How Intrinsic Security Protects Against Business Disruption

DELL Technologies

vmware

Table of Contents

Acknowledging Business Disruption

When it comes to IT, disruption is just another day at the office. From fending off cyberattacks to incorporating leading-edge technologies, today's organizations no longer experience "business as usual."

However, even a department built on disruption may not have been prepared for everything the world has recently gone through. Almost overnight, organizations big and small had to enact work-and-learn-from-home policies, rethink their business continuity strategies and reinvent their operational models to keep their business running. These organizations turned to their IT teams to make it all happen.

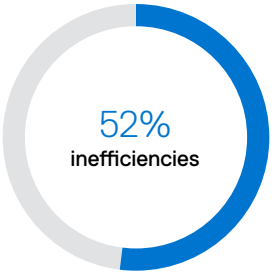
Millions of employees are now working remotely who weren't before. With their desktop PCs still stuck at the office in some cases, employees may also be using their home devices to connect to the corporate network and get work done. Even as the "new normal" is established, many of these workers and their businesses will prefer the flexibility of working from anywhere moving forward.

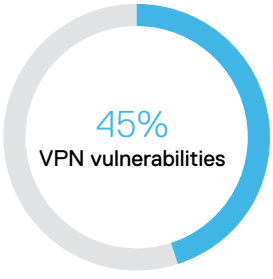
But with employees away from the watchful eye of IT, security will take on even greater importance. In 2020, organizations saw an increase in cyberattacks seeking to take advantage of unsuspecting employees working on unprotected personal devices, with ransomware attacks increasing 148% in March 2020 compared to February 2020.[1] Because IT teams were unprepared for the rush of employees working from home, their ability to protect the business was compromised, with IT professionals pointing to remote access inefficiencies (52%), VPN vulnerabilities (45%) and staff shortages (36%) as their greatest endpoint security challenges in managing cyberattacks.[2]

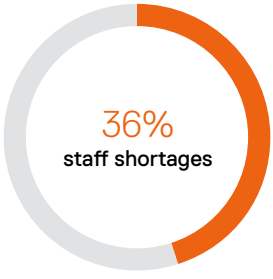
In a world where seven million data records are already compromised each day, security in a work-from-anywhere-world has never been more critical.[3] But if the current approach to security isn't working, what will?

CYBERATTACKS BY THE NUMBERS

148%
overall increase in ransomware attacks in March 2020







Intrinsic Security: A New Approach to Enhancing Security

Historically, cybersecurity is added after the fact to protect hardware and software already in place. But it's neither scalable nor manageable to keep adding layers and layers of security onto existing technology. This is especially true as trends like remote working, bring your own device, cloud, artificial intelligence, 5G, and the Internet of Things expand the number of potential data vulnerabilities across every facet of the organization.

The challenges of today and tomorrow's cybersecurity requirements can't be met using yesterday's thinking. A holistic, built-in approach that is intelligent and automated is required to quickly adapt to whatever unexpected changes come your way. Dell Technologies calls this approach "intrinsic security."

Intrinsic security isn't a tool or product: It's a strategy for incorporating security into the foundational level of your technology—below the operating system level—so that security is the first step in building your infrastructure, not the last. Intrinsic security factors in users, IDs, devices, assets and data in real time across any app or cloud so that you can identify risk and prevent threats at the scale of today's digital operations.

By driving security deeper into your organization's technology solutions, an intrinsic security approach allows you to be proactive instead of reactive when managing your company's cybersecurity needs.

The Principles of Intrinsic Security

An intrinsic approach to security is made up of three core principles:

Built-in

An intrinsic security approach builds security controls directly into the infrastructure, allowing business units to quickly scale without putting security requirements last.

Unified

Intrinsic security removes silos between IT and security teams by allowing both teams to use the same products and tools. This increases collaboration, empowers scarce security resources to be used more effectively, and ensures a more cohesive response to new vulnerabilities and active threats.

Contextual

Intrinsic security provides the context you need to understand both the threats you're facing and the endpoints, workloads, networks and clouds you're protecting. This context lets you intelligently prevent and respond to new threats to your most important assets so you can make smarter judgments about how to secure your environment.

How Dell Technologies Incorporates an Intrinsic Security Approach

The need for intrinsic security is at the root of how Dell Technologies manufactures, designs and delivers our products.

It starts with secure supply chain assurance. If a malicious actor tampers with components, embeds malware or inserts coding vulnerabilities into firmware during the manufacturing process, it creates underlying security vulnerabilities that are undetectable until it's too late. That's why Dell Technologies' manufacturing process includes multiple layers of controls to mitigate any risks that could be introduced into the supply chain, with tamper-evident seals providing assurance the device arrives in an untampered state. From secure factories to logistics and shipment security programs, Dell Technologies' secure supply chain program meets the highest standards for supply chain integrity.

In addition, Dell Technologies products are engineered using secure development lifecycle measures to make security an integral part of the overall design process. Proactive security testing throughout development reduces the opportunity for malware or vulnerabilities to be inserted into the software, while security engineers are embedded into Dell Technologies' product design process to ensure solutions are designed from the ground up to deliver intrinsic security.

As a hardware manufacturer, Dell Technologies is able to leverage a unique position in the infrastructure ecosystem to build in advanced security features that can't be replicated by software. For example, targeted attacks against a PC basic input/output system (BIOS) can allow hackers to compromise all of a device's endpoint security capabilities. Dell Technologies' solutions help you protect your BIOS by using silicon-based security and cryptographic root of trust to authenticate server booting and firmware updates, ensuring the BIOS can't be changed or tampered with. In addition, off-host verification provides confidence that systems haven't been compromised, while flexible reimaging options allow you to analyze any corrupted BIOS to better understand and prevent the attack.

Another example is Dell SafeID, which helps protect secure your operations by isolating user credential data away from the operating system and memory. Instead, all storage and processing of credential data take place on a dedicated security chip. This unique, hardware-based security solution hardens end-user credentials such as passwords, biometric templates and security codes, preventing attackers from stealing user credentials that would give them broad access to the network.

Using Dell Technologies Solutions to Deliver Intrinsic Security

Dell Technologies solutions incorporate advanced security features and, especially in partnership with VMware, those solutions can be leveraged to enhance your overall security posture across the business. Here are just a handful of examples:

Dell EMC Networking Solutions

The Dell EMC networking portfolio makes it even easier to meet the demands of modern workloads with integrated hardware and software solutions for virtualized networking functionality. For example, PowerSwitch switches are designed to provide architectural agility to power software-designed data centers, while the Dell EMC SD-WAN Solution powered by VMware combines purpose-built networking appliances with leading SD-WAN software for a simple yet powerful all-in-one solution. Together, Dell Technologies hardware and software can provide increased business flexibility, greater productivity through automation and reduced complexity for IT teams.

VMware Carbon Black Cloud

As a cloud-native endpoint management platform, VMware Carbon Black Cloud uses behavioral analysis to proactively detect threats and uncover attacker behavior patterns. VMware Carbon Black Cloud analyzes more than one trillion security events across the Dell Technologies customer base per day, allowing you to identify and isolate compromised users, endpoints and apps before an attack has the opportunity to spread throughout your network.

VMware NSX

With the ability to provide micro-segmentation, IT teams can use VMware NSX to deliver granular protection to the individual workload. This approach allows you to apply specific firewall rules to specific workloads, instead of running all rules against all traffic, making your approach to security more efficient. It also lets you secure east-west traffic to protect against the lateral movement of malware while eliminating visibility and security blind spots. This network virtualization platform is used by organizations to connect applications across data centers, multi-cloud, bare metal and container infrastructure.

Dell EMC PowerEdge Server Portfolio

PowerEdge servers provide high performance for a diverse set of workloads from the edge of the cloud to the core. In addition to using a hardware root of trust based in silicon to validate BIOS firmware, these servers automate many of the routine manual tasks that can result in configuration errors and security vulnerabilities. Embedded intelligent automation throughout the server lifecycle provides a deep layer of security, helping IT teams scale with speed and confidence.

VMware Workspace One

Dell Technologies' intelligence-driven digital workspace platform integrates access control, application management and multi-platform management into a single platform. This gives IT complete visibility while consolidating management silos to create and deliver consistent processes and policies, along with real-time, over-the-air management across devices and operating systems. With continuous verification of users, device and apps, Workspace One helps make zero-trust access a reality.

Dell Technologies Unified Workspace

This portfolio of solutions makes it simple to securely deploy, manage and support PCs no matter where employees work. Applications can be provisioned with VMware Workspace One at the factory, ensuring devices are shipped directly to remote employees with all required security protocols in place. When scaling remote workforces, Unified Workspace can help IT make sure employees work with trusted devices at home without spending time and labor unboxing, provisioning and shipping out devices.

Dell Trusted Devices for Endpoint Security

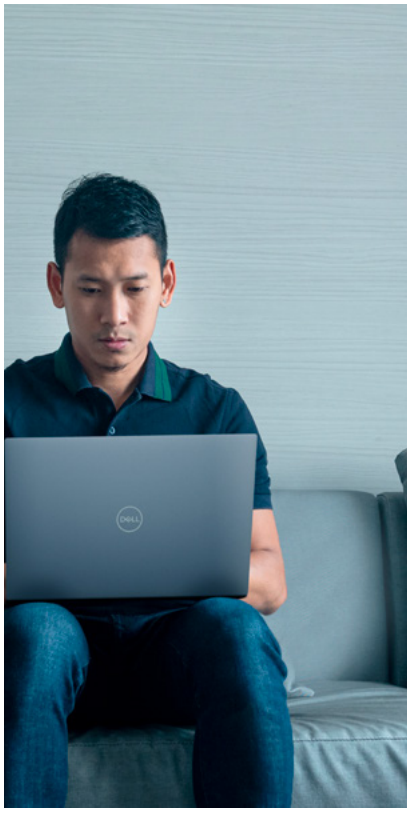
Dell Technologies' comprehensive approach to endpoint security offers built-in security and threat management to deliver the industry's most secure commercial PC by:[4]

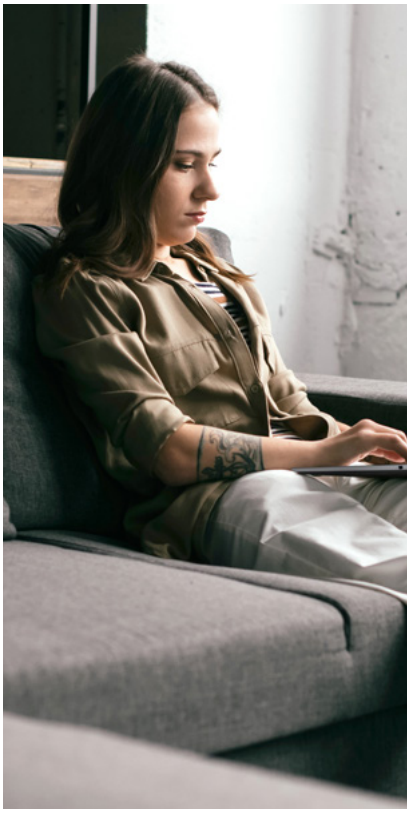
- Proactively detecting and blocking endpoint attacks, while providing security experts to hunt and remediate threats access the endpoint, network and cloud
- Enabling users to safely collaborate by encrypting sensitive data on endpoint devices while securing information in the cloud
- Providing off-host BIOS verification to mitigate the risk of BIOS tampering on endpoints
- Protecting against malware attacks using an exclusive security chip to isolate user authentication credentials away from potential attackers

Take Security to the Next Level

With an intrinsic security approach, you can put security where it needs to be: at the foundation of your business. Dell Technologies can help you leverage your infrastructure to help turn your devices, apps and users from points of vulnerability to points of protection.

Learn how Dell Technologies enables a digital workplace to help employees work and learn from anywhere.





Sources

[1] Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted, Jim Treinen, VMware Carbon Black, April 15, 2020.

[2] Global Incident Response Threat Report, VMWare Carbon Black, August 2020.

[3] The World in Data Breaches, Varonis, 2020.

[4] Based on Dell Technologies analysis, January 2020.