White paper

# Thrive with the Confidence of Cyber Resilience

Start strong, stay strong and outmaneuver security threats

## Security transformation enables digital transformation

In our data-driven world of seemingly unlimited opportunities — and unprecedented challenges — digital transformation can empower you to handle anything that comes your way. Building a nimble, modern IT environment that can rapidly respond to emerging business demands and customer expectations is your key to thriving in the digital economy.

However, there's something else you need to thrive in the digital era. Because even as you're reaching for new heights, cybercriminals are increasing the sophistication of their attacks, and exploiting every opportunity to steal, destroy or ransom your valuable data.

To win in the digital economy, you need to instill confidence in your customers and other stakeholders by keeping valuable data secure. You also need to maintain compliance with evolving global data security standards and regulations. And you need to do it all seamlessly and behind-the-scenes, without negatively impacting the business or your customers.

This level of cyber resilience requires security transformation. Because there is no digital transformation without a strong, secure foundation to build upon.

> To win in the digital economy, you need to instill confidence in your customers and other stakeholders by keeping valuable data secure.


© 2020 Dell Inc. or its subsidiaries.

# Table of Contents

Security transformation enables digital transformation ..... 1

Winning against a deluge of security threats ..... 3

The Dell Technologies point of view ..... 4

Giving you the confidence of strong security and data protection ..... 4

Start strong ..... 5

End-to-end intrinsic security ..... 5

Stay strong ..... 7

Innovations to bolster your cyber resilience ..... 7

Outmaneuver threats ..... 8

Achieve next-level mitigation through automation and intelligence ..... 8

The Dell Technologies difference ..... 10

Dell Technologies Customer Solution Centers ..... 10

Flexible payment and consumption solutions ..... 10

Services ..... 10

Confidently source your IT needs from a trusted provider ..... 11

Thrive with the confidence of cyber resilience ..... 11

Learn more ..... 11


© 2020 Dell Inc. or its subsidiaries.

**Risks by the numbers**

**64%**

of consumers would blame your company — not the hacker — for the loss of their personal data.[6]

**3.5 billion**

personal data records were stolen in just the top two data breaches of the last decade.[1]

**$13 million dollars**

is the cost of an average data breach.[4]

**63% of companies**

have already experienced data compromise due to an exploited vulnerability.[8]

## Winning against a deluge of security threats

The statistics around data security are daunting. The top two data breaches since the year 2000 resulted in the theft of 3.5 billion personal data records.[1] More recently, the devastating NotPetya cyberattack paralyzed multiple global enterprises by combining a ransomware attack with a wiper software that destroyed data and applications. The attack cost many of its highest profile victims hundreds of millions of dollars each in remediation and related expenses.[2] And every second, 158 more accounts are hacked.[3] What's more, the average cost of a breach is US $13 million,[4] with damages from cybercrime worldwide expected to reach US $6 trillion by 2021.[5]

If you can't stay ahead of these security threats, you risk squandering any lead that digital transformation brings — potentially damaging your reputation and losing your customers' loyalty — because the damage is more than just the immediate financial fallout. In a recent survey, 64% of Americans said that they would blame an enterprise for the loss of their personal data in an attack — not the hacker.[6] On the other hand, 84% of consumers said they are more loyal to companies they perceive as having strong security controls.[7]

But outmaneuvering cybercriminals is easier said than done. Industry analysts report that 63% of companies have already experienced data compromise due to an exploited vulnerability in hardware- or silicon-level security.[8]

It's clear that "business as usual" security can't keep pace with cybercriminals and regulatory demands.

[1] CSO, The 15 biggest data breaches of the 21st century, April 2020.

[2] The Wall Street Journal, One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs, June 2018.

[3] Review 42, 35 Outrageous Hacking Statistics & Predictions, September 2020.

[4] Accenture, Ninth Annual Cost of Cybercrime Study, March 2019.

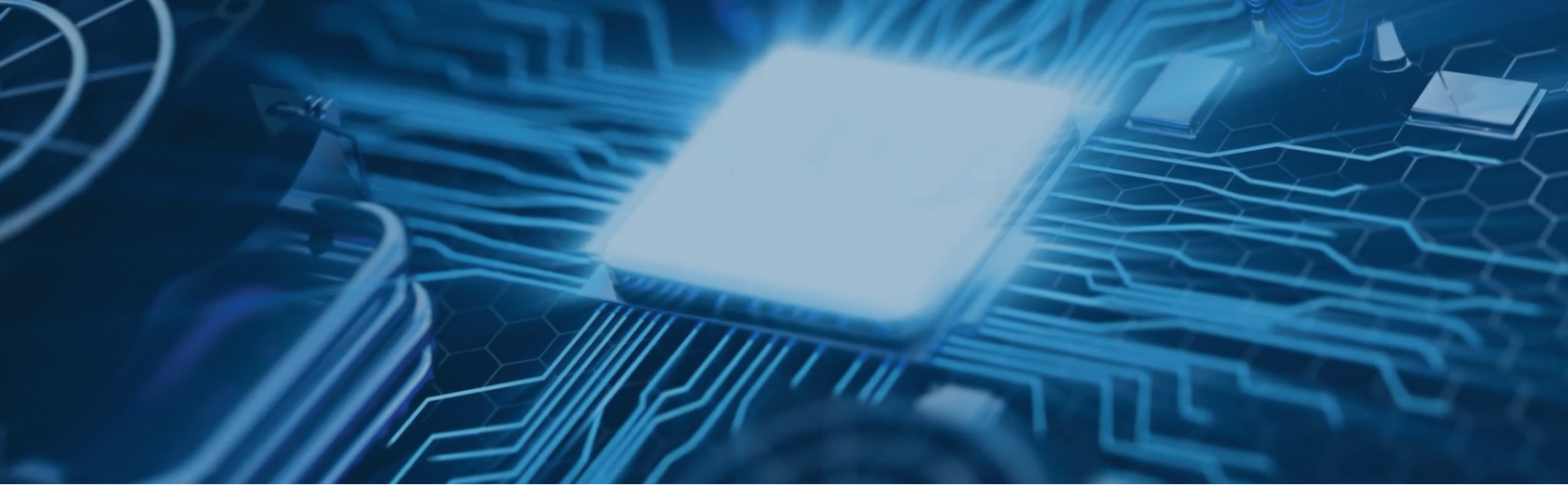
[5] National Law Review, Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion, February 2020.

[6] Forbes, 50 Stats Showing Why Companies Need To Prioritize Consumer Privacy, June 2020.

[7] SalesForce Research Report, State of the Connected Customer: Third Edition, June 2019.

[8] Forrester Consulting Thought Leadership Paper Commissioned by Dell, BIOS Security – The Next Frontier for Endpoint Protection, June 2019.


© 2020 Dell Inc. or its subsidiaries.



## The Dell Technologies point of view

### Giving you the confidence of strong security and data protection

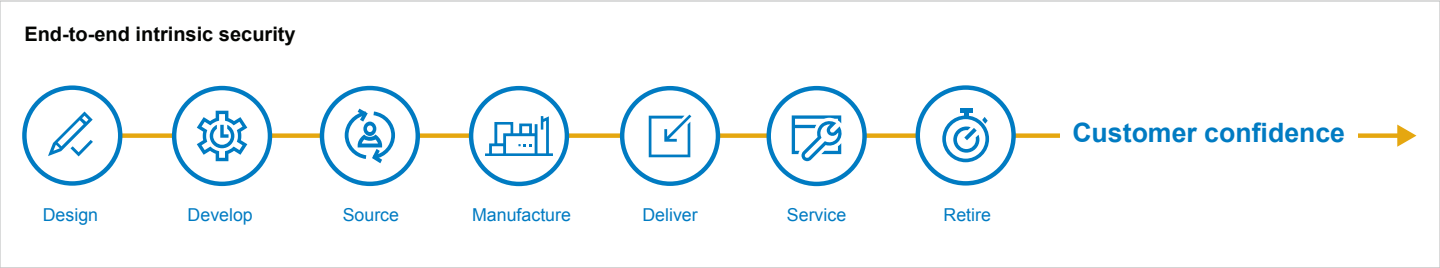
Pervasive protection, continuous security innovations, and intelligence and automation should work together across your entire data estate to create a strong security posture that helps you thrive with the confidence of cyber resilience. Dell Technologies gives you the confidence to accelerate your digital transformation, with security solutions that build in cyber resilience with continuing innovation and the automation and intelligence to do it efficiently and at scale. We call this built-in security “intrinsic security.”

By building your digital transformation on a secure foundation from Dell Technologies, you can:

- **Start strong** with built-in protection through a complete portfolio of solutions from the silicon and supply chain all the way to asset retirement — all from a single, trusted vendor.
- **Stay strong** with continuous innovations designed to build and bolster cyber resilience in the face of intensifying threats.
- **Outmaneuver threats** by mitigating risks through automation and intelligence — to stay a step ahead of cyberthreats.

> Dell EMC PowerEdge servers are made with a cyber resilient architecture that builds in security at every phase of the product lifecycle, from the silicon root of trust, to signed firmware and drift detection, to BIOS recovery.


© 2020 Dell Inc. or its subsidiaries.




# Start strong

## End-to-end intrinsic security

To successfully fend off increasingly sophisticated attacks, you need security that's built in, not bolted on. That's why Dell Technologies makes security an intrinsic element of our devices, services and operational models.

You also need security that covers your business from end to end. That's where you can leverage the large family of Dell Technologies companies to help you operate seamlessly across your data centers and clouds — on-premises, off-premises and at the edge.

For example, Dell EMC PowerEdge servers are made with a cyber resilient architecture that builds in security at every phase of the product lifecycle, from the silicon root of trust, to signed firmware and drift detection, to BIOS recovery. This same level of enterprise security focus can be seen across our enterprise portfolio, including storage, networking and data protection. Security rigor is infused throughout the Dell Technologies family of brands and through our client products, which include some of these features:

- **SafeBIOS** mitigates the risk of BIOS tampering with integrated firmware attack detection through Dell Technologies–exclusive off-host BIOS verification, BIOS Image Capture, and BIOS Events and Indicators of Attack.
- **Safe ID** enables device access with a fingerprint or card scan, freeing users from complex passwords. Only Dell Technologies secures user credentials in a dedicated security chip, keeping them hidden from malware.
- **VMware® NSX®**, a network virtualization product, allows for enhanced and seamless security capabilities such as micro-segmentation.

Intrinsic security starts within our secure supply chain. Dell Technologies takes a holistic and comprehensive approach to protect our supply chain and deliver solutions you can trust. We've mapped the most impactful supply chain attack vectors — such as counterfeit components, malware, and firmware tampering — and have invested heavily to harden our processes and practices against both physical and digital threats.

We have implemented cutting edge programs across the full spectrum of supply chain risk, from our threat-informed product designs, to training our tens of thousands of developers on secure development practices, to securing our factories, to logistics and shipment security programs, all the way through to post-delivery support and services. Our secure supply chain program aligns to — and in some cases exceeds — worldwide best practices and standards, and we continue to add security protocols and get better every day.


© 2020 Dell Inc. or its subsidiaries.

Dell Technologies takes a holistic and comprehensive approach to protect our supply chain and deliver solutions you can trust.

For example, the newly announced Dell Technologies Secured Component Verification for Dell EMC PowerEdge servers makes us the first server vendor with a cross-portfolio solution for cryptographically verified hardware integrity.[9] This new capability enables you to verify that servers from the Dell Technologies factory arrive without hardware component compromise. When the system is ready for shipment, the server components and their unique IDs are assessed, and the resulting data is cryptographically secured using a signed certificate. The encrypted inventory is embedded in the server. Once you receive the server, you can use the associated tool provided to authenticate that the inventory with the certificate is stored on the system.

To start strong on the commercial side, Dell SafeSupply Chain adds supply chain security to the industry's most secure commercial PCs.[10] The new services include:

- **SafeSupply Chain Tamper-Evident Services** verify nothing happens to the device during transport. These tamper-evident seals are added to the device and the box at the factory, prior to shipping. Pallet seals can also be added to increase security.
- **SafeSupply Chain Data Sanitization Services** prevent spyware or illicit agents from being injected into the hard drive. This is done through NIST-compliant hard drive wipe, guaranteeing a clean slate to imaging.

These new services are offered on top of the Dell Secure Development Lifecycle and standard supply chain security measures, which include:

- Unique identification labels to identify and track individual components.
- Hash verification applied on the BIOS prior to shipping to confirm the authenticity of the device.
- Preventative and detective control measures that protect physical assets, inventory and information.

Throughout the technology lifecycle, Dell Technologies Services help maintain vital data security, reducing the risk of unauthorized access to sensitive information and helping you align to the latest standards and regulations. For example, Data Sanitization for Enterprise and Data Destruction for Enterprise Services align to NIST 800-88 standards, helping you maintain compliance and security as you retire and refresh assets that have reached their end of life. And our Keep Your Hard Drive (KYHD) and Keep Your Component (KYC) for Enterprise Services allow you to maintain possession of failed drives and components while still getting the parts replaced so that sensitive data never leaves your control, maintaining security as well as enabling compliance with data privacy regulations.

[9] Based on Dell analysis of publicly available data, October 2020. Available on PowerEdge 14G and 15G, except for PowerEdge XE7100, XE7420, XE7220, C6420 and C6525.

[10] Based on Dell internal analysis, January 2020.


© 2020 Dell Inc. or its subsidiaries.

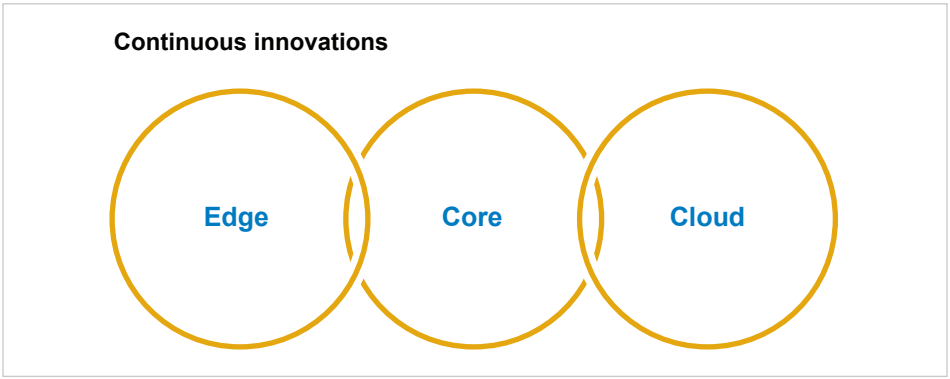
Dell EMC PowerEdge servers and Dell Precision Workstations were featured in the National Security Agency (NSA) UEFI Secure Boot Customization paper for securing the server boot process and maintaining high security status for server infrastructure.[12]

## Stay strong

### Innovations to bolster your cyber resilience

Once you have built strong security and data protection best practices into your entire data estate and throughout the IT lifecycle, it's time to take steps to continue to stay ahead of cybercriminals. Dell Technologies enables you to stay strong with a steady stream of innovations that build on your secure foundation and continue to bolster your resilience in the face of continuous and intensifying threats.

For example, Dell EMC PowerEdge servers strengthen infrastructure resilience and protect against boot-related exploits with the new PowerEdge UEFI Secure Boot Customization capability. In addition, Dell Technologies is currently the only server vendor to eliminate the need for third-party certificate authorities, providing organizations complete ownership of their certificates and boot security.[11] This reduces the risk of industry-wide boot vulnerabilities, such as GRUB2. In fact, Dell EMC PowerEdge servers and Dell Precision Workstations were featured in the National Security Agency (NSA) UEFI Secure Boot Customization paper for securing the server boot process and maintaining high security status for server infrastructure.[12]



Dell Technologies is always on the cutting edge of technology, and that includes innovations designed to help you comply with rapidly evolving cybersecurity standards and regulations. For example, Dell Technologies was the first solution provider to join the Sheltered Harbor Alliance Partner Program[13] and the first solution provider to offer a fully-endorsed Sheltered Harbor turnkey data vaulting solution. This is seamlessly integrated as an option within our Dell EMC PowerProtect Cyber Recovery solution, a market leader with an almost five-year history of protecting critical data from cyberattacks. Cyber Recovery for Sheltered Harbor is a fast, cost-effective and efficient means for forward-thinking financial services organizations to protect critical financial data by adopting the Sheltered Harbor standard.

[11] Based on Dell analysis of publicly available data, October 2020. Feature available on PowerEdge 14G and newer. Requires customer certificate(s).

[12] The Dell EMC PowerEdge R640 server, Dell EMC PowerEdge R740 server, Dell EMC OptiPlex 7050 workstation, Dell OptiPlex 9020 workstation and Dell Precision 7710 workstation were featured in the paper. National Security Agency Cybersecurity Technical Report, UEFI Secure Boot Customization, September 2020.

[13] Dell Technologies solution brief, PowerProtect Cyber Recovery for Sheltered Harbor, 2020.


© 2020 Dell Inc. or its subsidiaries.

In addition to the Dell EMC PowerProtect Cyber Recovery technology, it's critical to operationalize a strategy that is purpose built for your business's specific recovery requirements. After a destructive cyberattack, many of the most critical business applications may be down, so it's crucial to prioritize the recovery of those applications to get the business back up and running. Dell Technologies Business Resiliency Services help customers align business needs with resiliency and recovery preparations to reduce planned and unplanned downtime. Our expert consultants focus on developing strategies in three major areas of business resiliency: enabling recovery from cyberattacks, optimizing data protection infrastructure and operations, and ensuring business application availability requirements are met.

Compliance with NIST standards and guidelines is also a top priority for many organizations. These standards for recommended security controls encompass best practices controls across a range of industries and are endorsed by the U.S. government. Dell Technologies builds in innovations that help you meet and exceed NIST standards. For example, our new Data Sanitization for Enterprise and Data Destruction for Enterprise Services align to these standards, supplying you with Certificates of Sanitization that satisfy compliance needs in alignment to US NIST 800-88.

Extensive use of intelligence and automation makes it easier for you to mitigate risks more efficiently, stay ahead of rapidly evolving threats, and scale to meet the demands of ever-expanding usage models.

## Outmaneuver threats

### Achieve next-level mitigation through automation and intelligence

In addition to built-in security and continuing innovations that help you start strong and stay strong, Dell Technologies makes extensive use of intelligence and automation, taking data security to the next level. The Dell Technologies difference makes it easier for you to mitigate risks more efficiently, stay ahead of rapidly evolving threats, and scale to meet the demands of ever-expanding usage models.

An example of this is the integrated Dell Remote Access Controller (iDRAC). It delivers secure, advanced, agent-free local and remote server administration to automate a multitude of management tasks. iDRAC provides a complete set of automated and secure server management features at your fingertips. For example, Dell Technologies is the only server vendor to offer the ability to dynamically enable and disable system lockdown once your server is provisioned and in production without having to reboot.[14] System lockdown helps protect the system from unintentional or malicious changes during configuration and firmware updates.

With the latest iDRAC security release, we take this a step further, enabling you to seamlessly lock a NIC to prevent changes to the firmware from the operating system (OS) and any resident malware. With this release we also introduce two-factor authentication (2FA) and RSA SecurID® support to further verify user authentication. The iDRAC also now enables remote attestation technology to cryptographically confirm the identity of bare-metal servers, and for identity-based provisioning for zero-trust environments.

In addition to automation, you can also leverage telemetry from iDRAC. The iDRAC sends real-time data for over 5,000 different server measurements — from CPU utilization to power consumption to network utilization — to analytics tools such as Splunk®. While the vastness of the available server data is compelling, the value lies in analyzing and learning from the data of all the systems that make up the server infrastructure.

[14] Based on Dell analysis of publicly available data, October 2020


© 2020 Dell Inc. or its subsidiaries.

You can also use iDRAC with OpenManage Ansible Modules to automate security workflows such as system lockdown, user privileges, data storage encryption, secure enterprise key manager (SEKM), firmware configuration and updates, and certificate management. The latest release also enables managing certificates via industry-standard Redfish RESTful APIs. Secure erase can be automated as well, avoiding the need to write individual manual scripts, which saves time and further mitigates threats.

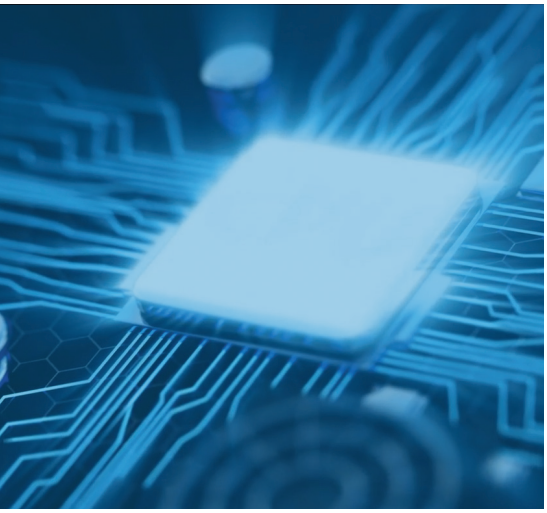
Dell Endpoint Security SafeGuard and Response, powered by VMware Carbon Black and Secureworks®, is designed to detect, prevent and respond to the full spectrum of modern cyberattacks with the least amount of administrative effort. It applies artificial intelligence (AI) and machine learning (ML) to streaming telemetry data to proactively detect and block endpoint attacks.

CyberSense, which is an integral feature in our PowerProtect Cyber Recovery solution, adds another layer of protection to real-time security solutions by using analytics to detect signs of corruption — such as mass deletions, encryption and other types of changes in files and databases — that can result from undetected attacks. Its innovative approach uses ML to analyze over 100 content-based statistics and finds corruption with up to 99.5% confidence,[14] helping you protect your data and recover quickly to avoid business interruption.

SupportAssist integrates data protection and threat prevention into a secure, automated support experience. The SupportAssist security architecture continuously monitors your devices and applies sophisticated AI models, including ML, to detect issues and initiate accelerated resolution.


© 2020 Dell Inc. or its subsidiaries.

Customer Solution Centers help reduce the risks associated with new technology investments and can help improve speed and ease of implementation.



## The Dell Technologies difference

### Dell Technologies Customer Solution Centers

Our global network of dedicated Dell Technologies Customer Solution Centers are trusted environments where world-class IT experts collaborate with you to share best practices, facilitate in-depth discussions of effective business strategies and help you become more successful and competitive. Customer Solution Centers help reduce the risks associated with new technology investments and can help improve speed and ease of implementation.

### Flexible payment and consumption solutions

Dell Technologies gives you more choice, flexibility and predictability in how you consume IT infrastructure. Flexible payment and consumption solutions enable immediate IT acquisition with the ability to pay over time. Pay-as-you-go solutions allow you to manage cash flow and plan for future upgrades while staying on budget. Pay-as-you-use solutions allow you to align costs with usage and maximize business agility. Dell Technologies offers a wide range of payment and consumption solutions to make it easier than ever to meetyour needs.

### Services

From design and implementation to support and systems management, Dell Technologies offers a comprehensive services portfolio. Dell Technologies partners with you every step of the way, linking people, processes and technology to accelerate innovation and enable optimal business outcomes, including protection of your data, business and reputation.

- Education Services offers training and certifications in security and data protection. From self-paced, on-demand courses to virtual, instructor-led options, both the Security and Data Protection tracks provide training and skills validation on the latest techniques for cybersecurity frameworks from Dell Technologies, VMware, NIST and more.
- Managed Services can provide security operations as part of a range of IT infrastructure management. Our team of experts has a vast range of experience protecting IT infrastructures from the data center to the cloud, ensuring systems are safe, secure and compliant.
- Services technology offerings include a secure automated support experience engineered to head off threat incursions and protect data integrity, and an online data analytics dashboard which integrates advisory remediation management for security advisories to speed risk evaluation and enable remediation tracking at scale.


© 2020 Dell Inc. or its subsidiaries.

## Learn more

**Storage and data protection**
- Dell EMC Power Protect Cyber Recovery — Sheltered Harbor Endorsement

**Server**
- Dell Technologies Secured Component Verification
- Dell EMC PowerEdge UEFI Secure Boot Customization

**Systems management**
- iDRAC
- Dell EMC OpenManage Ansible Modules

**Client**
- Dell SafeSupply Chain

**Services**
- Dell Technologies Keep Your Hard Drive for Enterprise / Keep Your Component for Enterprise
- Dell Technologies Data Sanitization for Enterprise / Data Destruction for Enterprise

## Confidently source your IT needs from a trusted provider

Dell technologies holds leadership positions across a wide array of IT solutions, so you can confidently source your needs from one, trusted provider. Dell Technologies is:

- #1 in servers[15]
- #1 in storage[16]
- #1 in cloud IT infrastructure[17]
- #1 in data protection appliances and software[18]
- #1 in converged and hyper-converged infrastructure[19]

See Dell Technologies Key Facts for more.

## Thrive with the confidence of cyber resilience

With security transformation that includes built-in protection, continuous innovation and intelligence, and automation, you gain the confidence of cyber resilience so you can advance your digital transformation goals and thrive in the data era.

[15] IDC Vendor Revenue, "WW Quarterly Server Tracker," September 2020.

[16] IDC Vendor Revenue, "WW Quarterly Enterprise Storage Systems Tracker," September 2020.

[17] IDC Vendor Revenue, "WW Quarterly Cloud IT Infrastructure Tracker," September 2020.

[18] Based on combined revenue from the IDC 3Q19 Purpose-Built Backup Appliance (PBBA) Tracker, with select Storage Software segments from the 3Q19 Storage Software and Cloud Services Overview.

[19] IDC Vendor Revenue, "WW Quarterly Converged Systems Tracker," September 2020.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. VMware® products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware® is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. Splunk® is a registered trademark of Splunk Inc. in the United States and other countries. Secureworks® is a registered trademark of SecureWorks, Inc. RSA® and RSA SecurID® are registered trademarks of RSA Security LLC. Other trademarks may be the property of their respective owners.
Published in the USA 12/20 White paper SECURITY-POV-101.

Dell Technologies believes the information in this document is accurate as of its publication date.
The information is subject to change without notice.

DELL Technologies