

# Protect and Preserve Your Data from Endpoint to Infrastructure

Achieve cyber resilience with help from the powerhouse partnership between Dell Technologies and VMware<sup>®</sup>

# Table of Contents

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

Recovering from a breach is just as important as preventing a breach

## Dell Technologies and VMware provide ..... 5 simplified, comprehensive cyber resilience

For most organizations, cybersecurity is complex and confusing, but it doesn't have to be

## Learn more ..... 8

Technology has made it possible for the world to maintain a somewhat business-as-usual stance, even when world-changing events occur. The technological solutions that enable modern scenarios such as distributed workforces are evolving at a breathtaking pace. The future of technology has never been more promising.

But every silver lining must have its cloud. For organizations that rely upon information technology — virtually every organization on the planet — that cloud is cybercrime. Nearly three-quarters of organizations believe that having a more distributed workforce has resulted in increased exposure to cyber threats.<sup>1</sup>

The perception of increased risk is grounded in reality. As the global pandemic has changed the way we use technology to work, cybercriminals have exploited the security gaps that have been exposed. In 2020, for example, more data records were stolen than during the prior 15 years combined.<sup>2</sup>

To make matters worse, many organizations don't feel as though they have a good handle on protecting themselves from cybercrime. In fact, 62% of IT decision-makers believe that their organization may not be sufficiently protected against threats such as malware and ransomware.<sup>3</sup>

Achieving your organization's goals in this new landscape requires a modernized approach to security and cyber protection. Cybersecurity leaders Dell Technologies and VMware are at the forefront of this effort, working together to deliver industry-leading security solutions designed to protect your organization from endpoint to infrastructure.

<sup>1</sup> "Global Data Protection Index 2021: Key Findings," Dell Technologies, July 2021, <https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/global-data-protection-index-key-findings.pdf>

<sup>2</sup> Misha Glenny, "Pandemic accelerates growth in cybercrime," Financial Times, April 27, 2021, <https://www.ft.com/content/49b81b4e-367a-4be1-b7d6-166230abc398>

<sup>3</sup> Ibid

# Nearly 75%

of organizations believe that having a more distributed workforce has resulted in increased exposure to cyber threats

# In 2020

more data records were stolen than during the prior **15 years combined**

# 62% of IT decision-makers

believe that their organization may not be sufficiently protected against threats

# The Dell Technologies point of view

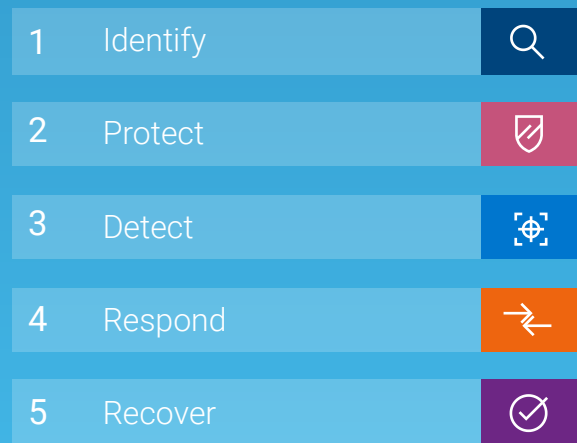
Recovering from a breach is just as important as preventing a breach

Data is the essential resource of our global economy. But unlike protecting a physical resource, such as currency or diamonds, data requires a far more comprehensive protection plan than simply hiding it from would-be thieves. While it's important to defend against unauthorized access to your data, it's just as critical that your data be preserved if a breach occurs.

Unlike gold or other tangible valuables, your data provides value to your organization even after a breach. Gold or jewels, once stolen, often are gone. After a cyber event occurs, your data can remain accessible, its value to your organization intact, and your organization's reputation preserved – but only if your cyber security strategy includes a comprehensive approach to security, data protection, and recovery: a cyber resilience approach.

Cyber resilience is the ability to maintain business continuity despite cyberattacks. It encompasses the real-world view that, despite your best efforts, breaches may occur. And when that happens, your organization must be able to quickly recover lost or compromised data, restore system functionality and resume business activities.

Cyber resilience incorporates people, processes, and technology in protecting your entire organization. An evolving concept, cyber resilience is founded on the NIST Cybersecurity Framework, which has five components:<sup>4</sup>



# 65%

of IT decision-makers lack confidence in their organization's ability to recover data and systems after a cyber incident.<sup>5</sup>

<sup>4</sup> "You may have heard about the NIST Cybersecurity Framework, but what exactly is it?" Federal Trade Commission, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework>

<sup>5</sup> "Global Data Protection Index 2021"

# Dell Technologies and VMware provide simplified, comprehensive cyber resilience

For most organizations, cybersecurity is complex and confusing, but it doesn't have to be

Today's organizations spend lots of money and juggle a plethora of different security solution providers. Many find that the complexity of managing multiple security vendors with individual products can undermine their efforts, potentially providing cyber criminals with gaps to exploit.

But cybersecurity doesn't have to be difficult. And it doesn't have to be pieced together from different service providers. Instead, you can achieve end-to-end cybersecurity and cyber resilience from a single source: the seamless partnership between Dell Technologies and VMware, two of the most trusted names in information technology.

The ability to achieve complete cybersecurity from a single partnership is of more importance than many IT decision-makers may realize. For starters, you can save money and simplify implementation and operation when you use a suite of solutions that were built to work together – seamlessly and securely. Surveys also indicate that organizations with multiple security vendors are more likely to have experienced data loss, data access issues or system downtime than those using a single vendor.<sup>6</sup>

**The volume of breached data records increased by**

**141% in 2020<sup>7</sup>**

<sup>6</sup> Ibid.

<sup>7</sup> Lance Whitney, "2020 sees huge increase in records exposed in data breaches," TechRepublic, January 21, 2021, <https://www.techrepublic.com/article/2020-sees-huge-increase-in-records-exposed-in-data-breaches/>

Dell and VMware have a longstanding, collaborative partnership that builds on each company's industry-leading expertise and technology. The partnership offers leading solutions for modernizing and maximizing cybersecurity protection and recovery from cyber incidents.



### Dell EMC PowerProtect Cyber Recovery

This offering assures recoverability by isolating critical data from threats like ransomware. An operational air gap and machine learning/analytics monitor data integrity to accelerate recovery from ransomware or other attacks that penetrate the data center.



### Dell Trusted Devices Endpoint Security

Seventy percent of security breaches originate at the endpoint.<sup>8</sup> Powered in part by VMware Carbon Black, Dell Trusted Devices prevent, detect and remediate attacks, keeping endpoints secure regardless of their geographic location.



### VMware security solutions

In addition to Carbon Black endpoint security, VMware offers workload and DevOps security, network security and cloud security solutions.



### VMware NSX Network Virtualization Platform

A full-stack network virtualization platform, this simple, integrated software firewall from VMware features network segmentation and micro-segmentation to the individual workload.



### Dell Supply Chain Security

Supply chain cyberattacks nearly doubled in the first quarter of 2021.<sup>9</sup> Dell assures supply chain integrity by using an integrated process to assure that technology deliveries are authentic and uncorrupted.



### Dell Technologies Managed Detection and Response

Cybersecurity detection and response managed by Dell leverages the experience of Dell security experts in containing and resolving known threats, identifying new threats, and rapidly initiating recovery steps in the event of a breach.

<sup>8</sup> "Endpoint Security Tools Eventually Fail, Says Report," Security, June 17, 2019, <https://www.securitymagazine.com/articles/90388-endpoint-security-tools-eventually-fail-says-a-report>

<sup>9</sup> Charlie Hart, "'Troubling' rise in supply chain cyber attacks," CIPS, April 13, 2021, <https://www.cips.org/supply-management/news/2021/april/troubling-rise-in-supply-chain-cyber-attacks/>



Nearly two in three organizations believe that their data protection measures may not defend them against escalating malware and ransomware threats.<sup>10</sup> Together, Dell Technologies and VMware address this gap with comprehensive cybersecurity protection and data recovery capability. This approach to combat destructive threats like ransomware is easier, more manageable, cost-effective, and far more effective than any solution cobbled together from a jumble of different security providers.

Don't leave your organization's data up for grabs to the first successful hacker or ransomware attack. Explore how Dell Technologies and VMware can secure your data across edge, core, and multicloud environments to ensure that you can recover your critical data and resume normal operations with confidence after an attack.

<sup>10</sup>"Global Data Protection Index 2021"

# Learn more about Dell Technologies security solutions.

[Learn more](#)

## About Dell Technologies

Dell Technologies (NYSE:DELL) 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.



## About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact.



Copyright © 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. ServiceNow® is a trademark and/or registered trademark of ServiceNow, Inc., in the United States and/or other countries. Microsoft® is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. VMware® and the VMware taglines, logos and product names are trademarks or registered trademarks of VMware in the U.S. and other countries. Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell Technologies believes the information in this document is accurate as of its publication date. The information is subject to change without notice. H18999