DELL Technologies

Focus On Trust Is Integral To Your Security Posture

FEATURING RESEARCH FROM FORRESTER

Defend Against Cyberattacks And Emerging Threats

It’s not news to anyone that cyberattacks, and the security and resiliency efforts to combat them, are of critical concern in this era of digital transformation. But it is worth calling out an emerging dynamic of this security battleground – that is, trust in institutions has become paramount.

In this data age, data is being produced, synthesized and stored at exponentially increasing rates. The Dell Technologies 2021 Global Data Protection Index (GDPI) indicates that organizations are managing 10X the data they were just five years ago – almost 15 petabytes on average now. There is understandably a growing concern among your customers and partners about just who oversees protecting the integrity of all that data. An organization should expect to be targeted in a cyberattack – likely multiple times. And the sheer volume and velocity of data in play today makes it difficult to scale security operations to keep pace. Customers, partners and influencers are questioning who best can help keep them safe, maintain continuity of service, and operate responsibly and with integrity.

IN THIS DOCUMENT

Recent cyber crime trends highlight the challenge. As we’re witnessing the impacts of large-scale, publicized attacks, faith in institutions continues to erode. As a result, organizations are seeking a trusted partner to work with in managing security complexity. This presents a “trust opportunity” for organizations as people seek entities that share the values they do. Organizations are beginning to understand this, and it’s causing them to re-think their security strategy.

It should come as no surprise that security challenges come up in virtually every conversation Dell has with its customers. And for good reason. The **consequences** of an attack can be devastating to an organization’s operations, reputation and financials. Still, according to the 2021 GDPI over two-thirds (67%) of IT decision makers **lack confidence** that all their business-critical data can be recovered in the event of a destructive cyberattack or data loss. This is due to the daunting **complexity** of securing the modern, hybrid, distributed IT ecosystem – where the attack surface becomes greater and cyber threats grow in frequency and sophistication. Complexity is the enemy of security, and cyber criminals are eager to exploit newfound vulnerabilities brought by accelerated digital transformation.

HOW DELL TECHNOLOGIES CAN HELP

Technology has never been more important. During the pandemic, technology has had an accelerated role in all aspects of society, and Dell Technologies believes technology is an overwhelming force for good. To help safeguard technology’s role in human progress, Dell Technologies is here to help you plan, prepare and protect against attacks.

Built-in security from an end-to-end provider. Security, privacy and resiliency must be central to the design, sourcing and manufacture of digital products and services. That is, it must be intrinsic. Every offering from Dell Technologies has security built-in, not bolted on. This provides a deeper and more organic starting position for organizations to defend themselves. And because Dell Technologies is among the world's largest technology providers, we have a unique perspective for enabling embedded security into solutions from core to cloud to edge.

Secured processes. For Dell Technologies, security and trust begin well before you purchase a product. Sophisticated attackers are constantly trying to insert vulnerabilities into processes and those threats can trickle all the way to where data and applications live. To combat this, Dell Technologies has, over decades, developed its Secure Development Lifecycle and Secure Supply Chain – two hardened processes that help ensure our solutions arrive free from threats and reinforced against vulnerabilities.

Have a plan to protect data and operations. Planning is critical to help combat and respond to cyberattacks. Utilize Dell Cyber Consulting Services with the expertise to bring together technologies, processes and people to create custom security solutions.

- Assume not just that you're going to be attacked, but that you've already been attacked. Adopt Zero Trust Architecture (ZTA) and principles that integrate redundant internal controls that can help prevent threats from proliferating even if they've already entered your environment.
- Run simulations that are designed to reveal your vulnerabilities and address them before live attacks enter your systems.
- Use a data vault such as Dell Technologies PowerProtect Cyber Recovery, that isolates data in immutable fashion, so recovery is secured, and you can direct a rapid return to operations.
- Adopt the NIST Cybersecurity Framework with dozens of industry best-practices for combating threats.
- Prioritize protecting data and operations within your company culture so that it becomes the core of trust with your customers.

Align on values with trusted partners. Security and resiliency are quickly evolving into a conversation about trust. Ultimately, that's really what this is all about. Your customers want a trusted partner who shares their values. In turn, you want a trusted technology provider who can help you ensure your customers' protection, who puts your interests first, and operates with transparency, integrity, and accountability.

Dell Technologies is committed to driving real human progress. Our Progress Made Real initiative and our corporate Moonshot 2030 goals reflect how we see our role in corporate and social responsibility, and the specific objectives we've set for ourselves to realize that vision. Our aim is to demonstrate our values in how we conduct ourselves in our industry and our global community – that is, to Win with Integrity.

Defend Against Cyberattacks And Emerging Threats

August 2, 2021

By Jeff Pollard with Joseph Blankenship, Melissa Bongarzone, Peggy Dostie

Summary

Defending against cyberattacks and emerging threats is a familiar mission for security, risk, and privacy pros. Now that mission is more strategic in nature: helping the business become — and remain — a trusted business. Doing this requires leaders to make competence, integrity, and empathy their guiding principles while executing the five stages of The Forrester Defend The Trusted Enterprise Model. These stages are bound together by Forrester's Zero Trust Model of information security, as they loop with each other to create incremental and transformational improvements, respectively.

Security, Risk, And Privacy Form The Foundation Of Trusted Business

Through the years, security lost its way. Defense in depth became expense in depth. An industry made up of autodidactic security, risk, and privacy pros morphed into something more akin to the cyberindustrial base as vendors hyping the latest tech emerged like mushrooms after a spring rain. Cash flowed in from investors to vendors to marketers, and then from customers to vendors back to investors, with limited results and virtually unnoticeable links to business objectives. This technology-first approach to security has to change. Savvy security leaders must move beyond current ways of thinking as they prepare for the trust imperative, the next major catalyst of enterprise change, moving beyond confidentiality, integrity, and availability (the old CIA triad). Instead, they will prioritize competence, integrity, and empathy (the new CIE triad), which will become the foundation of the trusted business. This requires a strategic shift in focus prioritizing:

- **Competence, but with far more balance than before.** Execution matters for every innovative and successful business. As threat actors improve, regulations multiply, and consumers get educated, security, risk, and privacy pros must demonstrate competency in their ability to defend the business and promote trust. Security, risk, and privacy leaders must invest in hiring, training, and retaining their teams to maintain a high competence level. At the same time, leaders must stop elevating competence above all else by eliminating requirements that prevent people from joining or staying in the industry. They must also remove toxicity from their teams while promoting diversity and inclusion.

- **Integrity, to ensure the firm can live its values.** As faith in institutions continues to erode, people seek entities they can trust and that share the values they do. Companies with an authentic commitment to the values they espouse will gain market share as the trust opportunity emerges. Security, risk, and privacy pros play an essential role as customers become more aware of the data they share with companies since protecting and defending that data — and the trust placed in the company when it's shared — is paramount. As companies use data to make more and more decisions — many of them automated — trusting that the data is accurate is also a must. Security, risk, and privacy pros will act as the conscience of the organization, providing assurance that data is protected, reliable, and being used in ways the brand promises.

- **Empathy, even as chaos spreads through industries and geographies.** Economic turbulence, geopolitical tensions, and discovery of major vulnerabilities being exploited by threat groups aren't new challenges, they are cyclical. With that backdrop, forgetting that users are just trying to do their job and are also victims is all too easy for teams charged with defending the enterprise. But operating with empathy internally to employees, and externally to customers, will become a defining characteristic of successful security, risk, and privacy leaders. No matter how competent and how much integrity teams and programs have, failing to remember that human beings represented in the rows and columns of each spreadsheet and record in a database will cripple leaders and their teams. Leaders in the trusted business empathize with their users, stakeholders, and their business's customers, remembering that security is a humane endeavor and not solely a technical exercise.

Defend Against Cyberattacks And Emerging Threats

The guiding principles of the CIE triad will underpin how security, risk, and privacy pros accomplish the tactical, operational, and strategic goals of their programs. Emerging threats to a business can include cyberattacks carried out by nation-state threat groups, aggressive regulatory oversight, or increased legislative activity designed to curtail monopolistic platforms. Security, risk, and privacy programs to defend the business must address each of these. While each of the five phases stands alone, they also link together to form a feedback loop of consistent, incremental improvements for the program. Security, risk, and privacy leaders moving from vision to execution should follow five steps (see Figure 1).

- **Evaluate and design: Tailor your strategy based on the threats to your firm.** Use customer and employee use cases, coupled with the firm's strategic objectives to become a trusted business, to dictate the components of your vision, strategy, and roadmap. This not only allows leaders to stay in sync via shared goals and objectives, it also places concepts like threat models as key to the firm's trust as a new focus area. Understand your program's maturity and standing in the company as well as the risks facing the firm. Use this understanding to design a program to address those risks and increase overall maturity.

- **Architect and implement: Customize and rightsize your tech stack.** Complexity remains the number one challenge for security and risk decision-makers. Numerous vendors and tools, the velocity at which business changes, and a vast array of deployment models ranging from on-premises to serverless infrastructure hosted in the cloud all play a part in that complexity. Using the Zero Trust capabilities like Zero Trust edge (ZTE) and Zero Trust network access (ZTNA) will reduce complexity while securing remote resources. Architecting and implementing security solutions that work across distributed, immutable, ephemeral, and autonomous workloads will create seamless security experiences for customers and employees. Instead of buying specific vendor technologies for every use case, look for vendors that solve for multiple use cases in an integrated security platform.

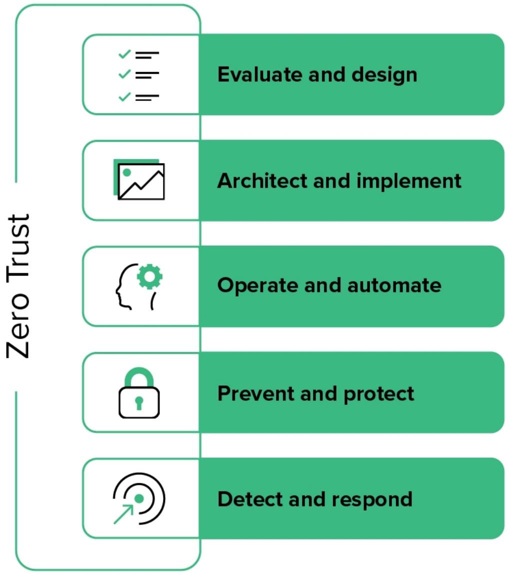
- **Operate and automate: Optimize and ruthlessly automate for efficiency.** Security teams have historically responded to rising operational challenges by throwing bodies at them. That is, they hired more and more security pros to operate technologies. With the scarcity of available security talent, security, risk, and privacy leaders must take a lesson from developers: If something repeats, automate it. Avoid tool and headcount sprawl by making this a cornerstone element of your security strategy. Doing this requires visibility, metrics, process, and maturity. Keep security, risk, and privacy teams focused on strategic objectives, not context switching between interfaces and checklists, to make sure something that should happen — is happening.

- **Prevent and protect: Stop breaches and threats when possible, prepare for the inevitable.** Trust is under constant scrutiny; stopping data theft and operation-disrupting threats like ransomware before they happen helps preserve that trust. Stopping data loss and business disruption also demonstrates competence, integrity, and empathy — by showing customers and employees that your firm means it when it says that it takes security and privacy seriously. Reduce the firm's attack surface by following Zero Trust principles, and harden the enterprise by taking lessons from the next phase to force improvements in this one.

- **Detect and respond: Hunt, contain, and respond to intrusions.** The goal is not to prevent an intrusion, the goal is to help the organization become a trusted business. Trusted businesses do not allow multiple intrusions to occur, or they will not remain trusted. This phase is not a failure state, but an opportunity for transparency and improvement, especially by demonstrating to customers and employees that they are the victims here. This is where observability for constant situational awareness, effective analytics, and expertise converge to find sophisticated and emerging threats that bypassed the earlier stages. Teams must find ways to shed tactical activity and become more proactive, allowing skilled personnel equipped with mature processes respond quickly. Take the lessons learned here, and use those as fuel to drive improvements in each earlier stage.

Figure 1

The Forrester Defend The Trusted Enterprise Model



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Defend The Trusted Enterprise

Forrester's security, risk, and privacy service features a set of interlinked reports that help leaders defend the trusted enterprise, guiding them from vision to execution. This research starts with the idea that business objectives — not security objectives — must be the primary motivating factor for leaders in these domains. From there, the research helps teams understand what's coming next and what to do about it. Then, it dives into the construction of a security program based on these new objectives. Finally, it discusses delivering results that matter to customers, stakeholders, and employees. These converge to advance your overall security, risk, and privacy maturity. This research falls into three stages.

- **Define: Observe your current state, find the gaps, and create your vision.** These reports note the important changes on the horizon that businesses — as well as security, risk, and privacy programs — will need to adapt to. These include challenges your organization currently faces. An assessment enables you to gauge your current Zero Trust maturity, and benchmark data lets you compare your progress to others. We also include research about the top threats faced by security, risk, and privacy pros in the near future and how to defend against them.

- **Apply: Adopt best practices, competencies, and technologies to achieve success.** This research provides detailed frameworks, methodologies, and best practices to address the needs of your enterprise as it orients itself around the trust imperative. The research includes a report to help you reinvent breach notification as an opportunity to demonstrate the firm's empathy. Other research explains what ZTE and ZTNA will mean for your organization and provides guidance on the adoption of Zero Trust prevention and detection technologies. Finally, research on the rapidly growing area of detection and response provides context on the categories of vendors and their offerings in emerging market segments.

- **Accelerate: Take specific steps to expand the impact of your competence.** Research in this topic will help your security program successfully execute. This research stream includes comprehensive Zero Trust security metrics, detailed evaluative research on managed detection and response (MDR), email security, and threat intelligence vendors. Practical guides to implement Zero Trust and improving threat detection efficacy using built-in operating system security act as a catalyst to help accomplish your security goal of defending the trusted enterprise.

Take The Assessment To Gauge Your Zero Trust Readiness

Security, risk, and privacy leaders charged with defending their trusted enterprises must regularly assess their firm's approach to Zero Trust. Based on the outcome of that assessment, you can then work with stakeholders throughout the enterprise to continuously improve. Take the assessment to identify your current state and set your baseline based on Zero Trust. This will help identify your current maturity stage: beginner, intermediate, or advanced. The assessment results will prescribe the pragmatic next steps to take on your guided journey to defend against cyberattacks and emerging threats.

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

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.