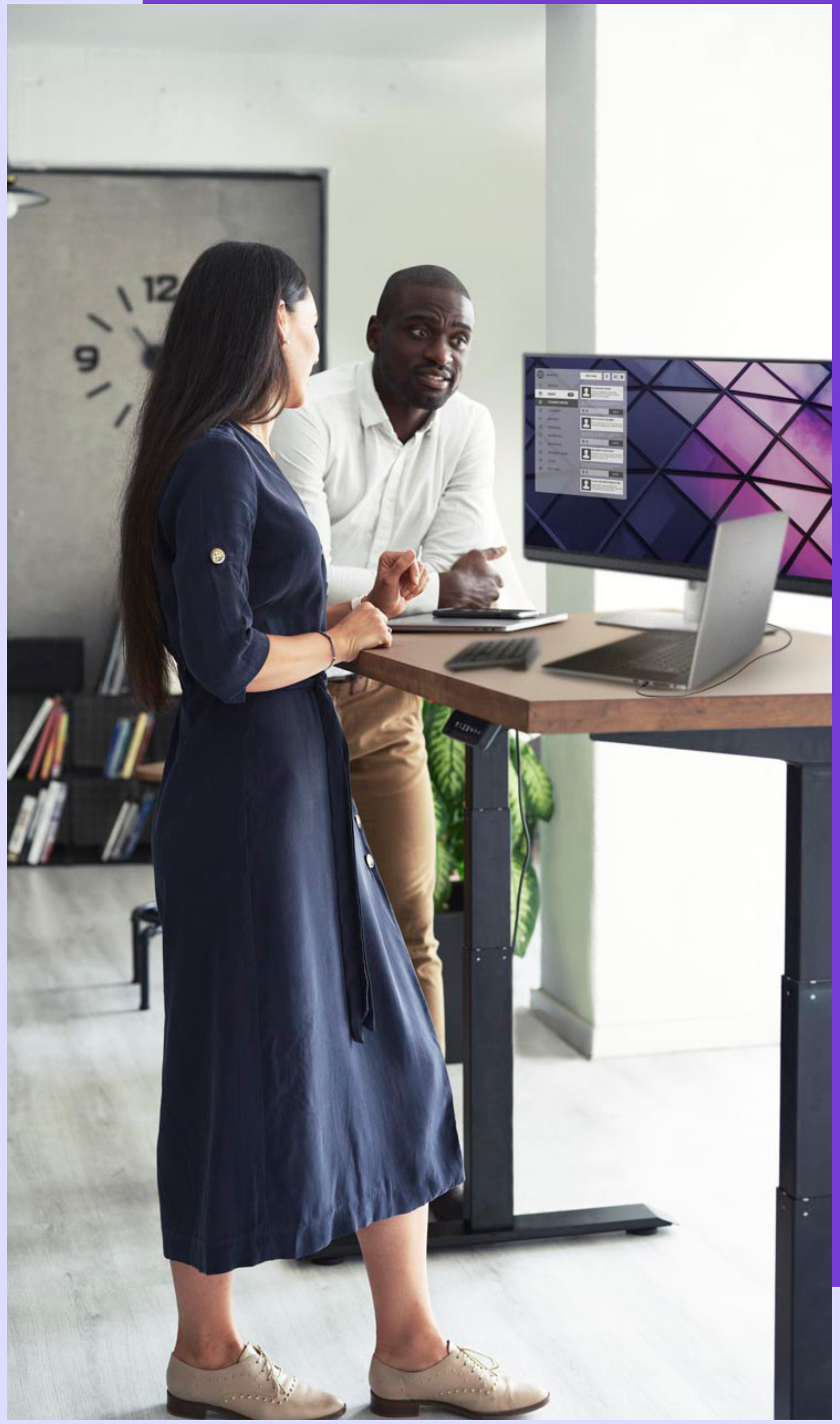
INNOVATION ACCELERATED

Innovate with a confidence born in security

DELL Technologies

Table of contents



Using modern security to empower innovation

In our recent eBook, *"Innovation Accelerated: How to turn ideas to impact faster"*, we explored the relationship between an organization's innovation maturity and its overall competitive success. This eBook explains why security in innovation is paramount: Security protects the source of an organizations' innovation—data—and gives them confidence to innovate.

As expected, security is a top concern for every organization. In the third quarter of 2022 alone, data breaches exposed nearly 15 million data records worldwide[1], a 37% quarter over quarter increase. Organizations of all shapes and sizes are dependent on their digital infrastructure: their data, end-user platforms and communications—a successful attack can have serious and grave consequences.

One consequence would be the erosion of an organization's practical and mental capacity to innovate, and with it, their ability to stay relevant and competitive. We see this reflected in our latest study, Dell Technologies' *Innovation Index*, based on responses from 6,600 business and IT decision-makers responsible for driving or influencing innovation in their organization. In the absence of sufficient protections and uncertainty about whether they can comply with new security and privacy regulations, organizations are more likely to put the brakes on their innovation: 40% admit security concerns and data/privacy regulations prevent their ability to innovate (they would focus more on surviving).

Instead, proactivity is required, in terms of consolidating many fragmented security solutions so they have greater security coverage and so they are able to adopt Zero Trust principles—a new security paradigm for protecting data and reputations in a distributed computing environment. A shift in mindset can also make a difference. According to previous *Dell research* from ESG [2], companies who have (prepared themselves for cyberattacks) are 7.7x more likely to deliver new offerings to market quicker than the competition. They're also more bullish about forward-looking business results and forecast revenue growth twice the rate of their exposed counterparts.

In other words how we contextualize security matters. We often talk about what companies have to lose in a cyberattack, but people are predisposed to try to diminish threats/hope they won't fall victim or the fallout be as dire as some people portent it might be. The Innovation Index proves this with the number three barrier to cybersecurity being not taking cybersecurity seriously (i.e., underestimating the threat). Focusing on what an organization have to gain will resonate across the board and lead to action that will make them more secure and more successful.

[1] - *Statistica Research: Number of data records exposed worldwide from 1st quarter 2020 to 3rd quarter 2022 (in millions).*

[2] - *Source: TechTarget's Enterprise Strategy Group, eBook commissioned by Dell Technologies, How to Build a Cyber-resilient Business Ready to Innovate and Thrive, March 2022*

> ***People are wired to block out bad news. Yet when we talk about security, we normally talk about what companies stand to lose and expect fear to motivate them to act. It's time to reframe the narrative and focus on what organizations stand to gain, such as the confidence to innovate and go to market faster, to develop an IP that they can protect and plan for a future where they're in control.***
>
> Bobbie Stempfley, VP, Business Unit Security Officer, Dell Technologies.

This paper will draw on further insights from the Innovation Index, including its assessment of how organizations are innovating during periods of uncertainity.

We will explore the importance of innovation to the success of modern-day organizations, the relationship between security and innovation maturity and common barriers to achieving security resilience.

Key Findings

Security plays a central role in ensuring that employees can ideate and innovate anywhere, anytime. But how well are organizations able to do this?

Only 41%

of respondents say with the utmost confidence that security is embedded within their technology and applications.

52% 48%

At present, the average organization spends more time firefighting security threats (52%) than enabling secure innovation (48%), highlighting that improvements can be made.

Focus area 2: RESILIENCE

Recover data and operations rapidly after cyberattacks and build proactive resilience with intelligent and scalable solutions.

27% have managed threat detection or automated response service in place

33% have a cyber recovery vault to protect high-value data

Focus area 1: PROTECTION

Secure and deploy data across any cloud, any workload, any consumption model and create a trusted workspace.

33% employ a holistic end-to-end security strategy integrating hardware and software protections

36% conduct audits for users, devices, assets, and cloud services to fully understand what needs to be protected

Focus area 3: CONFIDENCE

Embrace a Zero Trust mindset to future-proof your security strategy.

77% organizations have not yet explored or built a Zero Trust architecture

27% are uncertain around how to implement Zero Trust without compromising productivity

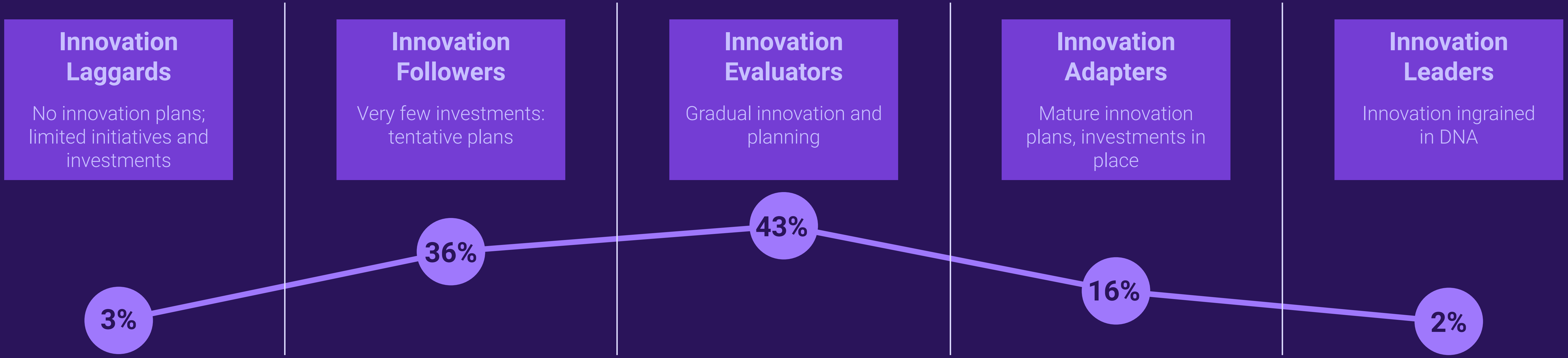
Relationship between security maturity and ability to innovate

Measuring innovation resilience

Innovation and security should go hand-in-hand. The ability to innovate freely is intrinsically linked with having a robust and mature security foundation in the organization. A secure backbone breeds confidence to innovate and protects innovation. One of the prime takeaways of the Innovation Index is the necessity to innovate through uncertainty and over time. This is innovation resilience, and it can only co-exist within a secure environment. Innovation efforts that crumple under the pressure of a cyberattack is the antithesis of resilience.

So how innovative are organizations?

By capturing and assessing how organizations' ready their people, processes and technologies for innovation, we have categorized respondent organizations into one of five innovation maturity groups– from the least mature "Innovation Laggards" through to the most mature "Innovation Leaders" based on their current performance. This is the present-day picture.



Innovation Laggards
No innovation plans; limited initiatives and investments

Innovation Followers
Very few investments: tentative plans

Innovation Evaluators
Gradual innovation and planning

Innovation Adapters
Mature innovation plans, investments in place

Innovation Leaders
Innovation ingrained in DNA

Figure 1: Showing innovation maturity model. Base: All respondents (6,600). More detailed description of each group can be found in the appendix.

Security maturity and innovation maturity are interrelated

When we compare the Innovation Index benchmark with the security measure, some interesting symmetries emerge—demonstrating the relationship between the two measures.

Overall, the distribution of organizations, based on their respective innovation and security maturity levels is similar, with only a relatively small proportion falling into the most mature groups: Security Leaders or Security Adopters, as can be seen in Figure 2.

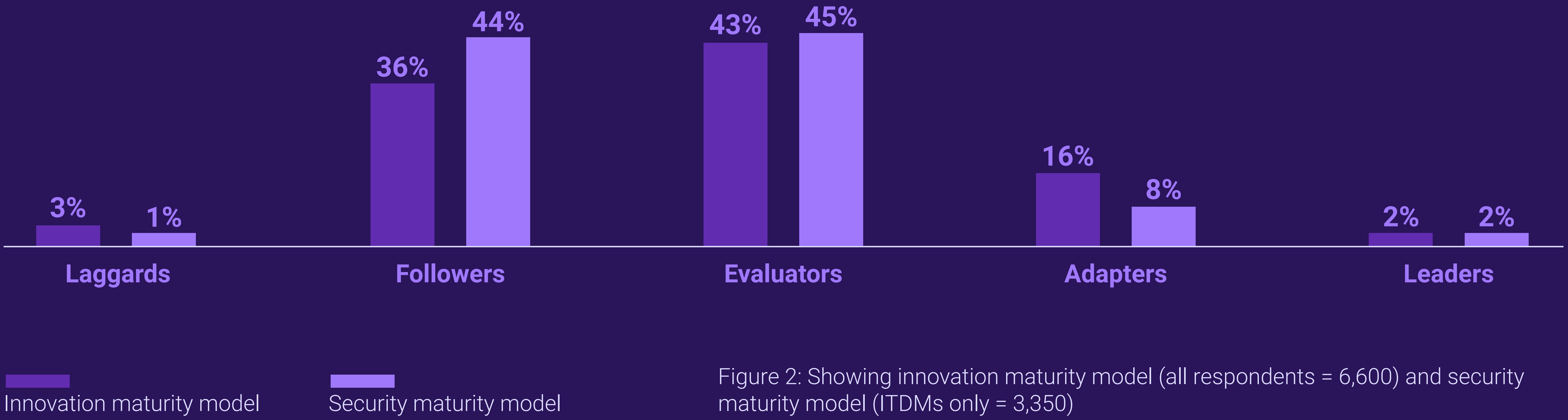


Figure 2: Showing innovation maturity model (all respondents = 6,600) and security maturity model (ITDMs only = 3,350)

For security, only 2% are Security Leaders and just 8% are Security Adopters—indicating most organizations have a lot of work to do to improve their people, processes and technology so they can innovate with confidence.

What's more, 87% of the lowest performers in terms of security (Security Laggards) are among the lowest performers in terms of innovation (Innovation Laggards or Followers). Meanwhile, 80% of the highest performers in terms of security (Security Leaders) are also the highest performers in terms of innovation (Innovation Leaders or Adopters).

Organizations that perform highly in terms of security are much more likely to perform highly in terms of innovation:

87%
of Security Laggards are Innovation Laggards or Followers

80%
of Security Leaders are Innovation Leaders or Adopters

The following ratio also draws a direct line between innovation maturity and security: Innovation Laggards and Followers spend more time firefighting security issues (57% on average) instead of enabling secure innovation (43%). Here security concerns are encroaching upon their ability to innovate. It therefore follows that they have a poor innovation score overall.

The correlations between these two maturity models proves out that developing a robust security infrastructure across the organization, with a concurrent focus on secure human behavior and secure processes are prerequisites for innovation.

Building the right security strategy to drive innovation without compromise

Key barriers

In an age where organizations' IT and data landscapes are more diverse, distributed and complicated to manage than ever before, maintaining security is a huge task. Fragmented security solutions create further complexity, meaning that the average organization is meshing countless different security providers' products, often with imperfect coverage.

The most common security issues faced by respondents: "overall complexity of the modern computing environment" and the "evolving threat landscape", reinforce complexity's reputation as the enemy of security. But there are other barriers to security that span people, processes and technology which are flummoxing the majority of organizations, who do not score highly on the cybersecurity register.

> ***Today's threats and regulatory environment require examining new areas of security when businesses are making purchasing decisions. It's no longer enough to consider only the features of a product. IT must consider the research, incident response, and overall product security assurance structure from vendors, on top of supply chain security and compliance.***
>
> Mohsen Fazlian, Corporate VP, Intel Product Assurance and Security

Top 5 elements compromising security:

1. Overall complexity of the modern computing environment
2. Evolving threat landscape
3. Employees don't take cybersecurity threats seriously/naïve
4. Too many discrete IT security solutions to manage
5. Security teams not working hand in hand with business stakeholders to define priorities

Fostering a culture of security among employees is critical

Employees also play a central role in the success or failure of an organization's security. Without organization-wide buy-in from employees on the importance of adhering to security best practices and without sufficient security expertise within the IT department, organizations will struggle to stay safe. More needs to be done to address the following:

Only 37% are educating their workforce via organization-wide cybersecurity training (including focus on multi-factor authentication and use of strong passwords)

Only 32% are augmenting personnel security capabilities with external security experts

Only 27% are hiring additional security experts

Training that addresses mindset is also important; a security culture needs to be embedded from top-to-bottom to tackle the human factor in cybersecurity.

> ***When organizations ask my advice on how to embed a security culture, I encourage them to spend less time focusing on mandatory behavior and more time celebrating success. So, when someone completes their security training on time and with great marks, congratulate and reward them. Make it a career growth opportunity and make training fun. A lesson on how to avert the bad guys is a perfect candidate for gamification.***
>
> Professor Sally Eaves, Author and Founder of Tomorrow's Tech Today and Aspirational Futures

Success factors when building an end-to-end security strategy

How do organizations become more secure? They need a strong and modern end-to-end security setup to effectively protect their operations, data and reputation, while enabling innovation. The study suggests that many do not have this currently.

Only 41% of respondents can say with the utmost confidence that security is embedded within their technology and applications. This is a boon for cybercriminals, who take advantage of gaps in defenses, no matter how small, to derail innovation efforts, steal organizations' data and hold victims to ransom.

With so much at stake, cybersecurity should be a top priority. Here are three strategic areas organizations should prioritize when architecting their security strategy:

Protection

Resilience

Confidence

Protect data and systems

Goal: Secure and deploy data across any cloud, any workload, any consumption model and create a trusted workspace

No organization can prevent a cyberattack, but they can prepare for it and take necessary steps to protect their business-critical systems and ringfence their data. A cyberattack does not need to be costly or disastrous, or successful for the attacker. Early detection and a cascade of defensive responses can mitigate the effects. However, the data suggests that presently, many businesses are not protected.

Only
33%
are securing data in transit, in use and at rest extremely well

Only
38%
are securing edge hardware, applications and data very well

Only
41%
are very confident security is embedded in their technology and applications

It therefore makes sense that the number one barrier to innovating with data is cybersecurity threats on their data. In this hyper-distributed world, security must stretch from the core to the edge to the cloud.

The only way to secure a vast attack surface and data everywhere is to develop a holistic security approach. That's not as commonplace as one would think. Just a third of organizations worldwide have a holistic end-to-end security strategy integrating hardware and software protections.

In part, the security industry is to blame. There's a glut of point-security solutions out there. Fragmentation is confounding many organizations (as the security barriers to innovation show).

And yet, according to our research, just 1 in 3 (33%) respondents say their organization is consolidating security applications to gain greater control of their IT infrastructure. One might assume they don't know where to start. In the meantime, siloed security solutions are creating interoperability issues, which cybercriminals can exploit.

Creating trusted workspaces has also never been more challenging. In the past, organizations focused on their four walls. Now they're having to secure everywhere. And yet, in this hybrid working world, just 30% of organizations are evaluating a larger, distributed attack surface for potential risks. A modest 42% are making security intrinsic to a great extent, so they can work anywhere without worrying about the security implications.

Organizations need a partner by their side that can streamline and integrate the environment to create an end-to-end ecosystem where there are no gaps.

> ***We need to remember that for most organizations, be they media companies, manufacturers, healthcare providers, consumer products firms and so on, security is not their bread and butter. They probably don't know how to outsmart a cybercriminal cell, and we shouldn't expect them to. They need a managed approach that takes nothing for granted and tracks against the changing threat landscape, so they can focus on the business.***
>
> John Scimone, President, Chief Security Officer, Dell Technologies

Partnering for success

A good security strategy starts with protecting your data. Dell is a leader in helping organizations prevent cyber threats across cloud infrastructure, workloads, and consumption models. We offer support and security from core to cloud to edge.

- Dell's Trusted Infrastructure and Dell Trusted Workspace solutions are designed to protect critical systems, applications and data while reducing systemic risk.
- Our portfolio of managed cybersecurity services provides around the clock monitoring and proactive detection of emerging threats.
- We have a global network of security experts to help thwart attacks across endpoints, infrastructure, and the cloud.

Enhance cyber resilience

Goal: Recover data and operations rapidly to lessen impact of cyberattacks and build proactive resilience with automated, intelligent, and scalable software-defined solutions

As we've established, cybersecurity should not be contained to four-walls and is not a moment-in-time effort. To achieve cyber resilience that will stand the test of an attack, organizations need to take a coordinated and sustained approach. Today:

Only 36% of organizations are conducting audits of users, devices, assets, and cloud services to fully understand what needs to be protected

Only 32% are practicing a secure development lifecycle that protects the processes by which new products, features and services are designed and developed

This vigilance extends to their IT supply chain. They need to know the goods they're supplied with are secure.

Only 36% ensure that IT suppliers have a secure supply chain in place (covering sourcing, manufacturing/assembly and delivery). Even though there is a growing expectation that organizations document their supply chain security measures

Presently, 52% say that in the event of a cyberattack, they'll likely be able to continue to trade/transact. In reality, given the large number of organizations behind the security maturity curve, the percentage that can withstand an attack and continue to operate would probably be lower. Regardless, one in two organizations believe an attack would bring down their business, albeit temporarily. How would an organization recover financially, reputationally etc.? What other area of the business would accept a one in two failure?

> ***To innovate securely and protect your data, your security teams need to be embedded in the business and their practices need to be persistent and non-negotiable. Essentially you need a robust secure development lifecycle. They're less commonplace than you would think and yet they're foundational.***
>
> Mark Lynd, Head of Digital Business, Netsync

Partnering for success

Dell helps organizations lessen the impact of cyberattacks and rapidly resume operations.

- Our portfolio of advisory services and global team of cyber recovery experts help you build resilience into everything you do and restore critical data and workloads should an attack occur.
- As you scale your multicloud environment, Dell will help you defend critical data anywhere it lives and utilize isolated vaults with immutable data for retaining critical data and applications.
- Dell can help you monitor your critical data with automated software-defined solutions designed to streamline recovery and restoration.

Protecting innovations with offensive research, defensive research and thinking like a hacker.

Security requires a multi-pronged approach—both offensive and defensive—and the ability to adopt the mindset of a hacker. With threats encroaching on every industry and along every supply chain, the vendors that IT chooses must warrant confidence in handling all of these aspects. This means that in addition to providing new technologies to businesses with built-in advanced defenses and help with detecting malware, vendors must also maintain a robust approach to cybersecurity from product development through end of support.

A security-first approach begins with processes that ensure engineers design for security, perform penetration testing, and execute threat analyses, among other things during product development. Dell and Intel both leverage the Secure Development Lifecycle, typically applied only to software, across their hardware development to implement such processes.

Businesses can find confidence in Dell products using the 11th Gen Intel® Core™ vPro® platform, codenamed "Tiger Lake," which has been put through rigorous testing against Intel offensive security engineers and an elite group of external hackers.

Intel engineers have been researching new attack vectors such as undervolting and power viruses and working to develop more advanced fuzzers that find and mitigate more potential vulnerabilities in the hardware.

Tiger Lake was also taken through Project Circuit Breaker, part of the Intel Bug Bounty program, which challenged a group of elite, outside hackers to find potential security vulnerabilities. The activity, named *Camping with Tigers*, led to further hardening of the product.

These are just a few ways Dell and Intel are contributing to a more secure supply chain and end product, delivering the devices that businesses need to innovate.

Increase security confidence

Goal: Embrace a Zero Trust mindset to modernize your security strategy

Today's security paradigm is broken. All industries are struggling to patch their way through a security model that was designed for a different era. Compounding the problem is a highly fragmented security market that requires organizations to piece together security solutions from thousands of point products. Today's complex security environment calls for a fundamental change in how we approach IT security–a new paradigm to address the way we work with distributed data, users, workloads, and resources. This new paradigm is Zero Trust.

Zero Trust is built on the idea that every point of access into your network, data, and workloads must prove it belongs there against a set of permitted behaviors or else it's treated as an attack and disallowed. It moves from a model of implicit trust to explicit trust where all devices and entities must be known and authorized. Everywhere your data and applications go, the rules go with them, and they're allowed to interact only with the known good. Zero Trust, by definition, is a highly integrated approach–it's not another point security solution.

It's a set of coordinated automated capabilities from an ecosystem of providers that must be built over time. As we're just at the dawn of mainstream Zero Trust adoption, it follows that 77% of organizations are yet to explore/build a Zero Trust architecture. But they recognize the need for Zero Trust in their organizations.

Top 5 factors accelerating the need for Zero Trust in their organization:

1. Increasing value of data means securing it is more paramount
2. Growing volume of endpoints for increasingly remote workforce
3. Increasing attack surface area due to distributed IT footprint across multiple cloud and edge locations
4. Increasingly complex supply chains that require rigorous security standards
5. Difficulty addressing new Edge and IoT security challenges

One thing holding many organizations back is lack of knowledge around how to implement Zero Trust–27% are uncertain about how to do so without compromising productivity. Leaning on a trusted partner with the expertise, scale and technology partnerships for guidance is critical for building a knowledge base, optimizing efficient rollout and avoiding blind spots.

> ***“Organizations need technology to innovate. But every IT outcome is based on consuming technology from someone, which is inherently risky unless you know who that someone is, how they built that product, how it got to you and whether it was compromised. A Zero Trust strategy puts the necessary safeguards in place to protect against these unknowns. It enables organizations to innovate with confidence in a multicloud world.***
>
> John Roese, Global Chief Technology Officer, Dell Technologies

Partnering for success

Dell is committed to leading the industry in Zero Trust adoption. Our leading infrastructure platforms and PCs, with decades of intrinsic security features built-in, are a critical foundation of the Zero Trust environment. And our global partnerships enable us to bring together the full range of technology that defines a Zero Trust ecosystem. Our approach to Zero Trust is straightforward:

- We activate all the Zero Trust principles, so you can benefit from a holistic, coordinated framework, across your hardware, workloads and clouds. We'll build on your existing capabilities in alignment with the US Department of Defense Zero Trust architecture to reach the full value of authentic Zero Trust.
- We simplify Zero Trust integration with a repeatable reference architecture. With our complete and validated approach you can achieve Advanced Maturity for Zero Trust, reduce your estimated adoption time, minimize operational disruption and manage solution cost.
- We partner to provide a cohesive, end-to-end experience. With our ecosystem of expert partners, we provide the scale and integration you need to succeed.

Project Fort Zero

Dell has launched *Project Fort Zero*, a Dell-led industry initiative with 30+ partners to ease the integration burden for organizations and accelerate the path to Zero Trust. We are delivering an end-to-end advanced maturity Zero Trust private cloud solution validated by the US Department of Defense.

Project Fort Zero brings together capabilities and technology from more than 30+ partners, integrated by Dell, to help accelerate adoption in the following ways:

- Enables advanced maturity Zero Trust from day one
- Provides a repeatable reference architecture serving a variety of use cases
- Leverages the U.S. Government's Department of Defense Zero Trust architecture as a blueprint
- Allows flexibility to migrate workloads at your own pace

Organizations are eager to embrace Zero Trust for the security assurances it provides. But for many, the path to Zero Trust is confusing and difficult. Dell is committed to demystifying Zero Trust with a streamlined approach grounded in technology, services and partnerships, so as to remove complexity and accelerate innovation.

Lessons learned from innovators

Studying how innovators are approaching and prioritizing security provides a useful blueprint for success.

Compared to Innovation Laggards and Followers, Innovation Leaders & Adopters are:

1.6x more likely to be already exploring/building a Zero Trust architecture

1.6x more likely to be to be using a managed threat detection and response service

1.6x more likely to be employing a holistic end-to-end security strategy for hardware and software

Innovation Leaders and Adopters have a higher level of confidence in their security posture and, by association, innovation potential, because of the time and expertise they have put into getting security measures right, Their security controls are effective without being intrusive or onerous.

Innovation Leaders and Adopters also perform highly in the following areas:

67% have a good balance between access and security controls

66% have achieved peace of mind that employees can work from anywhere and find inspiration from everywhere

65% have a secure edge (enabling them to securely innovate at the edge)

Of course, none of these stats are close to 100%. Innovators are also on a journey. In fact, with greater maturity comes greater awareness of what they need to do next. But they are lighting the way towards greater confidence to innovate and creative freedom.

INNOVATOR SPOTLIGHT:

The State of Oklahoma

Advancing the state by 20 years with secure innovation

Idea

The State of Oklahoma wanted to be the smartest state in the world and deliver a gold standard in customer service by using technology to provide secure mobile services to its citizens. It had a long way to go. Its systems and data were siloed and unprotected. Engineers weren't confident that if their primary data center went down, they would ever be able to recover their systems. That was a scary proposition as the organization provides the IT backbone for every agency in the state.

+

Technology

It embarked upon an ambitious digital transformation to protect a diverse environment with a single platform. Cognizant that a cyberattack could shut-down state services, it modernized its disaster recovery and moved 2.6PB of data and 9,000+ databases to a remote data center. Not only was the size of the migration substantive, data had to be moved from "all over the place". Without the modernization effort, this would have been a very manually intensive undertaking, if not impossible.

=

Impact

The State of Oklahoma estimates that in the space of one year, it moved its information services forward by 20 years. It now has the core technologies to confidently support 189 agencies, affiliates and municipalities and enable secure innovation.

Since partnering with Dell, the state has already successfully fought off more than 3.8 trillion cyberattacks. With its data recovery solution, it can be up and running within hours of a cyberattack. And with security built into all its software, it can now unleash its team to connect four million citizens to services and become a top 10 state.

Learn more **here**

Conclusion

With cyber threats exploding in volume and sophistication and with organizations' IT infrastructure growing in complexity and distribution, security is a greater challenge now than ever before. There are more data and applications spread across multiple clouds, more people working in more locations, and more security solutions to manage.

Of course, every organization strives to be more secure but, every day brings new security vulnerabilities and attack vectors. They also have to tread a fine a line. The wrong sort of security can crush innovation. The right sort emboldens employees to innovate.

We're at an historic crossroads in cybersecurity. Organizations tend to think of security as a daunting, never-ending effort that may never assure them protection. To some extent they would be right.

In this connected world, motivated cybercriminals will always find a way in. In fact, no IT or cybersecurity company should claim they can fully prevent organizations from falling prey to or being impacted by cyberattacks. But trusted security partnerships and a Zero Trust approach can both protect and fuel innovation.

Organizations know they can trust Dell Technologies to help them solve their biggest IT and business challenges. We solved hybrid work, we help organizations solve multicloud chaos, and with Zero Trust as a north-star, we'll help you solve your toughest security challenges.

To learn more about Dell's security portfolio, visit *Dell.com/SecuritySolutions*

To explore other important building blocks for your innovation strategy, visit *Dell.com/AccelerateInnovation*

Innovation and security maturity curve group descriptions

Laggards	Followers	Evaluators	Adapters	Leaders
Innovation Laggards perform poorly across a range of innovation markers, with considerable improvements needed across the board. They almost never have processes in place to facilitate innovation and do not work with partners to improve innovation success. Leaders do not model or encourage innovation from across the organization.	**Innovation Followers** underperform across a range of innovation markers, with improvements needed. They are unlikely to have processes in place to facilitate innovation, but they may work with partners, in a limited capacity, to improve innovation efforts. Leadership is unlikely to encourage innovation across the organization.	**Innovation Evaluators** innovate in some areas but are mostly stuck in evaluation stage. They lack a clear and holistic strategy and means to move forward. They have processes in place to facilitate innovation and will partner with organizations to advance these efforts. Leadership needs to be coached to encourage innovation from across the organization.	**Innovation Adapters** are largely successful in their innovation efforts, but small improvements are needed. They're likely to have processes in place to facilitate innovation and often work with multiple partners to improve innovation efforts. Leaders encourage innovation from across the organization.	**Innovation Leaders** are successfully advancing innovation across the business. They have end-to-end processes in place to facilitate innovation and typically work with multiple partners to progress innovation efforts. Leaders actively encourage innovation from across the organization—their workforce is empowered to innovate.
Security Laggards are very unlikely to have robust end-to-end security in place, with this often hindering innovation. Remote work is typically not secure. They are unlikely to be improving cybersecurity skills across the company and protecting their data well. Laggards have not implemented a Zero Trust architecture.	**Security Followers** are unlikely to have robust end-to-end security in place, with this often hindering innovation. Remote work is unlikely to be secure. They are unlikely to be improving cybersecurity skills across the company and protecting their data well. Followers are highly unlikely to have started exploring implementation of a Zero Trust architecture.	**Security Evaluators** are relatively likely to have robust end-to-end security in place that enables confidence when innovating but they sometimes struggle with this. Remote work is relatively likely to be secure. They are relatively likely to be improving cybersecurity skills across the company and protecting their data well. Evaluators are unlikely to have implemented a Zero Trust architecture but will often have explored this.	**Security Adapters** are highly likely to have robust end-to-end security in place that enables confidence when innovating. Remote work is highly likely to be secure. They are highly likely to be improving cybersecurity skills across the company and protecting their data well. Adopters are relatively likely to have implemented a Zero Trust architecture already or at least explored this.	**Security Leaders** have very strong end-to-end security in place that enables total confidence when innovating. Remote work is always secure. They are always improving cybersecurity skills across the company and protecting their data well. Leaders have almost certainly implemented a Zero Trust architecture already.

Methodology

Dell Technologies commissioned independent market research specialist Vanson Bourne to conduct this research. The study surveyed 6,600 respondents from organizations with 100+employees from across the following regions: North America, LATAM, EMEA, APJ and Greater China. These organizations are from a range of public and private sectors.

All respondents either drive or influence innovation in their organization. Of the total number of respondents, 3350 are IT decision-makers (ITDMs) and 3250 are business decision-makers (BDMs). We asked only ITDMs to answer questions related to multicloud, data, edge, security and hybrid work strategy/performance in their organization.

The interviews were conducted online and via telephone in September and October 2022 and were undertaken using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

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. **www.delltechnologies.com**

intel.

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. **www.intel.com**

VansonBourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. **www.vansonbourne.com**