DELL Technologies

Innovation Built-in intel

Cyber security and business resilience

Creating strong businesses through cyber resilience

Threats and opportunities

More than half of all businesses now see cyber attacks as their number one digital risk. No matter how seriously you treat the dangers, it's a matter of "when" rather than "if" a cyber attack will impact your business.

Businesses must evolve to stay ahead of increasingly complex threats to their systems and data. Cyber criminals are more expert than ever; they understand that the traditional IT perimeter is blurring as the workforce becomes more mobile and third-party vendor relationships multiply.

Approaches to cyber security must be granular and pervasive, but transparent to the end user. "Business as usual" will not keep pace with today's threat environment or technology-driven business initiatives.

Businesses need to move from cyber security policies to cyber resilience.

From erecting barriers that prevent incidents, and detecting them when they occur, cyber resilience benefits businesses across four key areas.

1. Swiftly responding to incidents..
2. Notifying the relevant authorities.
3. Implementing disaster recovery and business continuity plans.
4. How to learn from the experience, to minimise the risk of recurrence and to maximise the effectiveness of the response and recovery effort.

$133.7 billion

Worldwide spending on cyber security is forecast to reach $133.7 billion in 2022. (Gartner)

144,000 complaints filed

In the first year of GDPR, there were 144,000 complaints filed with various GDPR enforcement agencies and 89,000 data breaches recorded. (EDPB)

Business leaders feel risks are increasing

68% of business leaders feel their cyber security risks are increasing. (Accenture)

Breaches—what tactics are utilised?

52% of breaches featured **Hacking**

33% included **social attacks**

28% involved **Malware**

Errors were causal events in **21%** of breaches

15% were **Misuse by authorised users**

Physical actions were present in **4%** of breaches

External actors and their entry points

Advanced threat actors such as nation-states, cyber criminals and cyber espionage actors represent the greatest information security threat to enterprises today.

Detecting these clandestine threats can be difficult due to their resource sophistication, and their deliberate "low and slow" approach. Enterprises need insight beyond their network borders to counter-act advanced threats specifically targeting their organisations and infrastructure.

- 52% of breaches featured hacking,
- 28% involved malware and
- 32–33% included phishing or social engineering, respectively. (Verizon)

Types of cyber attack

Malware

Malware refers to the practice of deploying malicious software, including ransomware, spyware, viruses and worms to infect and breach a network.

This can result in blocked access to files and systems, criminals covertly obtaining sensitive information, and disruption to service, amongst others.

Data Integrity

Malicious data manipulation can be detrimental to a business. This is a highly sophisticated, and easily undetectable cyber attack that causes users to doubt the accuracy of their information. Manipulating public opinion through smear campaigns or changing information in a medical system are two examples of how this type of attack poses a huge threat to society.

SQL Injection

Deploying malicious code into an SQL-based server can force the server into revealing information it wouldn't normally reveal. This type of attack can allow attackers to tamper with services enabling them to pose as other individuals, void transaction, change data, destroy data and approve administrative access to users.

Distributed Denial of Service

This type of attack uses multiple compromised systems to attack servers, networks, and systems to flood and exhaust resources forcing the network to fail and deny service to legitimate users.

Snooping

Similar to the act of eavesdropping, snooping is the practice of unauthorised access to systems and data. This can include monitoring of keystrokes, passwords, login information, communications, webcams, etc.

Cyber Collection

Used by nation states to conduct espionage and even corporate spies to gather intelligence on rivals, cyber collection is similar to snooping but is with the intention to scan, collect and extricate sensitive information. An example of this is the famous Stuxnet computer worm first uncovered in 2010.

What are the cyber attackers' motives?

Financial
71% of breaches are financially motivated

State Sponsored
Governments have quickly realised that cyber attacks are quicker, cheaper and easier than traditional warfare methods

Intelligence Gathering
Cyber criminals use the practice of scanning, monitoring, collecting, and exfiltrating sensitive information in order to extort, blackmail or gain advantage over a rival business

Hacktivism
The use of computers and computer networks to promote political or social change

Terrorism
Politically motivated extremist groups and non-state actors using computers to cause harm or fear pose a mayor threat to critical infrastructure

TYPES OF THREATS

Internal threats from a transforming workforce

A transforming workforce

The workforce is undergoing profound changes sparked by globalisation, shifting demographics and digital transformation. Bring-Your-Own-Device, Software-as-a-Service solutions, mobile apps and gig workers make for a dynamic working environment, but create complex challenges for the CISO and CIO. More employees accessing data from more devices mean more digital identities to protect.

What happens when identities are compromised?

Today, 2.2 billion compromised usernames and passwords from high-profile breaches are available on the dark web. These can later be manipulated for credential stuffing attacks which, in 2018, were behind more than 30 billion login attempts – and this threat will continue to grow.

For security leaders and CIOs, this means transforming workforces must be met with a modern authentication and risk management strategy.

300 billion passwords
By 2020, the estimated number of passwords used by humans and machines worldwide will grow to 300 billion. (Cybersecurity Media)

Over 1000 sensitive files
53% of companies had over 1,000 sensitive files open to every employee. (Varonis)

+27% working from home
The UK's Trade Union Congress (TUC) estimated in 2019 that there were 373,000 more employees working from home than 10 years previously, a 27% increase, bringing the total to 1.7 million. (TUC)

34% of data breaches involved internal employees
(Verizon)

Protecting mobile end-points

The increasing use of mobile devices, and the growing reliance on mobile endpoints that allow employees to work from anywhere, are forcing a greater focus on endpoint security, with a focus on two key areas:

Protecting data
Ensuring GDPR compliance

Preventing threats
Guarding against cyber attacks

A TRANSFORMING WORKFORCE

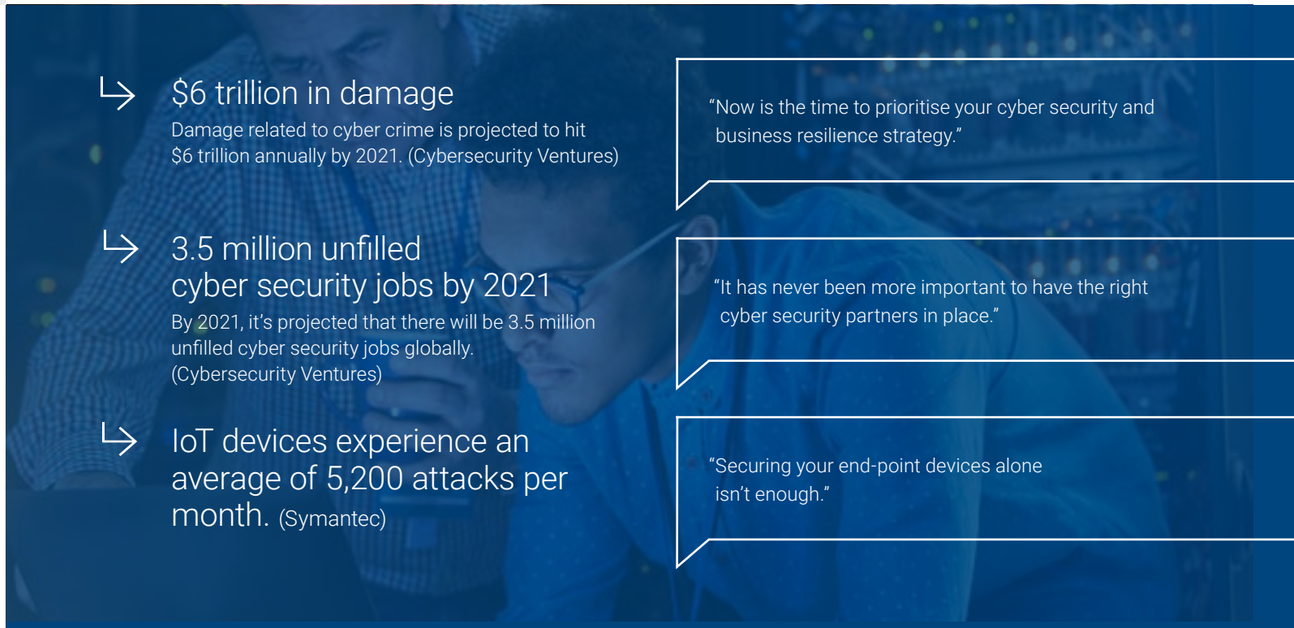
The Dell Technologies response

When you buy Dell Technologies, you buy security. It's in our DNA.

We can protect and secure your data throughout its entire lifecycle, from inception to archive.

A growing reliance on data within digital businesses means that data security must be everyone's responsibility – from the mailroom to boardroom. This requires a new top-down culture of managing digital risk with security controls that are pervasive yet not obstructive, allowing everyone to become enablers and accelerators to innovation, rather than simply just barriers.

Dell Technologies empowers you to move further faster. By providing intrinsically secure infrastructure platforms and devices, we enable you to generate and process vast amounts of data at the core, edge and in the cloud. All while giving you the peace of mind that your IT assets are secure, protected and available.



$6 trillion in damage
Damage related to cyber crime is projected to hit $6 trillion annually by 2021. (Cybersecurity Ventures)

3.5 million unfilled cyber security jobs by 2021
By 2021, it's projected that there will be 3.5 million unfilled cyber security jobs globally. (Cybersecurity Ventures)

IoT devices experience an average of 5,200 attacks per month. (Symantec)

"Now is the time to prioritise your cyber security and business resilience strategy."

"It has never been more important to have the right cyber security partners in place."

"Securing your end-point devices alone isn't enough."

A unified workplace and security

Security is key to workplace productivity. Unified Workspace solutions from Dell Technologies comprise trusted devices, trusted access and trusted data. With security built in, they are major productivity and innovation enablers – empowering your employees to work anywhere, anytime – without compromise.

Trusted devices

Dell builds unique security into every commercial device to ensure a secure foundation for all your users

Trusted access

Together with VMware Workspace ONE and VMware Carbon Black, Dell protects users with trusted access – constantly monitoring and validating devices, users, networks, and applications.

Trusted Data

Our comprehensive threat management portfolio combines prevention, detection, and response. Our end-point security and Unified Workspace offerings also include SafeData and our SafeGuard and Response solution, which enable your workforce to work anywhere without the need to lock down data.

PERSONAS

Cyber security in the workplace

C-Suite

C-suite users are key in influencing and delivering transformative IT solutions for their entire organisation. They need to know that their technology is strong enough to combat increasing digital threats whilst empowering their workforce.

Mary is the Chief Information Security Officer at a leading retail bank.

She faces a steadily rising tide of threats; from malware, web-based and denial of service attacks to ransomware and highly sophisticated fraud attempts.

As well as defending against sophisticated cyber criminals, Mary must also ensure the business can respond and recover fast, in the event of an inevitable breach. She must do all this while complying with stringent data protection regulations. Dell Technologies enables her to build capabilities and resilience in these key areas.

As a global leader in cyber security services directly, and through subsidiaries like Pivotal and VMware, Dell Technologies helps Mary protect her company's critical assets. All while complying with regulations and strengthening her operational resilience.

Mary must also adapt to an increase in remote working, which is demanding more efforts in managing mobile devices, applications and access permissions. With VMware Workspace ONE, her IT administrators can deliver, manage and secure employees' remote access to corporate applications and cloud-hosted virtual desktops from their mobile devices.

IT security should not be a collection of siloed activities. Dell Technologies helps Mary build a joined-up mechanism that provides real-time threat detection, keeping valuable assets safe. Mary is no longer just defensive, but an advocate of innovation.

Mark is Head of Operational Transformation at a leading bank.

So far, his transformation remit has covered IT infrastructure, digital banking, distribution channels and customer experience.

Mark needs a strong technology partner, as he must replace legacy systems with new technology in all areas of the business. All while never losing focus on the ultimate customer experience.

Dell Technologies has transformation at the heart of all its Fintech solutions, from big data management, data analytics, and artificial intelligence, through to cloud services and mobile banking. Our Fintech transformation covers three critical areas:

Cyber security: Dell Technologies helps Mark in Securing the Digital Enterprise. Our enhanced security spans the whole enterprise; the network, ATMs, PCs, mobile devices and all customer interactions.

Workforce Transformation: By adopting Dell Technologies solutions, such as augmented and virtual reality, video conferencing and webinars, Mark has empowered his staff and their working practices.

Leveraging New Technologies: Mark can access world class IT experts, through Dell EMC Customer Solution Centers. We have all the servers, storage, networking and data protection solutions Mark could possibly need for his transformation objectives.

End users

End users need reliable technology wherever they are. Increasingly, they are working remotely and rely on powerful technology to keep company data safe while they are on the move.

James is a Project Manager at a start-up.

He spends half of his time away from his desk, attending meetings out of the office, but still needs powerful technology and reliable connectivity to present content with clients while he is on the move.

On a coffee-shop stop between meetings, James misplaces his Dell Latitude 7000 Series Laptop. His immediate concern is for the sensitive data held on the device. Fortunately, with VMware Carbon Black Cloud Endpoint built into the laptop, all his critical data is protected with rock-solid, enterprise-class, datacentric encryption.

James informs his IT Manager about the loss of his laptop. They use the Dell Data Security Management Server to suspend user encryption keys and arrange a wipe of the hard drive. The device itself can be frozen as soon as it is reconnected to the Internet, avoiding a potential data breach.

Jane is Regional Sales Manager for a large-scale international enterprise listed on the FTSE Stock Exchange in London.

She is largely away from her desk, in and out of meetings. To keep herself mobile, Jane uses a range of PC technologies and accessories to stay productive and connected to 'office everywhere'.

Whilst travelling by train between meetings, Jane sends an email over an unprotected wireless network. Unknown to her, a hacker is using the network and intercepts the document. However, as the file is protected by Dell Full Safe, it is useless to the hacker.

Jane's IT Department have received an alert in real time, and instruct Jane to disconnect from the network, avoiding any further data breaches. Her company's Dell Full Safe security policy also blocks external recipients of confidential documents from copying, editing or printing. Jane had put a four-hour time expiry on the document, so she can relax secure in the knowledge that her information is safe.

VERTICAL IN FOCUS

Financial services

With pressure to change growing constantly, finance is at a turning point. Its institutions need to be more open, transparent and intelligent. Delivering tailored services securely and in real time.

At current rates of digital disruption, the World Bank predicts new players will capture 30% of global business revenue by 2025. From banking to insurance and asset management, this spans the entire financial services sector.

80% of banking CEOs are concerned by the speed of change. They need ways to rethink business models and innovate while maintaining high quality, safe and secure products and services for their customers.

819 cyber incidents in 2018

819 cyber incidents were reported to the UK's Financial Conduct Authority in 2018, a huge rise on the 69 incidents reported in 2017. (Data obtained by accountancy firm RSM under a Freedom of Information (FoI) request)

85 cyber attacks per year

A typical financial institution faces an average of 85 targeted cyber attacks every year, a third of which are successful. Source: Basel Committee on Banking Supervision

3 million customers' data copied

UniCredit, Italy's biggest bank, in October 2019 revealed that a file containing details of 3 million Italian customers had been illegally copied.

CASE STUDIES

Working with us

mastercard

Results

Protecting customer data with analytics

Global payments leader Mastercard wanted to use predictive analytics to study customer purchase patterns. It needed to analyse data from 2.2 billion payment cards globally, and up to 160 million transactions per hour. It also required the highest levels of security to protect this sensitive data. Mastercard worked with Dell Technologies companies to build a secure Payment Card Industry (PCI)-certified Hadoop cluster to create a data analytics capability. The solution has created business value from anonymised data in three key areas: share-of-wallet compared to competitors, average spend, and purchase frequency. It has also increased security and fraud protection because of the way it uses machine learning to analyse customer purchasing patterns, affinities and rhythms.

Business continuity plan
now only takes a few minutes instead of 3 months

Internal audit
time and costs reduced

DZ BANK

Results

Improving information security in the compliance function

DZ Bank, one of Germany's biggest banks, chose Dell Technologies to strengthen its governance, risk and compliance (GRC) capabilities. The bank wanted to improve the security of its compliance function. Previously, security was not centrally organised, creating silos and inconsistencies across the bank. The Dell Technologies RSA Archer solution provided a unified view of all security-related work for management and compliance. Dell Technologies equipped DZ Bank with an efficient, collaborative enterprise governance, risk and compliance (eGRC) programme across various functions, including policy, risk, compliance, enterprise, incident, vendor, threat, business continuity and audit management. The solution improved security and provided quicker reporting to the board and incident response teams.

PCI-certified
Hadoop cluster enables data analytics

Machine learning
helps increase security and fraud protection

74%
of customers say they would reconsider using a company if it could not keep their data safe

Large Latin American retail bank

Results

Sophisticated data analytics protects ATMs from fraudsters

A large retail bank in Latin America suffered a sophisticated attack on 2,000 of its ATMs in one weekend, with losses of more than $7 million. Dell Technologies worked with the bank to create a data analytics solution to protects its network of nearly 50,000 machines from future attacks. We integrated non-structured data from each ATM, overlaid it with structured data, created statistical models and used advanced analytics to embed predictive alerts into the bank's monitoring systems. The bank uses Dell Technologies' data platform, to which other data and analytics can be added for other uses, such as analysing video footage from branch surveillance cameras.

$10-$20m
annual reduction in fraud losses

50,000+
ATMs protected

INTEL

Intel solutions

To protect businesses and empower their employees, Dell Technologies partners with Intel to enable a comprehensive portfolio of solutions spanning edge, endpoint, data center, cloud, and network.

Intel Builds Security Into the Silicon

As cyber attacks move down through the layers of the system stack, software-only security is no longer sufficient.

To maintain a more secure computing environment, businesses should develop on a trusted foundational system layer: the silicon.

Intel's products are architected to deliver advanced security, with built-in, silicon-enabled security technologies that help protect potential attack surfaces. Rooted in silicon, their security technologies are meant to operate beyond the reach of potentially corrupted software. This helps create a trusted foundation for computing that customers can depend on.

Learn more about Intel built-in security solutions:

Intel vPro →

Intel Secure Device Onboard (Intel SDO) →

Security by design

Security is an ongoing priority, not a one-time event or project. Intel is committed to helping advance security and performance as the cornerstones of future architectures, by using world-class product development policies, processes, and tools. Their security design principles require designers, developers, coders, validators, and architects to proactively and consistently consider the security implications of design decisions and to build resilience into their products.

Learn more about the Intel security first pledge →

Learn more about Intel device security solutions →

Learn more about Intel cloud and enterprise security solutions →

DELL Technologies

Innovation Built-in intel

We listen. We collaborate. **We help you transform.**

Transform your business with a Virtual Executive Briefing about Security Transformation and Business Resilience

Our Virtual Executive Briefing Program

A Virtual Executive Briefing is a highly personalised experience; with a customised agenda designed completely around you - your needs, challenges, opportunities and goals.

We provide an environment to explore and develop strategies openly with Dell Technologies executives and subject-matter-experts, enabling a collaborative and strategic approach to your transformation.

Learn More About Our Executive Briefing Programme →