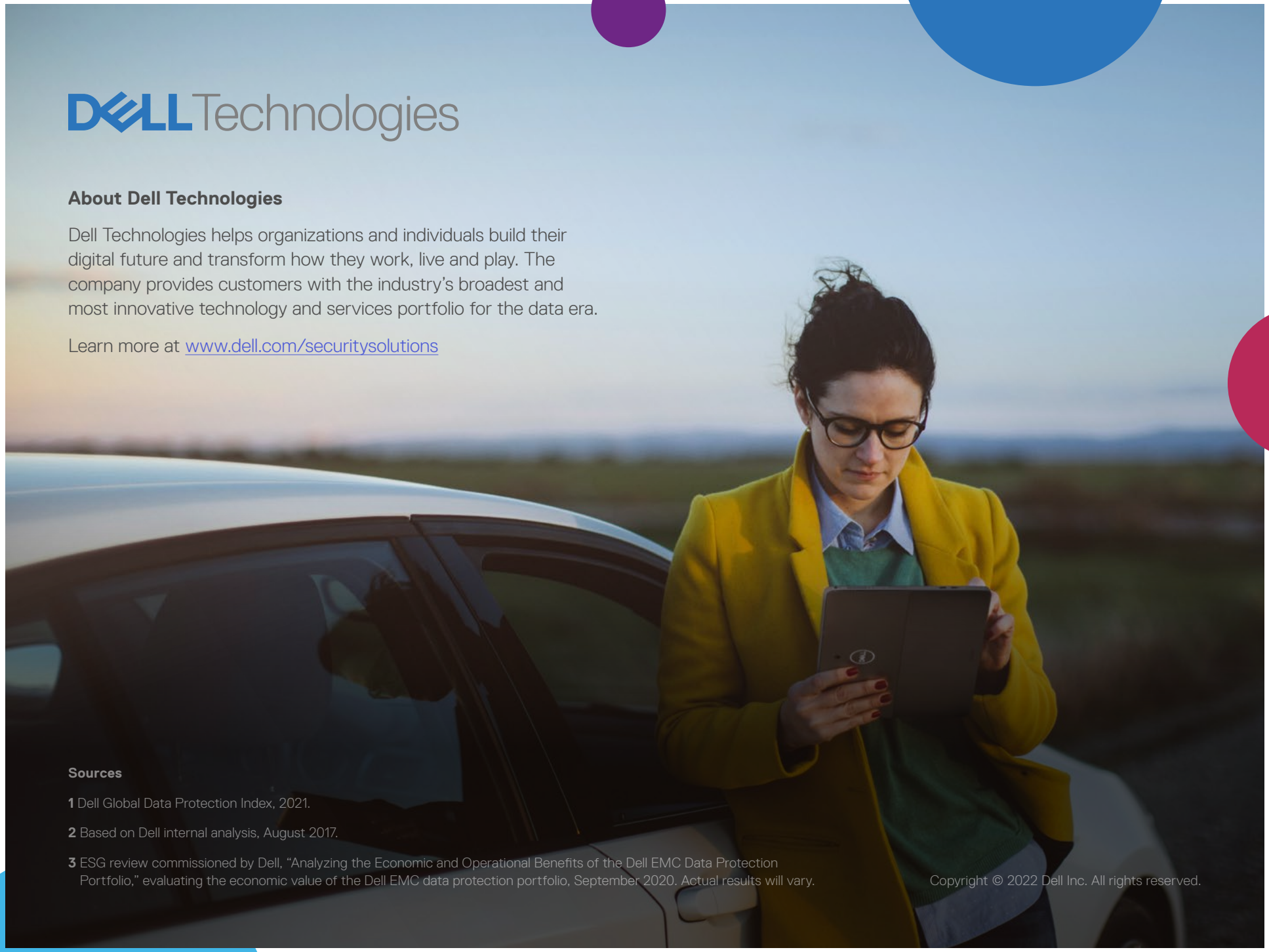
As organizations expand their security capabilities and become more mature and cyber resilient, overcoming complexity is crucial to ongoing success. Dell is a trusted partner in modern security. We deliver the expertise and end-to-end tools to help you achieve these three core outcomes:

Protected data and systems
Select Dell as a trusted security partner with the scale and resources to provide advanced tools and intrinsic capabilities holistically across an organization's IT spectrum.

Enhanced cyber resiliency
Plan, prepare and practice mature resiliency programs to protect critical data and apps and to lessen the impact of cyber attacks.

Reduced security complexity
Utilize automation, consolidate security tools and make use of Dell security experts to intelligently scale.

Dell stops at nothing to help our customers build their breakthrough. Our modern security approach is designed to help ensure that an organization's environment is secure and resilient, so they can focus on their core competency, build their breakthrough and advance human progress.



DELL Technologies

About Dell Technologies

Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

Learn more at www.dell.com/securitysolutions

Sources

1 Dell Global Data Protection Index, 2021.

2 Based on Dell internal analysis, August 2017.

3 ESG review commissioned by Dell, "Analyzing the Economic and Operational Benefits of the Dell EMC Data Protection Portfolio," evaluating the economic value of the Dell EMC data protection portfolio, September 2020. Actual results will vary.