DELL Technologies

INDUSTRY SOLUTION BRIEF

DELL TECHNOLOGIES SECURE MANUFACTURING SOLUTIONS

# An intrinsic cyber resiliency approach to addressing security risks at all levels of the manufacturing IT and OT landscape

## The current state of security on the manufacturing floor

The factory floor is a crucial component of any manufacturing operation. It is where raw materials are transformed into finished products, and it is the beating heart of the manufacturing process. However, the factory floor, with a mix of IT and OT[1] systems, is also vulnerable to cyber threats.

Unlike modern IT systems, many OT systems are often not designed with security in mind. As a result, they are vulnerable to attacks that could disrupt or even shut down production. In fact, critical manufacturing was the most targeted sector for ransomware attacks in the first half of 2022,[2] and 55 percent of manufacturing and production organizations were hit by ransomware in 2021, up from 36 percent in 2020.[3]

[1]OT, or operational technology, includes industrial control systems (ICS)s, supervisory control and data acquisition (SCADA) systems, and other specialized equipment.

[2]Global Resilience Federation (GRF) Semiannual Ransomware Report for January to June 2022, https://bit.ly/3O9BYIW

[3]Sophos, https://bit.ly/3BvuGkX

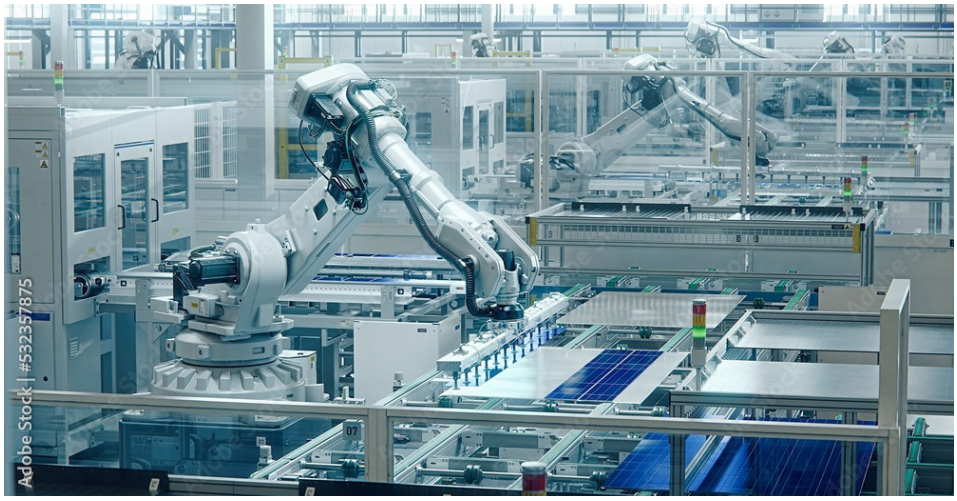
### COMMON MYTHS IN A FACTORY SETTING

- **The industrial area/asset is air gapped:** There is a false sense of security/safety in the idea that the assets are protected because they are not connected to the internet. In today's hyper-connected world, there are often not just one but many ways to access assets. And internal threats, such as a disgruntled worker breaching physical security or a well-meaning employee who applied an untested patch, can be as effective as an external attack.
- **A firewall is sufficient:** Traditionally, a firewall is located between the industrial area and the IT area. But as companies rely more and more on data-driven insights, they need to connect their industrial assets to their business systems. This data flow requires exceptions in the firewall, creating security holes that make the firewall less effective.
- **The current security plan covers us:** Cyber insurance companies are asking the important questions. Namely, are you doing the same due diligence on the OT side as you are on the IT side? If they are not, a manufacturer may be denied coverage or will have to pay a much higher premium because they can't demonstrate that they understand the risk to their industrial assets.

## Challenges in protecting OT

### SAFEGUARDING ASSETS REQUIRES A NEW APPROACH TO SECURITY

There is a great misconception that IT security is enough when in fact the landscape in manufacturing is quite different, requiring skill sets outside the domain of traditional IT. Understanding the mechanisms of a facility's OT assets is critical to helping to protect the data that is generated by these assets, as well as protecting the data that flows to/from them.




A top challenge is the lack of visibility into manufacturing/industrial assets. Many OT devices reside in a single enclosure, making it difficult to understand the extent of systems that are running and exposed to threats. For every IT device that's sitting in a manufacturing facility, there's usually a 15:1 or 20:1 ratio of industrial assets.

Additionally, passive listening tools are needed to identify OT assets and detect threats. Traditional IT applications use active scanning and do not understand industrial protocols. Without an understanding of how OT devices communicate and what is considered good versus bad behavior, an attack could be in motion and go undetected. In addition, using the wrong tools to attempt to identify industrial assets could break processes or the timing between multiple robots could be thrown off, which could have disastrous consequences.

Another challenge is lack of ownership. Who owns factory assets and the requirements to protect those assets? Consider a robot, for example. Is it an IT asset because it's connected to the network or an OT asset? And how is it best protected? OT security platforms are relatively new. Manufacturing security managers who drive an enterprise-wide strategy may not know that these tools exist or how they differ from the IT tools they're familiar with, resulting in a strategy that is either incomplete or likely to fail. If they incorporate OT tools into their plan, another concern is whether they have properly trained staff who can manage the volumes of data that are generated and draw appropriate enterprise-wide conclusions.

Ultimately, manufacturers might not realize the risks they face or their exposure.

## Pathway to securing OT

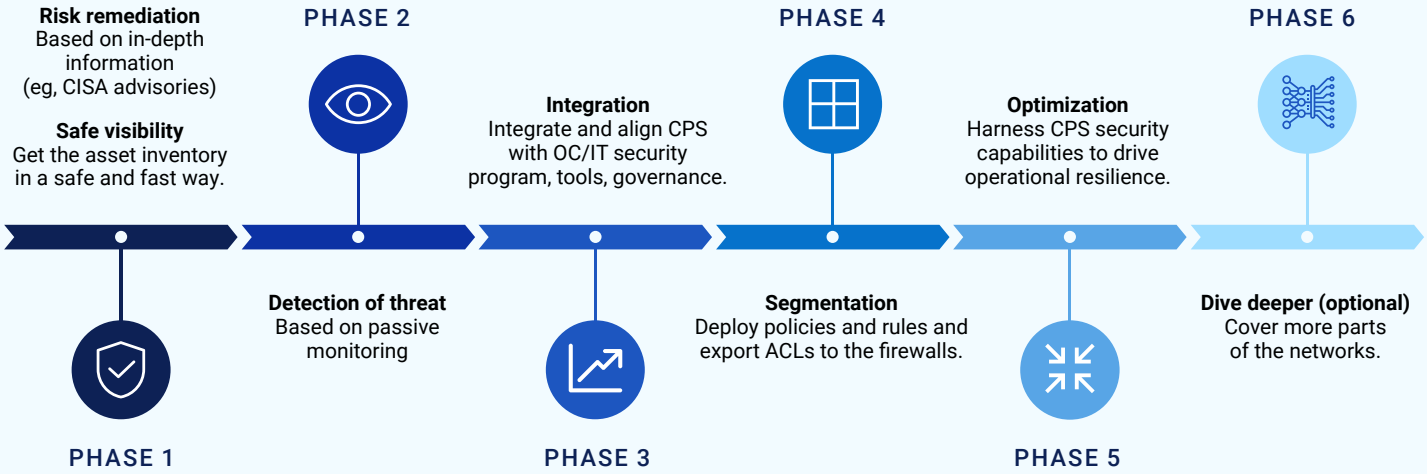
You can't protect what you can't see. Because enterprise security doesn't typically cover industrial security, it is essential to address OT security as part of any manufacturing cybersecurity strategy.

Building in OT cybersecurity requires protecting your primary areas of vulnerability and risk, which is your assets. Those assets may include industrial equipment, intellectual property, people and machine data (process integrity).

All connected devices, whether OT or IT, create a convergence of risks. Reducing the threat landscape and risks is about identifying risks, understanding the interoperability of devices with IT security controls, and protecting an organization's resiliency through threat detection and remediation of vulnerabilities.

Figure 1 shows an overall phased plan that manufacturers can follow to ensure they are addressing risks and building in security for OT and IT throughout the enterprise.

**Figure 1.** Steps on the digital safety journey




In Phase 1, it's important to gain visibility into your manufacturing assets—which can be visibility on the IT and OT side. Organizations need to understand what assets are out there, who's talking to who and ultimately what's being said. Then risk remediation is performed, based on data gathered from the manufacturing environment as well as security threat information from well-known sources such as CISA advisories.[4]

Phase 2 involves leveraging a passive monitoring platform to understand the behavior of assets connected to your network and whether there is a detection of a threat.

In Phase 3, you integrate and align data from cyber-physical systems (CPSs) with security operations center (SOC) and IT security programs, tools and governance.

Phase 4 involves segmenting the network and grouping devices logically, which are managed with firewall policies and rules, and access control lists (ACLs).

[4]Cybersecurity & Infrastructure Security Agency (CISA) advisories at https://www.cisa.gov/news-events/cybersecurity-advisories.

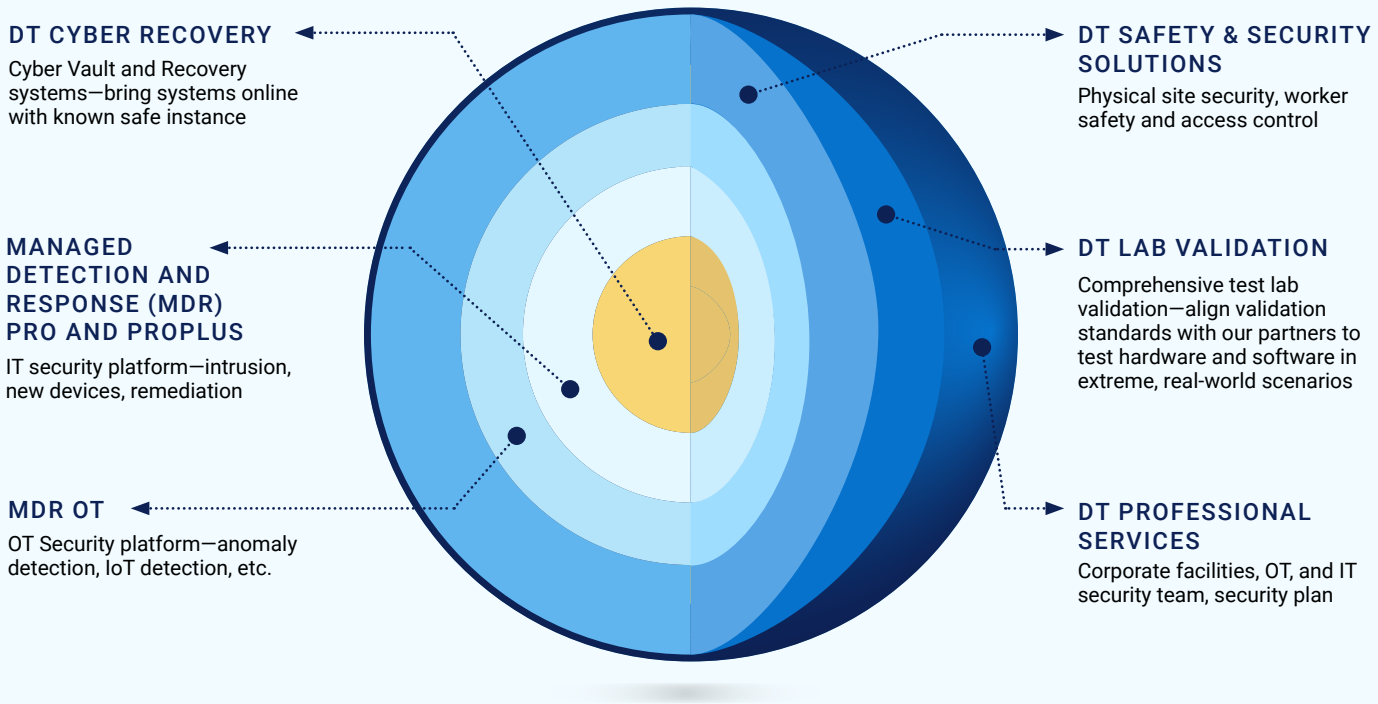
Organizations must ultimately operationalize all the data that's coming from the security tools and platforms in order to take a proactive stance to enterprise-wide security. Phases 5 and 6 are about optimization in driving operational resilience and diving deeper to cover a greater part of the network, respectively.

## Dell Technologies' holistic security approach for manufacturing

Distributed data, hybrid work models, multi-cloud environments and as-a-service sourcing are changing virtually everything about cybersecurity in manufacturing. Manufacturing requires a secure, scalable, industrial network with connectivity from anywhere to anywhere to meet Industry 4.0 initiatives and to work seamlessly with end-to-end supply chains.

Manufacturers need a trusted partner with a comprehensive security portfolio to help you confidently build and sustain cyber resiliency across IT and OT environments. It's imperative to fortify with modern security that is scalable, intelligent and holistic (Figure 2) to enable your organization to focus on driving production and improving business outcomes.

**Figure 2.** Dell Technologies' holistic approach to end-to-end security for Manufacturing




### DELL TECHNOLOGIES CYBER RECOVERY

PowerProtect Cyber Recovery is a cyber resiliency solution that isolates copies of applications and data in an air-gapped secure data vault, enabling recovery of known-good files to recover and resume normal operations after a ransomware or cyberattack.

## IT AND OT SECURITY PLATFORMS

With Dell Technologies Managed Detection and Response (MDR) Pro Plus, manufacturing organizations can continuously monitor IT and OT networks to help prevent threat actors from probing, exploiting and damaging their environment. In the event of an attack, our fully-managed, 360° security operations solution helps you respond and recover. Our experts work with internal security teams to steadily improve an organization's security posture and continuously stay prepared. The MDR Pro Plus solution includes MDR, vulnerability management, pen testing and attack simulation management, managed security awareness training, and incident recovery care.

## DELL TECHNOLOGIES SAFETY AND SECURITY SOLUTIONS

Our Safety and Security solutions encompass Dell Technologies physical and computer vision solutions that combine validated workloads for video analytics, safety and security, converged and hyperconverged infrastructure (CI/HCI), and partner-supplied appliances in a scalable architecture.

## DELL TECHNOLOGIES LAB VALIDATION

Validated designs are engineered purpose-built architectures designed for Dell Technologies hardware on the manufacturing floor. Each validated design is customized to meet the specific needs of each manufacturer.

At the foundation of this multifaceted approach is a secure supply chain process. Equipment used in the supply chain, such as desktops, laptops, servers, and data storage arrays, is designed, deployed, maintained and validated with security as a top priority.

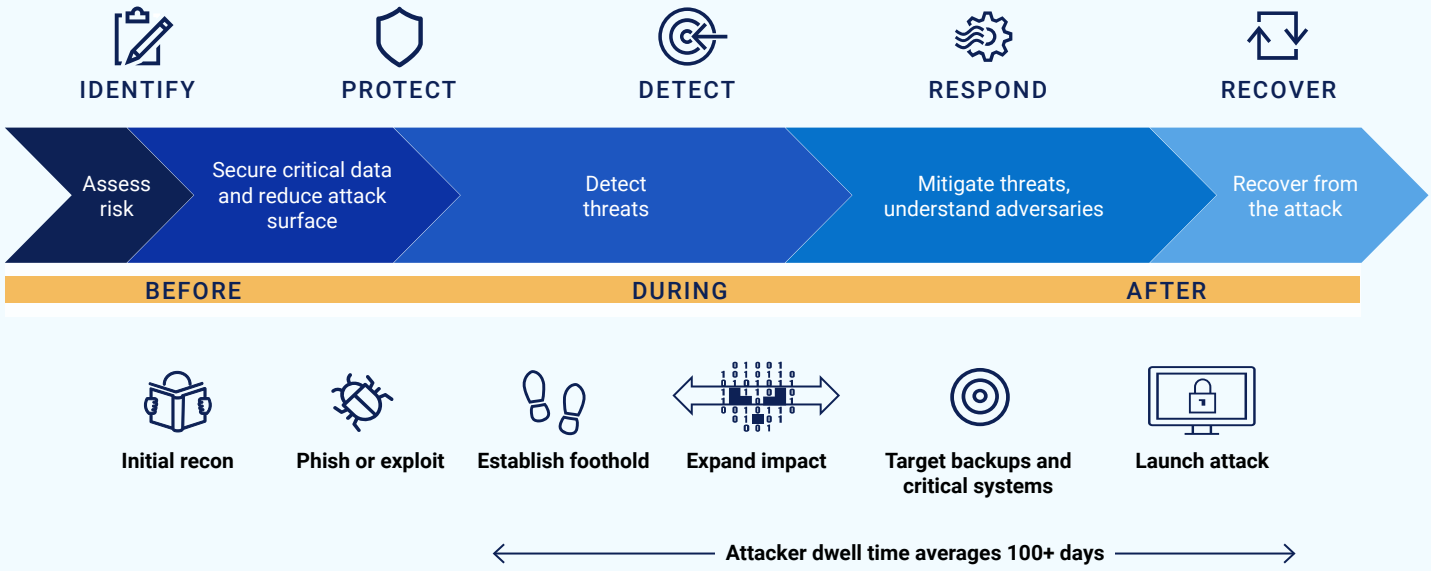
## DELL TECHNOLOGIES PROFESSIONAL SERVICES

Dell Technologies Professional Services provides assistance with planning, implementation and operations. This process drives mature cybersecurity programs that are aligned to key business/manufacturing processes, including advisory services for OT and IT teams, implementation and custom design of security plans.

## Achieving a cyber resiliency strategy

Dell Technologies' security approach enables you to implement a cyber resiliency strategy (Figure 3). While cyber criminals' tactics may vary, they use fairly predictable approaches for introducing and carrying out attacks. Resiliency is first about understanding, then protecting against, how attacks are carried out, so that no matter how the attack is structured, it can be identified and arrested before it has fully manifested. Should an attack successfully breach defenses, a resilient environment is able to recover quickly and efficiently.

**Figure 3.** Resiliency before, during and after an attack

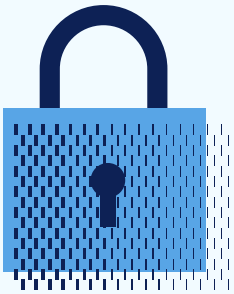



### BEFORE AN ATTACK: PLANNING AND IMPLEMENTATION

When a customer initially engages with Dell Technologies, we take a consultative approach to the architectural design and planning process. Through client interviews/workshops, and as-is and to-be security assessments, the design is created with validated Dell Technologies hardware and software solutions right-sized to the environment.

Once an OT security solution is put in place, securing operation technology involves several processes, including asset discovery, vulnerability management, risk awareness/management, continuous monitoring, and ongoing employee security awareness training.

The asset discovery process listens to the factory floor for devices and builds an architectural baseline from an IT and OT perspective. At the core of OT security is continuous monitoring, in which the system constantly monitors OT networks, identifying and prioritizing risks and vulnerabilities as well as detecting potential threats in real time. Unlike ordinary IT tools, an OT security platform understands hundreds of protocols used by OT systems and, through deep-packet inspection, can detect unusual behavior within communications between those protocols.



**DETECTION AND RESPONSE FROM DELL ENABLES MANUFACTURERS TO:**

- Check device vulnerability.
- Perform penetration testing.
- Determine if a network can be accessed through OT devices.
- Monitor for threats.
- If any anomalies or threats are detected, respond effectively and perform remediation

Because the OT security platform is installed on the factory floor, data is collected and analyzed locally, at the edge. This system works in tandem with computer vision, which relies on cameras located throughout a manufacturing facility, ingesting video that is then analyzed, turned into valuable insights and used for real-time decision making. Computer vision insights generally affect five key outcomes: personnel and facility safety and security, operational efficiencies, "people" experiences, sustainability and revenue generation.

Employees can be the weakest link in organizational cybersecurity, with negligence and lack of awareness accounting for nearly 50 percent of cyberattacks.[5] With Dell Managed Security Awareness Training, employees on the shop floor gain customized security training to help inform and make security awareness top of mind for them, reducing an organization's chance of a cyberattack.

## DURING AN ATTACK: DETECTION AND RESPONSE

Responding to modern IT threats takes the latest approaches that bring together the tools and a team of experts to better identify, respond and mitigate threats in real time. Dell Technologies' detection and response security services help customers extend their constrained resources and reduce complexity.

Our solution is part technology and part managed service, bringing the right combination of incident response tools and experts. The incident response service is SaaS-based. It is continuously updated with data on the latest threats and proactively protects against complex cyberattacks across endpoints, the network and the cloud, giving administrators a comprehensive view of an attacker's end-to-end activity. As an integrated component on the computer vision platform used in manufacturing environments, it has been tested at scale on the Dell validated design solution implemented at a customer site. The technology is backed by Dell's team of certified security experts who use the latest AI-based capabilities to strengthen the customers' security posture, helping them confidently address the most pressing threats.

## AFTER AN ATTACK: CYBER RECOVERY

Ransomware and other attacks are becoming more sophisticated, and no security technology is ironclad. In the event of a security incident, especially if high-value assets have been compromised, Dell Technologies helps you initiate the process to recover from the event and get your organization back up and running. We also have intrinsic capabilities in production such as immutability and multi-factor authentication to help secure a customer's environment.

Our cyber recovery solution includes regularly scheduled synchronization of applications and data to an air-gapped vault. Command and control of the vault is maintained from within the vault autonomously. That is, the process to get information into the vault is initiated autonomously from inside the vault via the software. The vault has three requirements that are critical to cyber recovery:

- **Isolation:** The contents of the vault are physically and logically isolated from the rest of the network.
- **Immutability:** All data written to the vault must be "locked"; no deletions or changes are allowed until the locking period expires.

[5]Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2018). Insider threat: The human element of cyberrisk. Retrieved November 15, 2022, from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/insider-threat-the-human-element-of-cyberrisk


- **Intelligence:** Full content analytics performed on vault contents determine the last known good copy (the level at which only Dell Technologies currently provides). The analytics feature also performs integrity checks by analyzing data in the vault to ensure it's free from manipulation or corruption.

Once a customer has a locked copy of data and applications in the vault and has performed analytics on the contents, they can work on the maturity of their recovery strategy. Should recovery be necessary and a customer doesn't have the required skill set, Dell Technologies can provide an incident response service to get boots on the ground within hours.

## A closer look at Validated Designs

Dell Technologies aligns validation standards with our partners to test hardware and software in extreme, real-world scenarios. Validated designs are created by our team of experts, who have years of experience in manufacturing cybersecurity.

We design and validate the architecture for each customer's unique factory floor, end to end, ensuring that a customer's assets work with Dell hardware. This type of baseline design typically takes months for a customer to determine on their own through proofs of concept.

Validated designs can help manufacturers create a robust and secure end-to-end architecture that protects both their IT and OT systems, reduces vulnerability risk and reduces time to implementation. This architecture can include measures such as firewalls, intrusion detection systems and other security controls.

All validated designs are created using Dell Technologies products, which are built on the secure supply chain process. Dell Technologies supply chain assurance program implements safeguards that enable zero trust across the physical, personnel and cybersecurity realms to ensure a resilient manufacturing and delivery process.

### KEY OUTCOMES FROM DELL PROCONSULT ADVISORY SERVICES

- Transition from legacy to best-in-class IT operations
- Target IT investments towards greater business needs
- Leverage IT agility to generate and deploy innovative solutions
- Provide guidance for day-to-day operational demands and long-term strategic planning
- Deliver a plan for transitioning from your as-is to your to-be state

Dell Technologies' architectures address OT cybersecurity by following the Purdue model, a framework developed by Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) for securing OT systems. Additionally, validated designs can help manufacturers comply with industry standards and regulations, such as the NIST Cybersecurity Framework and the ISO/IEC 27001 standard.

## Dell Technologies and partner professional services

Dell Technologies and partner professional services for secure manufacturing for planning, implementation and operations include Dell Secure Manufacturing Services and Dell Technologies Security Analysts.

We work with companies leading and driving manufacturing innovations to bring you the best IT and OT security solutions.

Whether it's running a production application critical to your business, expanding a new system seamlessly or quickly, or bringing the right data together at the right time for delivering business insights, Dell Technologies and our valued partners are ready to work toward a secure solution.

## Are you doing the same due diligence on your OT/industrial side as you are on your IT side? If not, Dell Technologies can help.

Dell Technologies is a leading IT company, specializing in manufacturing cybersecurity. With a focus on both IT and OT security, we are dedicated to helping manufacturers protect their operations from cyber threats.

We have engineers with OT experience that are specifically dedicated to edge technologies, helping customers design a cyber resilient architecture and be confident in their ability to recover from a disruptive cyber event. It's critical that organizations are proactively implementing technologies, which are supported by tested and documented recovery programs, to form a last line of defense for the business.

We are one of the few companies creating a story that encompasses truly enterprise-wide cyber strategies. Some companies do a fantastic job in the industrial/manufacturing space. Other companies do a fantastic job in the IT space or in the security space. Dell Technologies can connect the dots for all of that across the enterprise.

Learn more at **Dell.com/security**