DELL Technologies

The imperative for data-smart security

Building a resilient business in the digital transformation age

PART 1 IN A 2-PART SERIES

Security as the competitive differentiator

In the digital era, data drives the success of your business, powering everything from customer acquisition strategies to the evolution of your business model. Your teams rely daily on the digital information from the data that they generate, collect, share, and store as they do their work and interact with customers. As the foundation under every aspect of your digital organization, data also gives you the insights into how to become more agile, derive more value for your customers, and grow revenues.

Your ability to collect, share, and store all this information securely becomes business-critical—and that means data changes the role of your security.

Viewing data security as an asset rather than a barrier enables you to build digital trust, which boosts brand loyalty, improves the customer experience, and propels employee innovation. Proactive security is no longer simply a fundamental requirement that protects your organization from disruption and financial loss. It becomes the cornerstone that gives you a competitive advantage.

Medium businesses that want to turn security into a strategic pillar need to find a balance between innovating and mitigating risks. How can you, as an IT leader, use data intelligently in security decision-making—and ensure you have the right infrastructure, systems, and culture?

Proactive security is no longer simply a fundamental requirement that protects your organization from disruption and financial loss. **It becomes the cornerstone that gives you a competitive advantage.**

Top five consequences of a disruptive event for midmarket organizations in 2019:[2]

- Loss of employee productivity
- Loss of revenue
- Inability to provide essential services
- Loss of customer loyalty
- Delay in product or service development

The challenges of the connected world

As you integrate new digital technologies into all aspects of your business, data transforms how your employees, partners, and customers engage with your organization. Yet this growing number of touchpoints, along with the evolving IT infrastructure, challenges the ability of your business to remain resilient in the face of new threats.

There is no question that your bottom line can take a hit from a security breach. In 2019, the mean cost of a security incidents for medium firms was $184,000 in 2019, up from $44,000 in 2018.[1] But there's more at stake than loss of revenue.

Disruption caused by weak security is a growing trend—35 percent of organizations surveyed in 2019 suffered a disruptive event in the previous 12 months that prevented data access due to a cyberattack or cyber incident.[2] In 2018, that number was 28 percent.

And this risk is growing: 35 percent of those surveyed in 2019 suffered a disruptive event in the previous 12 months that prevented data access due to a cyberattack or cyber-incident, compared to 28 percent in 2018.

Digital transformation has also placed a higher priority on new and emerging technologies such as cloud-native applications and the Internet of Things. These technologies bring specific risks as well as more data that's shared with business partners and others outside the corporate network.

Defending this growing IT ecosystem and amount of data—on every device, in the data center, and in the cloud—requires a comprehensive, end-to-end, embedded security strategy. But too often, security creates barriers that impede productivity, innovation, and customer engagement. For IT leaders, the challenge then becomes how to implement robust protections without overly restricting employees and deterring customers. This is where your security strategy and investment can become a differentiator.

1. Hisccox, "Hiscox Cyber Readiness Report," 2019.
2. Dell Technologies, "Global Data Protection Index–Cloud Environments," March 2020.

In an international survey of more than 1,300 workers at medium businesses, **37 percent admitted to sometimes working outside of corporate security protocols.**[3]

How to differentiate? Be data smart.

Budget constraints. Smaller IT staff. Competing business priorities. When you put these and other challenges against the growing footprint and complexities of your IT landscape, it's clear that you need a game-changing plan for security.

Using a data-smart approach to guide your decisions makes the path toward business resilience less daunting. It enables you to streamline resources while building a solid foundation that allows security to evolve in step with the fast-paced changes in your organization. What does smart-data security look like? It's a strategy built around three elements:

1. Data-first lens

For security to work, you need to examine every layer and touchpoint in your IT landscape, whether data is used and accessed on endpoints, in the data center, or in the cloud. Visibility into who touches critical data (including outside, unauthorized, and malicious actors), how, and where ensures you can create a comprehensive, end-to-end strategy.

2. Data-guided decisions

Your technology—including hardware and software—and your people and processes all impact risk. To make informed decisions about protecting assets, you need to look at the intersection of these components, using data as a guide.

People and processes: As a digital organization, you've empowered employees to be productive, and not just inside the corporate walls. This increasingly mobile and remote workforce accesses customer data and intellectual property from different locations, which can increase vulnerability. In an international survey of more than 1,300 workers at medium businesses, 37 percent admitted to sometimes working outside of corporate security protocols.[3] Sixty-three percent of those employees said they circumvent controls in order to work more effectively. Data can show you where your processes are breaking down and help you develop a security-first culture without stifling employee efficiency.

Software: Collaboration fuels the modern workplace, yet about half of midmarket organizations struggle to enable employees to share data easily and securely.[4] Many medium businesses make device security a priority, and rightly so—considering that 68 percent of organizations report at least one successful endpoint attack that compromised data or IT infrastructure.[5] Yet that's only a baseline. You need to ensure that files remain secure even when they're shared via the cloud, email, and portable media.

Hardware: Threat actors are exploiting hardware-level and silicon-level weaknesses, and 63 percent of organizations have experienced a security breach in the past 12 months due to a vulnerability at these levels.[6] Security needs to start below the operating system, with data protection physically built in at the BIOS level.

3. Data as a differentiator

Data-smart security is not about "checking a box." Only when you address the full spectrum—from devices to data center, across network, and in the cloud—will you position your organization for differentiation. As you adopt intrinsic security and build your business around trusted devices, trusted data center, and trusted data, customer trust will follow.

[3] Dell EMC, "Securing User Devices and Data in the Age of Digital Business," 2019.
[4] Forrester Consulting, "The Case for End-to-End Solutions for Mid-Market Firms," July 2019.
[5] Ponemon Institute LLC/Morphisec, "The Third Annual Study on the State of Endpoint Security Risk," January 2020.
[6] Forrester Consulting, "BIOS Security – The Next Frontier for Endpoint Protection: Today's Threats Upend Traditional Security Measures," June 2019.

Your data-smart security approach

Using your data-smart lens, take a comprehensive view of your entire IT ecosystem. These are the key questions to ask:

1. What are the policies, processes, and strategies that hold your people accountable?

A strong security culture is instrumental to an end-to-end security program. A lot of your risk, after all, comes from people—not only your employees but also business partners, vendors, and contractors.

Your policies and processes are ineffective without a way to keep people accountable. But before you can require accountability and compliance, you need a security culture that fosters proactive security awareness and is embedded across your entire organization—starting with IT managers who think security first.

In addition to cultivating a strong culture, use tools to secure people-centered processes. Best practices such as multifactor authentication and secure credential management ensure that only authorized users access data.

2. How are you managing, protecting, and encrypting critical data?

Many organizations encrypt data at rest while on an endpoint, but what happens when that data leaves the device? Is it still within your control and can you monitor access and continue to provide protection? File-centric encryption ensures data remains protected whether it's on a device or in the cloud, and even when it's emailed or transferred to a storage device.

Data centers also play a critical role in the resilience and security of your IT, which means your assessment can't stop at the device level. Whether data is accessed on-site or in the cloud, you can manage data more securely by implementing technology such as servers equipped with layered security and storage that has both drive-level encryption and built-in data protection.

3. Are your hardware safeguards adequate?

The growing sophistication of security technologies forces attackers to explore new infiltration tactics. The BIOS is emerging as a new exploitation vector. And it's not just data at stake—breached hardware can compromise entire systems, and systemic damage has wide-reaching implications.

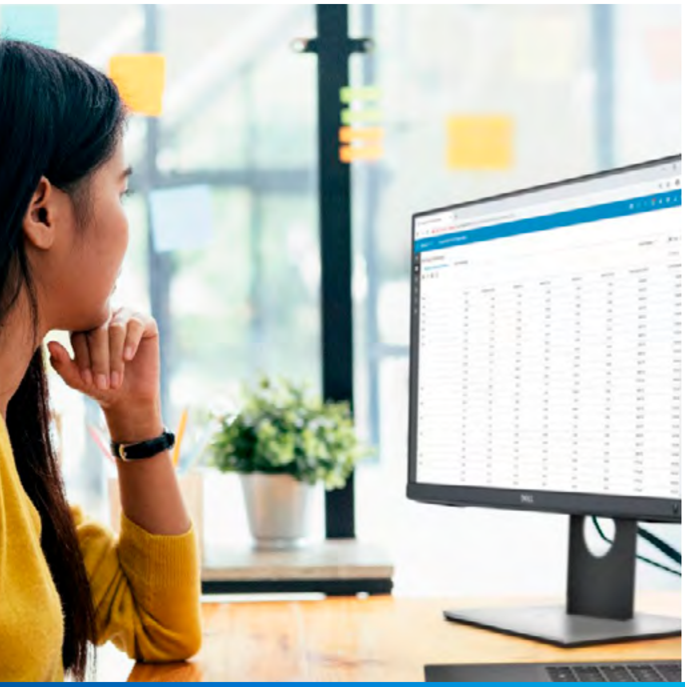
Hidden at the deepest PC layer, chip-level attacks are difficult to detect. A combination of BIOS-level protections, firmware security, and automatic monitoring (by AI and security experts) can address this threat by verifying BIOS integrity and other features that improve resilience.

Know your desired outcomes before you ask these questions. As you thoroughly examine your technology, processes, and culture, you'll start formulating a strategic approach that aligns with your end-to-end vision and chart the solutions you need.

What's next?

Data-smart security ultimately means decision-smart growth. Creating a resilient organization built on trust requires a new mindset.

Reliance on data transforms the way businesses of all sizes operate, innovate, and grow. Viewing security as an opportunity in this fast-changing world gives your organization a competitive edge while positioning it for the future.



To learn how to choose or build the right security solutions for medium businesses, read part 2 in this series, "Enacting Data-Smart Security Solutions."

Read it now

End-to end, data-smart security from Dell Technologies

Dell Technologies enables your data-smart approach with end-to-end security built in, from devices to the data center. We offer best-in-industry and best-in-category solutions that include industry-exclusive features designed to help you lay the foundation of your digital organization and meet the needs of your modern workforce.

Our range of security solutions includes:

- Dell SafeData—enterprise-grade data encryption to protect sensitive data on the device an in the cloud and maintain compliance.
- Dell SafeID—secure processing and storage of user credentials on an exclusive, dedicated chip.
- Dell SafeBIOS—automatic detection of BIOS changes and prevention of tampering beneath the OS with Dell-exclusive off-host BIOS verification.

Dell Technologies enables medium businesses to protect their entire IT ecosystem by providing:

- Trusted devices—enterprise-grade Dell Latitude and Dell OptiPlex laptops with built-in SafeBIOS, SafeData, SafeID, and other security features.
- Trusted data centers—built-in BIOS-level security, like dual root of trust in PowerEdge servers, and extending across the data center with Unity XT storage, VxRail HCI, and data protection appliances.
- Trusted data—data security built into HCI, storage, and purpose-built backup appliances, as well as device-level security such as Dell SafeGuard and Response, offering a comprehensive approach to endpoint threat management.

To learn more about our complete range of end-to-end security solutions for medium businesses, talk to a Dell Technologies security expert.

Visit www.DellTechnologies.com/SMB/Security.