DELL Technologies

Intel
Innovation
Built-in

intel.

Innovation unleashed

Strategies on how to advance cybersecurity and achieve Zero Trust maturity from Dell Technologies and Intel

Table of contents

The world increasingly runs on data — but are your customers confidently innovating with data, or are they held back by the myriad of security risks that modern businesses face? This white paper discusses how you can help customers innovate fearlessly with data, opening up a world of possibilities.

The rising challenge of secure data triangulation

In today's fast-paced economy, continuous innovation enables organizations to respond faster to market disruption, accelerate ideas and successfully navigate operational or macroeconomic challenges. Agile, advanced data analytics helps anchor this innovation by delivering powerful insights that enable your customers to make the right decisions and investments. Data-powered initiatives such as generative artificial intelligence (AI), machine learning (ML) and automation further boost business growth while fueling innovation.

Data triangulation — analyzing multiple, complex datasets from across the business to gain richer understanding and develop additional layers of insights — is an essential part of innovation. Teams ranging from product development, IT and finance to marketing and sales rely on data triangulation to bring together disparate pieces of data, extract business intelligence, generate new insights and make strategic decisions. But organizations must be able to use their data without exposing it to threats and making security cumbersome.

The modern distributed environment makes it increasingly challenging for your customers to break data silos and enable secure access to the data that resides everywhere. Secure data triangulation is one of the common barriers to innovation.

As a Dell Technologies partner, you have access to resources that enable your customers to overcome this hurdle. Dell Technologies brings together the technology, partnerships and end-to-end IT solutions to help you solve customers' complex security problems.

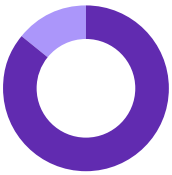
34%

of surveyed business and IT decision-makers believe cyberthreats are a top challenge that stops their organization from innovating with data.[1]

1. Dell Technologies, "The Innovation Index," February 2023, https://www.dell.com/en-us/dt/perspectives/innovation-index.htm.

How partners can help

Organizations view technology as a core enabler of innovation.



86%

are actively pursuing technologies that can help them achieve their innovation goals.[2]

IT leaders face tremendous pressure to modernize their IT infrastructure while supporting daily operations. Many IT teams are struggling to keep up with these requirements and support employees with on-demand data access across an increasingly complex ecosystem.

To innovate without fear or compromise, organizations need a comprehensive, mature cybersecurity strategy that allows them to securely share and triangulate the data that fuels business initiatives reliant on AI and other emerging technologies. Innovators are seeking guidance from experts like you to support them in executing these objectives.

You have a deep knowledge of the IT market, your customers' business and their industry requirements. By combining this expertise with the right tools and solutions, you can show customers how maturing their security approach can facilitate their innovation. Dell Technologies, together with Intel, provides holistic, integrated, intelligent and cyber-resilient IT solutions that power flexible and agile data use, unlock collaboration and support data-fueled initiatives — so your customers can advance their cybersecurity maturity and confidently innovate with cutting-edge technologies and analysis.

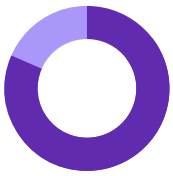
2. Dell Technologies, "The Innovation Index," February 2023, https://www.dell.com/en-us/dt/perspectives/innovation-index.htm.

Driving innovation in a fast-changing world with data-fueled AI

Artificial intelligence has the potential to disrupt every sector as well as contribute as much as $22.1 trillion annually to the global economy.[3]

Machine learning, predictive analytics, intelligent automation and other AI technologies drive innovation in areas such as:

- **Employee productivity:** Automation of routine tasks, along with augmentation of employees' skill sets, can free up employee time so they can focus on more strategic initiatives and have more autonomy to spark new ideas. Their ability to innovate not only drives business forward but also boosts retention. In fact, 78% of business and IT leaders believe that people join their company in part because they believe they'll be empowered to innovate.[4]
- **Customer experience:** More organizations are adopting a customer-centric mindset to keep up with their customers' dynamic needs. Nearly half of surveyed organizations say their main goal of investing in enterprise technology is to amplify customer centricity.[5] Businesses can deliver better and more personalized, real-time customer experiences with ML and other AI technologies.
- **Business strategy:** Advanced data analytics is becoming a core part of the business. Predictive analytic models, for instance, deliver critical insights into potential future trends, enabling organizations to make more effective decisions, accelerate digital initiatives and improve business strategy.



81%

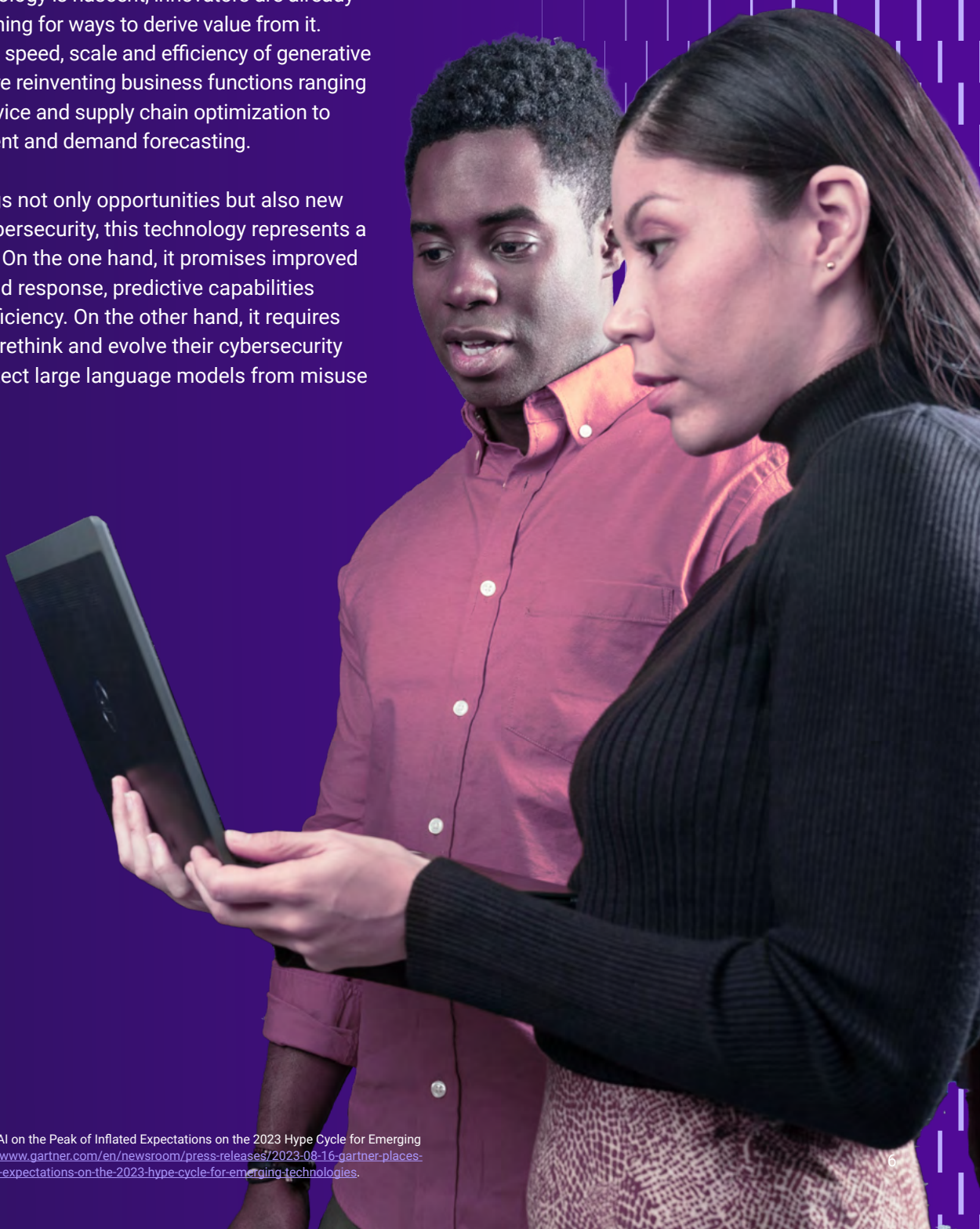
of IT decision-makers agree that emerging technologies such as AI and the edge pose a risk to data protection.[6]

3. McKinsey, "The economic potential of generative AI," June 2023, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier.
4. Dell Technologies, "The Innovation Index," February 2023, https://www.dell.com/en-us/dt/perspectives/innovation-index.htm.
5. KPMG, "Digital to the core," 2022, https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2022/digital-to-the-core.pdf.
6. Dell Technologies, "Global Data Protection Index 2024," October 2023, https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm.

Your future-focused customers are also investing in cutting-edge technologies that facilitate groundbreaking transformation.

Generative AI, for example, is expected to deliver transformational benefits in the next two to five years.[7] Although the technology is nascent, innovators are already aggressively searching for ways to derive value from it. Benefiting from the speed, scale and efficiency of generative AI, organizations are reinventing business functions ranging from customer service and supply chain optimization to product development and demand forecasting.

Generative AI brings not only opportunities but also new challenges. For cybersecurity, this technology represents a dual-edged sword. On the one hand, it promises improved threat detection and response, predictive capabilities and operational efficiency. On the other hand, it requires your customers to rethink and evolve their cybersecurity strategies and protect large language models from misuse and cyberattacks.



7. Gartner, "Gartner Places Generative AI on the Peak of Inflated Expectations on the 2023 Hype Cycle for Emerging Technologies," August 2023, https://www.gartner.com/en/newsroom/press-releases/2023-08-16-gartner-places-generative-ai-on-the-peak-of-inflated-expectations-on-the-2023-hype-cycle-for-emerging-technologies.

Transforming security into an innovation enabler

Innovation leaders and adopters are 2.6x more likely to turn data into real-time insights extremely well. Yet despite 69% of organizations saying they're drowning in data, only 26% of IT decision-makers believe their innovation efforts are data-informed.[8] At the same time, the average organization spends more time firefighting security threats than enabling secure innovation.[9] These trends tell us that security often holds your customers back from transforming with data.

As a trusted expert, you are instrumental in assisting your customers in protecting their data, whether at the core, in the cloud, or at the edge.

To support their data-fueled innovation initiatives, you need to address three key security challenges:

Reduce the attack surface:
Digital transformation — including the rise in cloud solutions and hybrid workplaces — has greatly expanded the number of entry points that cybercriminals can exploit to compromise your customers' data, systems and networks. A smaller attack surface makes it more difficult for malicious actors to launch successful cyberattacks and creates a more secure space for organizations to innovate and thrive.

Threat detection and response:
With the continuous evolution of cyberthreats, threat detection and response have become a vital part of adapting to the new data landscape and safeguarding an organization's assets. By proactively identifying and addressing potential security incidents and malicious activities, organizations can neutralize threats before they inflict significant damage.

Recover quickly from cyberattacks:
Attacks are inevitable in today's threat environment. A well-executed recovery plan ensures your customers can quickly restore operations efficiently and strengthen their cyber-resilient posture.

You can grow your business by helping customers reimagine security with proven solutions that solve these challenges and advance their cybersecurity maturity. Your first step for capitalizing on this market opportunity is to understand the foundations of a robust security posture and how Dell Technologies builds these foundations for your customers. Discussing these fundamental aspects with them can also help you better position security as a critical component of innovation.

8. Dell Technologies, "The Innovation Index," February 2023, https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm.
9. Dell Technologies, "Innovation Accelerated: Innovate with a confidence born in security," 2023, https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/innovate-with-confidence-born-in-security-ebook.pdf.

The foundations of a robust security posture

Zero Trust

Organizations are adopting a Zero Trust approach to cybersecurity as they move away from the legacy, perimeter-based defense model, which doesn't address the expanded attack surface in a distributed and dynamic environment. Research shows that organizations with a mature Zero Trust architecture can reduce the cost of a data breach by 36%.[10]

In addition to designing our solutions with a Zero Trust architecture in mind, Dell Technologies and Intel demonstrate our commitment and thought leadership with Project Fort Zero — planned to be the first federally validated Zero Trust architecture for the U.S. Department of Defense and creating a repeatable reference architecture to simplify adoption.[11]

Secure supply chain

Threat actors have discovered that compromising the supply chain yields a high return on investment in the interconnected, technology-driven economy. Supply chain attacks have been growing at a rapid pace, and the European Union Agency for Cybersecurity expects supply chain compromise of software dependencies to become the top cybersecurity threat by 2030.[12]

Both Dell and Intel have implemented defense-in-depth and defense-in-breadth approaches, as well as effective risk management strategies, to effectively mitigate threats that enter the supply chain.

> Research shows that organizations with a mature Zero Trust architecture can reduce the cost of a data breach by 36%.[12]

Our strategies include:

- **Practices**, **policies**, **and principles** designed to protect digital data against unauthorized access and use that could result in data exposure, exploitation, deletion or corruption.
- **Safeguards** to protect sensitive information about products, solutions, suppliers and partners — throughout the supply chain lifecycle — against exposure and exploitation.
- **Quality control processes** to help ensure solution component integrity.

10. IBM Security, "Cost of a Data Breach Report," 2022, https://www.ibm.com/downloads/cas/3R8N1DZJ.
11. Dell Technologies, "Dell Technologies Project Fort Zero to Transform Security," May 2023, https://www.dell.com/en-us/dt/corporate/newsroom/announcements/detailpage.press-releases~usa~2023~05~dell-technologies-project-fort-zero-to-transform-security.2154.htm?hve=view+press+release#/filter-on/Country:en-us.
12. ENISA, "Cybersecurity Threats Fast-Forward 2030: Fasten Your Security-Belt Before the Ride," November 2022, https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030.

Intrinsic, embedded security

Cyber-resilient organizations are much better positioned to support innovation. ESG research shows that prepared — or highly resilient — organizations are 7.7x more likely to get their new offerings to the market ahead of their competition and grow 2x faster compared to organizations that are exposed.[13] One of the characteristics that distinguishes prepared organizations is their focus on intrinsic security: 95% say intrinsic security is either critical or important to the end-user device purchase process, and 90% say the same about data center technology purchases.[14]

Dell Technologies and Intel design cyber resilience into our solutions from the ground up. We integrate software engineering best practices throughout the development process for operating systems, applications, firmware and device drivers. Our Secure Design Lifecycle (SDL) approach ensures our products are built with secure code and includes a threat assessment process and rigorous testing.

Further, with Dell Technologies and Intel, your customers get the assurance of hardened processes, automated defenses and embedded security that begins below the OS — from the moment they boot a device — and extends to both hardware- and software-based protections.

Examples of intrinsic security features include:

SafeBIOS, a suite of tools to ensure attackers cannot corrupt the device BIOS to gain control of the system.

Intel® Hardware Shield, which provides built-in hardware security including advanced threat protection.

Silicon-based root of trust in our **PowerEdge** servers to cryptographically attest to the integrity of the BIOS and the Integrated Dell Remote Access Controller (iDRAC) firmware.

Advanced crypto acceleration technologies embedded in **Intel® Xeon®** scalable processors, enabling high levels of cryptographic security and enhancing performance.

13. ESG, Research on cyber resiliency and ransomware, 2021, https://www.delltechnologies.com/asset/en-us/solutions/infrastructure-solutions/industry-market/esg-research-cyber-resilience-and-ransomware-instagraphics.pdf.
14. ESG Research summary, "Intrinsic Security and Cyber Resiliency," March 2022, https://www.delltechnologies.com/asset/en-us/solutions/industry-solutions/industry-market/esg-cyber-resiliency-research-intrinsic-security.pdf.

Secure infrastructure and workspaces

Every component of the infrastructure — from servers and networking to storage and hyperconverged systems — as well as every endpoint device are integral to boosting security posture and cyber resilience. With Dell Technologies Trusted Infrastructure and Trusted Workspaces, you can implement a streamlined approach that reduces the attack surface and delivers multiple layers of defenses across their data ecosystem.

Dell Trusted Infrastructure

In the modern era, IT infrastructure extends far beyond centralized data centers into multicloud environments, virtual and software-defined systems, edge devices and more. Security must evolve in response to this infrastructure that operates everywhere. Dell Trusted Infrastructure provides your customers with a modern, resilient and intelligent technology foundation that enables them to protect data and systems whether on premises, across multiple cloud providers or at the edge.

Dell Trusted Workspace

Empowering employees to securely collaborate and innovate anywhere without compromise is a priority for modern organizations that want to create a competitive edge. Dell Trusted Workspace delivers a robust suite of endpoint security solutions with multiple layers of defenses to secure work-from-anywhere, minimize the overall attack surface, and protect data and applications.

The modern workforce expects fast experiences and consistent productivity anywhere. This means that device security should not make them jump through hoops. Our seamless, built-in protections empower your customers to access and triangulate data when and where they need it.

Proactive resilience

While many of your customers understand that successful cyberattacks are inevitable in the digital workplace, in a global survey more than half of public and private organizations of all sizes believe they will not be able to continue trading or transacting in the event of a cyberattack.[15]

This is where the discipline of resilience comes in. A relatively new but rapidly growing area, resilience shifts organizations' efforts to recovering from an attack and resuming operations with minimal loss and disruption. This approach complements protection by proactively preparing your customers to recover operations as quickly as possible and to lessen the impact on people, data and business operations — all while minimizing financial and reputational losses.

Dell Technologies and Intel's holistic approach to security ensures our cyber-resilient solutions can be the foundation your customers need to build their own cyber resilience.

15. Dell Technologies, "Innovation Accelerated: Innovate with a confidence born in security," 2023, https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/innovate-with-confidence-born-in-security-ebook.pdf.

A mature resilience strategy combines a well-defined incident response plan with practices such as regular backups of critical data and systems, data encryption and immutable off-site storage solutions.

You can help customers implement proactive resilience so they can recover quickly and advance their readiness with solutions such as:

- **Dell storage systems** provide multiple security layers including data-at-rest encryption, secure snapshots for granular recovery and Zero Trust protocols like role-based access.
- **Dell PowerProtect Cyber Recovery** offers air-gapped, immutable vaults to ensure your customers can retain critical data and applications in the event of a cyber incident. The vaults are monitored by CyberSense, an intelligent, automated, software-designed solution that proactively detects unusual patterns and suspicious activity with machine learning and analytics, sends alerts, protects data and streamlines recovery and restoration activities.
- **Managed Detection and Response** as well as **Managed Detection and Response Pro Plus** solutions offer a range of services aimed at boosting resilience, including a team of cyber recovery specialists to help customers restore critical data and workloads efficiently.

Data protection anywhere

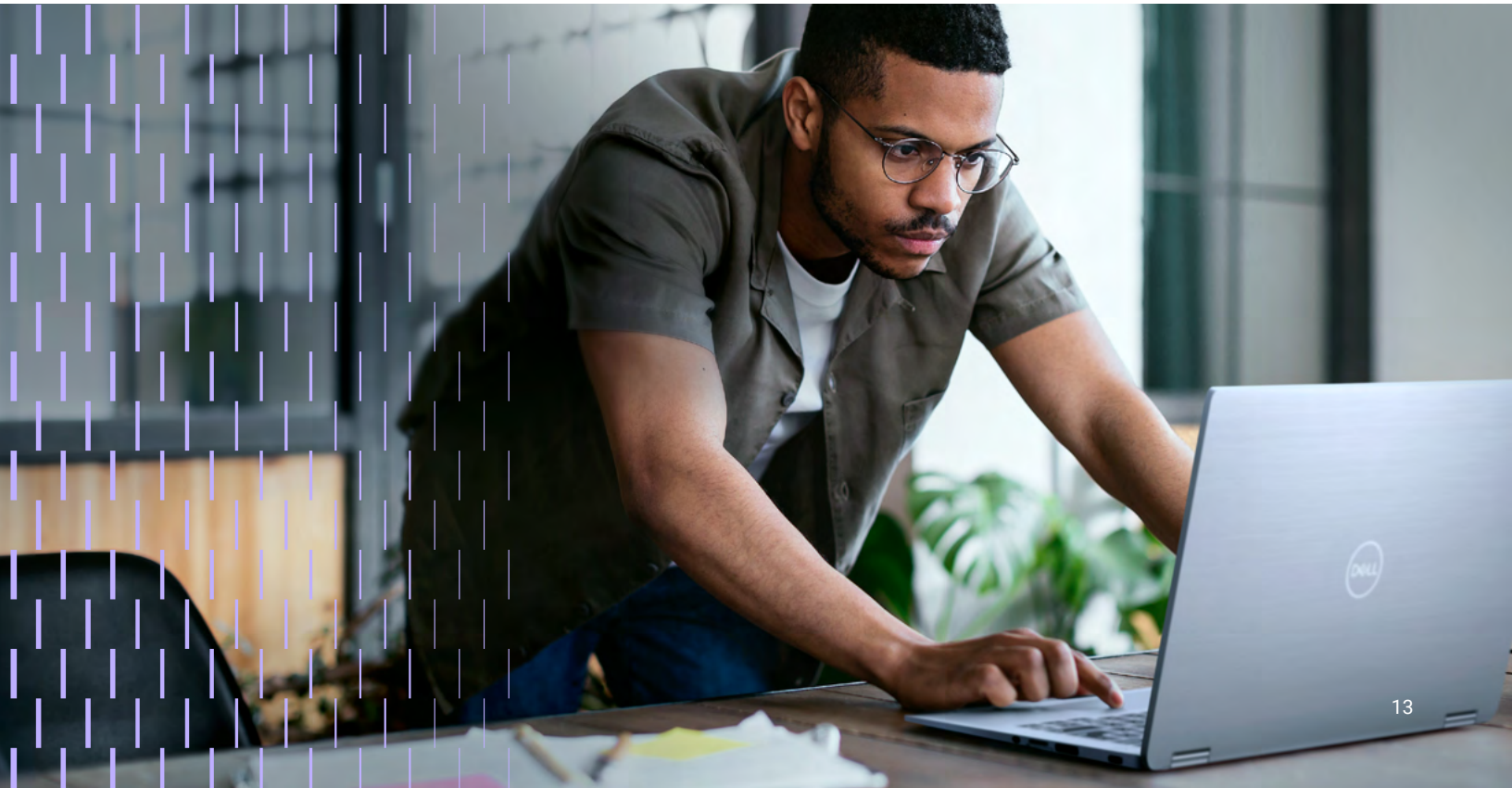
Your customers need assurance that their data is secure and protected anywhere it resides. Increasingly, the data resides in the cloud, and security is seen as the second-biggest challenge in cloud adoption (surpassed only by managing cloud spend).[16]

The complexity of multicloud environments compounds security problems, particularly when organizations use multiple security vendors. According to our Global Data Protection Index,[17] organizations that used a single data protection vendor have experienced fewer cyberattacks or other incidents that prevented access to data, compared to those that used multiple vendors. Additionally, those working with a single vendor had a lower cost of cybersecurity incidents and were less likely to experience data loss.

Dell Technologies provides you with access to a full suite of integrated data protection offerings that span software and hardware — from simple, affordable and integrated appliances for small and medium-sized businesses to robust, comprehensive data protection for enterprises. The breadth of these solutions allows your customers to consolidate their data protection, boosting security and saving costs.

> 85% of surveyed organizations that use multiple vendors for data protection believed that reducing the number of vendors would be beneficial (up from 78% the prior year).[18]

16. Flexera, "2023 State of the Cloud Report," 2023, https://info.flexera.com/CM-REPORT-State-of-the-Cloud.
17. Dell Technologies, "Global Data Protection Index," October 2022, https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm.
18. Dell Technologies, "Global Data Protection Index," October 2022, https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm.



Overcoming cybersecurity complexities with end-to-end solutions

Digital transformation and the rapid changes in how organizations use data have expanded the attack surface. Security teams have been coping by implementing a patchwork of point solutions that address specific new threats. Some teams have tried to piece together an integrated solution, but challenges such as talent shortages limit their ability to implement a unified, holistic approach.

Consequently, many organizations are looking to move away from the complexities created by the proliferation of tools and the market fragmentation. Some estimates show that 75% of organizations are seeking vendor consolidation as a way of simplifying security.[19]

No single security provider can deliver everything your customers need. End-to-end security takes an ecosystem of providers specializing in cybersecurity, along with an experienced partner such as Dell Technologies to bring it all together and help manage the complexity. Working with us gives you access to an expansive network of partners who bring valuable expertise, experience and resources to the table so you can help your customers navigate the fast-moving threat landscape.

Your partnership with Dell Technologies gives your customers an advantage by allowing them to streamline their security strategy, protect their data everywhere, reduce their attack surface and recover quickly after incidents — breaking down their barriers to innovation.

19. Gartner, "Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022," September 2022, https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-survey-shows-seventy-five-percent-of-organizations-are-pursuing-security-vendor-consolidation-in-2022.

Power the future securely with Dell Technologies

Innovative organizations are constantly pushing boundaries in how they deliver services, manufacture products, engage with customers and employees, and explore what's possible. The confidence to innovate gives your customers the edge to lead in their markets, deliver new value and drive their business forward.

Technologies such as AI, machine learning and advanced analytics make all these things possible, while secure data triangulation ensures the business is protected in the process. Differentiate yourself by showing your customers how they can harness the power of data and advanced analytics without compromising security. Rapid, data-fueled innovation is powering the future — and you can play an exciting role in helping your customers break new ground.

Harness the power of innovation with modern security from Dell Technologies.