DELL Technologies

intel

OEM Solutions

Designing Solutions On Zero Trust Architectures And Cyber Resilience Strategies

Introduction

Your customers rely on you, as a solution builder, to help protect their data from cyber attacks, withstand such attacks when they occur and—when necessary—recover their data and operations after cyber attacks. The threat landscape is ever-changing. By some estimates, the frequency of cyber-attacks is increasing 50 percent year-over-year.[1] That's why you need to supply your customers with products and systems that include high levels of layered security and cyber resilience.

It all starts with selecting your technology provider. Dell Technologies is a supplier you can rely on for your cyber resilient technology infrastructure. Dell Technologies supports Zero Trust principles, which state that because cyber threats are present everywhere, measures must be taken throughout the technology life cycle.

Cyber resilience at Dell Technologies is not created by a single product or during a single phase of the development process. Rather, it results from a strategy of layered security that spans all Dell products and permeates all stages of the product design and development process.

Dell Technologies creates a modern cyber resilient architecture that supports Zero Trust and is based on the NIST Cybersecurity Framework (CSF), as shown in Figure 1.

Cyber Resilience:

The ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources.

— National Institute of Standards and Technology (NIST) glossary[2]

Zero Trust:

A cybersecurity model that shifts how organizations approach security from reliance solely on perimeter defenses to a proactive strategy that allows only known good activity across ecosystems and data pipelines. It allows organizations to better align their cybersecurity strategies across the data center, clouds and at the edge. Dell Technologies aims to serve as a catalyst for customers to achieve Zero Trust outcomes by making the design and integration of this architecture easier.

— Dell Technologies

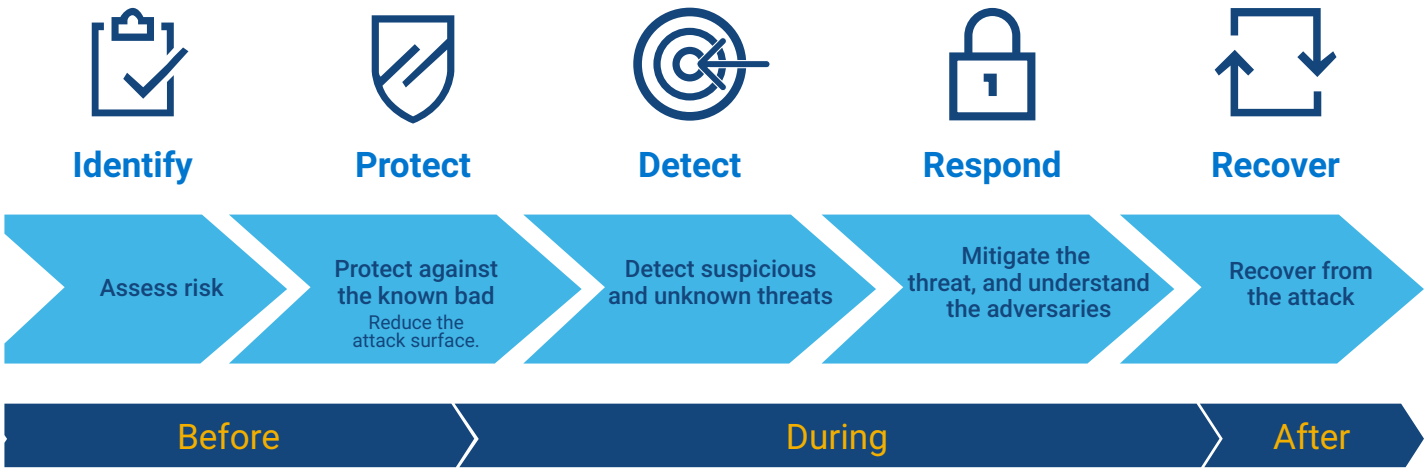


Figure 1. Dell's cyber resilient architecture is based on the NIST Cybersecurity Framework

By working with Dell Technologies OEM Solutions as a trusted technology partner, you can ensure that the technology infrastructure you use to build your solution is secure and resilient.

© 2023 Dell Inc. or its subsidiaries.

The Dell Secure Development Lifecycle

Solution builders need to provide their customers with products and features—from servers to firmware to software—that deliver the highest levels of security and cyber resilience. Dell tools and processes encourage collaboration among developers, security specialists and operation teams to build products and features that are both efficient and secure.

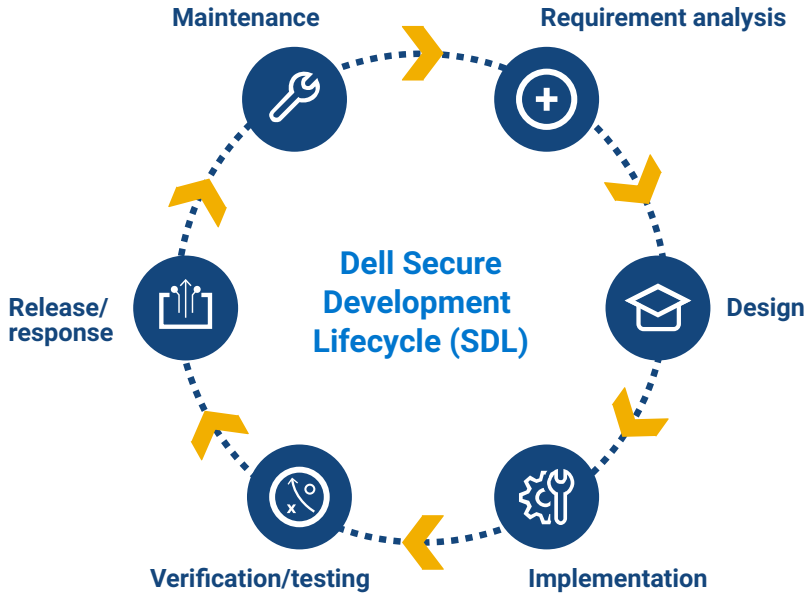


Figure 2. Dell's Security Development Lifecycle (SDL) model

The Dell Secure Development Lifecycle (SDL) program integrates security testing at every stage of the development process for products and features, including hardware, firmware and software.

At Dell Technologies, the SDL model is a key part of the overall design process. This process encompasses a view of security needs throughout the entire product lifecycle. Features are conceived, designed, prototyped, implemented, set into production, deployed and maintained with security as a key priority.

Firmware for servers, clients and appliances is designed to obstruct, oppose and counter the injection of malicious code during all phases of the product development lifecycle. Secure coding practices are applied at each stage of firmware development and during the threat modeling and penetration testing stages of the design process. For critical technologies, external audits supplement the internal SDL process to ensure that firmware adheres to known security best practices.

During software design, engineering teams create threat assessments and threat models to determine the threat surface and what mitigations, if any, need to be implemented in order to reduce the threat. Once the engineers have created and refined the code, they follow a rigorous testing process of the source code to ensure that it has been designed safely. Risk assessments are conducted using special tools to scan for security vulnerabilities and verify that the threat model was accurate. Software in the Dell Technologies integration and delivery pipeline undergoes SDL automation when building, testing and deploying applications, ensuring that security is integrated within each phase. When needed, a team of expert ethical hackers is directed to conduct penetration testing.

This exacting SDL process for ensuring cyber resilience across products and features is a key component of Dell Technologies' larger commitment to delivering a cyber resilient architecture for your customers. And the dedication to resilience does not end with a product release. Dell Technologies closely monitors security vulnerabilities and provides customers with timely Common Vulnerabilities and Exposures (CVE) information, guidance and mitigation options to minimize associated risks to their systems.

© 2023 Dell Inc. or its subsidiaries.

Dell Secure Supply Chain

A lot can happen between the time a component or device leaves the factory and when it arrives at its destination. Each step in the supply chain represents a new vector that opens your customers up to potential cyber attacks. Solution builders run a risk if the supply chain to their customers is not secure from the first mile to the last.

Supply chain attacks are widespread and impactful. They exploit the natural seams between organizations, and they abuse relationships—targeting organizations in a way that embeds compromise deep into the technology stack, from software down to firmware and hardware components.

Dell Technologies operates one of the world's most reliable and secure supply chains, and it has extensive protocols in place to prevent the malicious introduction of counterfeit components and malware.

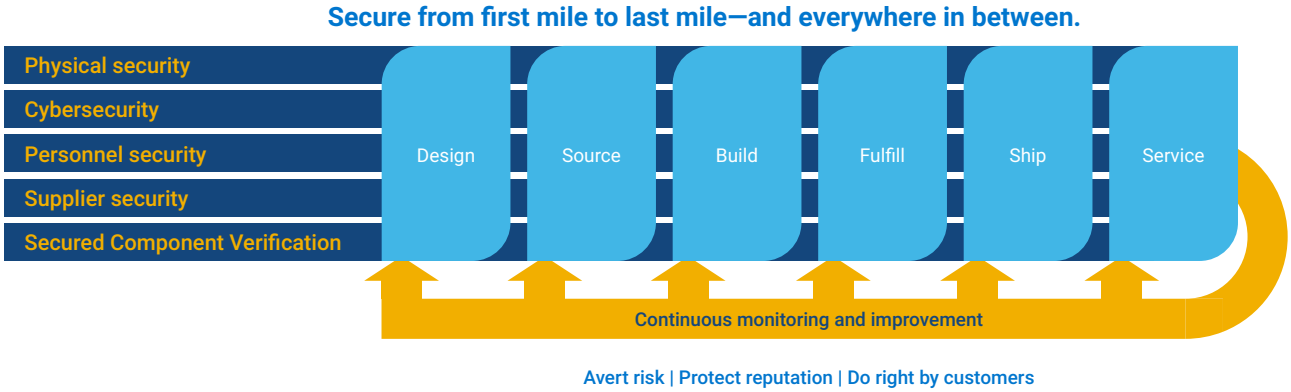


Figure 3. The secure supply chain lets you trust where your silicon and firmware came from

Dell Technologies has developed tools, technologies and processes to help ensure the security of products before they reach your customers and to enable self-verification of authenticity before devices are deployed. Multiple layers of controls mitigate threats that could be introduced into the supply chain. These controls, along with effective risk management, help establish supply chain security for you and your customers.

Dell Technologies component suppliers are fully vetted and validated, and all global manufacturing sites are ISO 9001 certified for quality control practices.

A core element of the Dell Technologies supply chain assurance program is Dell Secured Component Verification (SCV), which assures that no changes or substitutions have been made to your hardware after it left the factory. SCV uses a hardened system identity framework that attests to the authenticity of components and firmware subsystems. Before a system is deployed, you can securely validate that it was delivered to you as built in the Dell Technologies manufacturing facility. This complements the robust firmware signing and drift detection provided by Dell Technologies Systems Management Tools. SCV is available across the Dell PowerEdge server portfolio and Dell client portfolio, so you can confidently deploy PowerEdge servers into your customers' security sensitive environments knowing they are validated using industry and regulatory trends.

Learn more about Dell Supply Chain Security.

© 2023 Dell Inc. or its subsidiaries.

Dell Technologies and Intel Cyber Resilience Above and Below the OS

Dell SafeBIOS provides visibility to hidden and lurking attacks with BIOS tamper alert, with exclusive off-host BIOS verification, capture and storage and indicators of attack. Dell servers, clients and appliances emphasize security at both the hardware and firmware levels by leveraging an immutable Root of Trust. The Root of Trust is used to verify subsequent operation. This verification establishes a chain of trust that extends throughout the hardware and software stack. The hardware Root of Trust is built on Dell Technologies and Intel security features that operate below the level of the operating system (OS), where traditional anti-malware programs cannot protect.

Dell Technologies and Intel have been partnering in the commercial device space for decades and have earned customers' trust with some of the most secure commercial devices in the industry. Intel Hardware Shield consists of advanced threat protections, application and data protections and below-the-OS security, which includes Intel BIOS Guard, Intel Boot Guard, Intel Firmware Guard and more than 20 innovative security technologies. Dell Technologies has harnessed these capabilities to develop security solutions that provide customers with some of the most secure commercial devices on the market.

For more information, see "Achieving pervasive security above and below the OS."

Dell Product Portfolio: Elements of a Trusted Infrastructure

A trusted infrastructure operates everywhere, from edge to data center to multicloud, providing maximum flexibility and business agility without compromising security. Dell Technologies OEM Solutions is committed to providing you with a trusted infrastructure that is cyber resilient and that supports a Zero Trust architecture to secure and preserve your customers' most vital digital assets.

Dell Technologies trusted infrastructure is built on a broad product portfolio that includes servers, storage, data protection, networking, hyperconverged infrastructure (HCI) and edge solutions. Dell Technologies takes a holistic approach to cybersecurity with platforms and processes engineered to be intrinsically secure:

- Silicon root of trust
- Firmware protection (NIST 800-193)
- Advanced detection and response
- Threat modeling and vulnerability assessment through testing of code

Servers

As servers become more critical in your customers' software-defined data center architecture, server resilience becomes the foundation of their overall enterprise security. Every PowerEdge server is constructed with a cyber resilient architecture that builds in security at every phase of the product lifecycle. Security is baked in, from the silicon to signed firmware and drift detection to BIOS recovery and systems management integration.

Intel Software Guard Extensions (Intel SGX) and other security features help bring a Zero Trust security strategy to life while unlocking new opportunities for business collaboration and insights—even with sensitive or regulated data.

At the heart of PowerEdge server resilience is Integrated Dell Remote Access Controller (iDRAC). iDRAC is at the center of the Dell Technologies Root of Trust, and it has many security features built into it, including the following:

- At boot time, iDRAC checks to make sure that the correct Dell firmware is loaded.
- iDRAC runs through the BIOS to ensure that there has been no tampering, to verify that all components are attested and to confirm that the platform is sufficient as designed.
- iDRAC protects your data at rest with SEKM (secure enterprise key manager)/iLKM (integrated local key manager).

© 2023 Dell Inc. or its subsidiaries.

This chain of trust, along with security controls and comprehensive Dell OpenManage Systems Management Tools, provides robust layers of security across Dell servers and firmware. The result is a cyber resilient architecture that extends across every aspect of the server, including the embedded firmware, the data stored in the system, the OS and any peripheral devices. Your customers can build a process to protect their valuable server infrastructure and the data it contains. They can detect any anomalies, breaches or unauthorized operations, and they can recover from cyber attacks or potentially harmful unintended events.

Dell Technologies recently launched a new OEM PowerEdge portfolio based on 4th Gen Intel Xeon Scalable processors, including the Dell OEM PowerEdge R760 server. The new server portfolio is built to power your innovation engine with a secure infrastructure that supports a full range of modern workloads and objectives.

Dell PowerEdge Server

The Dell PowerEdge R760 server, with dual Intel Xeon Scalable processors, provides performance and versatility as needed to address your most demanding applications.

Storage

Dell Technologies storage solutions are designed with threat intelligence and cyber resilience built-in to safeguard your customers' valuable data from cyber-attacks. Data isolation options boost their cyber resilience with network separation of business-critical data to protect against ransomware and to automate failover and recovery.

Dell PowerScale

Modern, flexible scale-out file storage available in all-flash, hybrid and archive nodes with built-in security features and integrated cyber protection options.

Intelligent threat detection monitors storage and data access to identify suspicious activity and minimize exposure. Centralized storage and continuous cybersecurity monitoring provide early detection. Tools powered by artificial intelligence (AI) detect patterns in data access that indicate security compromises. And security alerts are integrated with upstream security platforms through API-based automation.

PowerScale also brings a host of additional security features, including: multi-factor authentication, software-based firewall, FIPS-compliant data in flight encryption, SEC17a-4 compliance locking, data segregation with access zones, security reporting for auditing, role base access controls and ransomware protection to name a few.

Rapid recovery of stored data is a key feature of cyber resilience. Dell storage solutions provide flexible, granular data recovery that secures data with policy-driven automation to enable space-efficient snapshot creation and retention to ensure business continuity with instant recovery in the event that data is corrupted or deleted.

Data Protection

Utilize software and data protection appliances that are specifically designed to secure your data across the edge, core and multicloud settings. To help you safeguard all your data and applications, Dell Technologies offers cyber recovery, backup, disaster recovery, long-term retention and more. With the appropriate solution that satisfies your business objectives, you can streamline data protection, boost efficiency and quicken agility.

© 2023 Dell Inc. or its subsidiaries.

Dell PowerProtect Data Manager Appliance

The Dell PowerProtect DM5500 appliance, built on 2x Intel Xeon processors, provides secure operational and cyber resilience including Active Directory, two-factor authentication, Role-Based Access Controls (RBAC), retention locking, private network for internal communications, end-to-end verification and fault avoidance.

Protecting your business starts with protecting your data from ransomware. One of the ways Dell Technologies helps accomplish this is to isolate critical data from ransomware and other sophisticated threats. With machine learning (ML) to detect suspicious activities, you can restore known-good data and confidently resume your routine business operations.

Networking

Dell networking solutions combine multiple layers of security at the edge and in the network, in hardware and software, including a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of network assets.

Each network security layer implements policies and controls, including network segmentation, centralized management, automation and scalability. When implemented through open standards, software-defined networking simplifies network design and operation and helps support Zero Trust network access.

Hyperconverged Infrastructure (HCI)

Not all HCI solutions are equal. Dell Technologies provides your customers an agile infrastructure with full-stack integrity and comprehensive lifecycle management to drive operational efficiencies and reduce risks.

Dell Technologies HCI product development includes security that is integrated throughout the product lifecycle. Product features are designed with security in mind, and the Dell Technologies concepts and designs are thoroughly analyzed to assess the potential security impact. Furthermore, Dell Technologies HCI solutions can be easily integrated with existing security infrastructures to meet your customers' security objectives and compliance requirements.

VxRail is developed in accordance with the Security Development Lifecycle (SDL) standards from product design through development, test, deployment, security alert monitoring, and timely remediation. In addition, VxRail provides manual and automated steps for configuring VxRail system to comply with DISA STIG requirements in support of the NIST Cyber Security Framework. VxRail supports 2-factor authentication, secure access with Access Control Lists (ACLs) and Role-Based Access Control (RBAC). Network segmentation, secure logging, Data at Rest Encryption (D@RE) with vSAN Encryption, enterprise key management and full stack lifecycle management are all supported to ensure VxRail is secure and trusted.

Dell VxRail for HCI

Dell VxRail, with Intel® Xeon® Scalable processors, delivers a turnkey experience with the built-in security layer of the hardware and software stack.

© 2023 Dell Inc. or its subsidiaries.

Dell NativeEdge - Edge Operations Software Platform

The Dell NativeEdge ensures security from design to deployment and all along the supply chain to protect applications, data and infrastructure across the edge estate using Zero Trust security principles.

The Dell NativeEdge is an edge operations software platform that helps enterprises across industries securely scale their edge operations to drive business outcomes. Designed with seven zero trust security principles at its core (device trust, user trust, transport and session trust, data trust, software trust, visibility and analytics and automation and orchestration) the Dell NativeEdge is an inversion of security control that never implicitly grants access to compute and data resources on the network. Zero trust seeks to continually verify access to all resources with a combination of identity and authorization verification through a granular policy engine.

Dell Trusted Workspace

Client Solutions

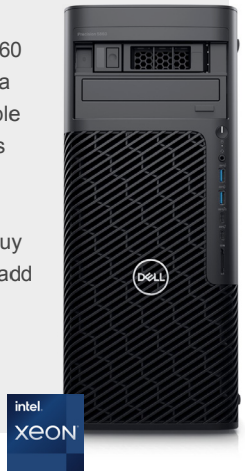
Perimeter security alone is no longer an option for your customers because, with so much traffic passing through the cloud and so many enterprise devices now being mobile, the perimeter is dissolving. Devices have more sensitive documents stored on them and traversing through them than ever before, and employees could be working from anywhere. Reduce the attack surface with a comprehensive portfolio of hardware and software protections exclusive to Dell. Our highly coordinated, defense-based approach offsets threats by combining built-in protections with ongoing vigilance.

The cyber resilience of Dell client solutions starts with a secure supply chain that implements Zero Trust principles at every step, from the controls around manufacturing to device assembly and delivery to customers. SCV allows you to validate and make sure that the components Dell Technologies shipped are the components you received.

Much like Dell servers, Dell client devices are protected by below-the-OS security features to ensure that the BIOS has not been tampered with and the right firmware and software are running on the right hardware.

Dell OEM Precision 5860 Workstation

The Dell OEM Precision 5860 workstation, available with a variety of Intel Xeon Scalable processor options, provides scalable performance in a mid-sized tower with OEM-ready options so you can buy the product de-branded or add your own brand to it.



Built-on Security Advanced protection for any fleet

Thwart advanced cyberattacks with Dell SafeGuard and Response. Dell SafeGuard and Response, powered by CrowdStrike® Falcon, VMware® Carbon Black and Secureworks®, provides a comprehensive approach to endpoint threat management. Artificial intelligence and machine learning proactively detect and block endpoint attacks, while security experts help hunt for and remediate identified threats across the endpoint, network and cloud.

Protect data on the device and in the cloud with Dell SafeData. Enable users to collaborate safely from anywhere. Netskope takes a datacentric approach to cloud security and access, protecting data and users everywhere, while Absolute gives IT visibility, protection and persistence outside the corporate firewall.

Built-in & Built-with Security via Dell commercial PCs

Detect tampering with Dell SafeBIOS. BIOS attacks are notoriously difficult to identify. Dell SafeBIOS alerts you to BIOS tampering so you can take swift action to quarantine and investigate the device. With Dell-exclusive off-host verification, the comparison image remains in a protected and separate location for post-attack forensics.[3]

Trust hardware is tamper-free on delivery with Dell SafeSupply Chain. Dell Trusted Devices, the industry's most secure commercial PCs[3], are built with industry-leading supply chain defenses and integrity controls. Offers like Secured Component Verification and tamper-evident packaging help ensure devices are safe from the first boot.

© 2023 Dell Inc. or its subsidiaries.

Secure user credentials with Dell SafeID. Only Dell secures user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.[3]

Keep information private with Dell SafeShutter. Enable users to work from anywhere while keeping private information secure.

Learn more at: Dell.com/Endpoint-Security

Supporting Diverse Use Cases of Solution Builders

Dell Technologies OEM Solutions customers can be found everywhere. In healthcare, they're pioneering genomic research and developing electronic health records (EHR) systems. In telco, they're building out 5G networks. In transportation, they're automating ports and developing new ways to track shipments. Solution builders have been at the forefront of industry change and have been powering new use cases driven by emerging technologies such as AI, 5G, edge and multicloud.

Security is a crucial foundation for all this innovation, and Dell Technologies understands that delivering the best security depends on understanding the use case of the solution builder. Solution builders need the ability to tune systems to meet their exact use cases, depending on their level of security sensitivity, where systems are deployed and who is responsible for the maintenance of a system moving forward.

In some cases, the appliance vendor wants complete lock down of the device and its security, with the end customer having no access to the configuration of the BIOS, or the OS. At the other extreme, the appliance vendor might want to give end users a high level of access to manage security settings themselves, either remotely through iDRAC, locally through the OS or the BIOS, or through a combination of those approaches. And there is a wide variety of use cases that fall between these all-or-nothing scenarios.

For use cases with unique requirements, Dell Technologies OEM Solutions works with solution builders to customize their systems to meet those requirements. When use cases become more common, Dell Technologies will add controls that let the solution builders themselves turn services and features on and off to achieve the configurations they want without needing Dell customizations.

Additional Security Considerations at the Edge

The use cases for many solution builders are not in the data center but at the edge, where real-world environments can be harsh. Extreme temperatures, humidity, air quality and vibration are a few of the environmental challenges at the edge. Sometimes edge solutions run with no people present onsite. Devices at the edge also need to have additional security protections beyond what is typically expected in a data center environment where everything is behind lock and key.

Dell Technologies OEM Solutions has a broad portfolio of innovative products and solutions purpose-built for the edge. Not only is this portfolio ruggedized against harsh conditions, but it also benefits from the same secure development lifecycle, secure supply chain and cyber resilient technologies as Dell applies to products designed for data center environments. Dell server technologies such as iDRAC, for example, are also used to manage many Dell storage and data protection products for use at the edge.

For customers requiring advanced physical security, Dell Technologies OEM Solutions offers encryption, chassis locks, rugged enclosures and firmware lockdowns that ensure sensitive data remains protected. Examples include:

- Military-grade encrypted drives
- Anti-tamper protection on packaging
- Container seals and tracking

© 2023 Dell Inc. or its subsidiaries.

Dell Technologies OEM Solutions Capabilities

The Dell Technologies OEM Solutions organization is a fully dedicated team of more than 1,000 people comprising engineering, program management, operations, support and more—all of whom are focused on helping solution builders design, market and support their solutions built on Dell trusted infrastructure, powered by Intel. As an engineering and design consultancy, OEM Solutions have helped our customers bring to market more than 10,000 unique, innovative designs, supporting a variety of use cases, in more than 40 industries globally.

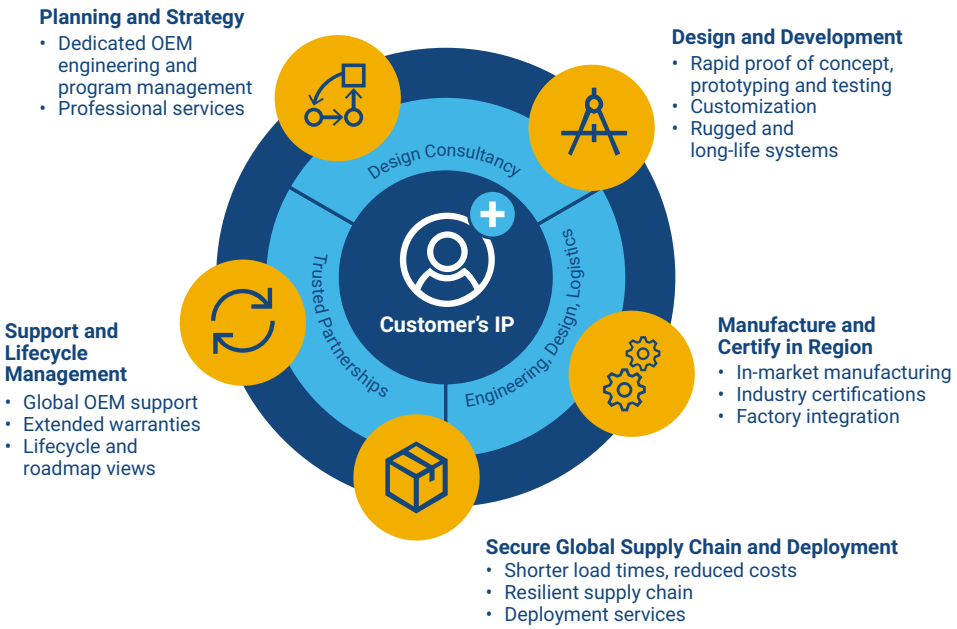


Figure 4. Engage with Dell Technologies OEM Solutions to help design, deliver and support your vision

What can you expect when you engage with the Dell Technologies OEM Solutions team? It all starts with planning and strategy, with "art of the possible" discussions to evaluate your solution's requirements, architecture options, go-to-market strategy, lifecycle management, deployment strategy and services. The team's sales engineers engage Chief Technology Officers (CTOs) and architects to understand your business imperatives and to partner with your innovators to maximize your intellectual property's potential.

During design and development, the OEM Solutions team's product, program and engineering teams work to design your solution while accommodating any unique requirements your solution has, depending on the required performance or form factors.

If your solution includes a manufacturing component, you can partner with Dell Technologies to benefit from the company's ability to manufacture in convenient locations. The ability to manufacture locally reduces the number of challenges that prevent you from getting your innovations into your customers' hands. If you need a specific model or specification for a particular region, Dell Technologies has global capabilities that give you that flexibility.

Rather than simply shipping the appliance or infrastructure to you, which requires you to handle the imaging, branding, application installation, BIOS and third-party configuration, Dell Technologies does it all for you in its facility, to your exact specifications. Dell Technologies can rack it, stack it, tag it, package it and ship it to your customer. It can also add your documentation in your branded box, if required.

Dell Technologies OEM Solutions offers standard platforms, as well as OEM Unique and Custom solutions. Dell Technologies has solutions that are tested and validated against recognized industry standards such as military, telco, energy and marine standards.[4] The Dell Technologies regulatory team can also help support any additional country-specific certifications you might need to obtain.

© 2023 Dell Inc. or its subsidiaries.

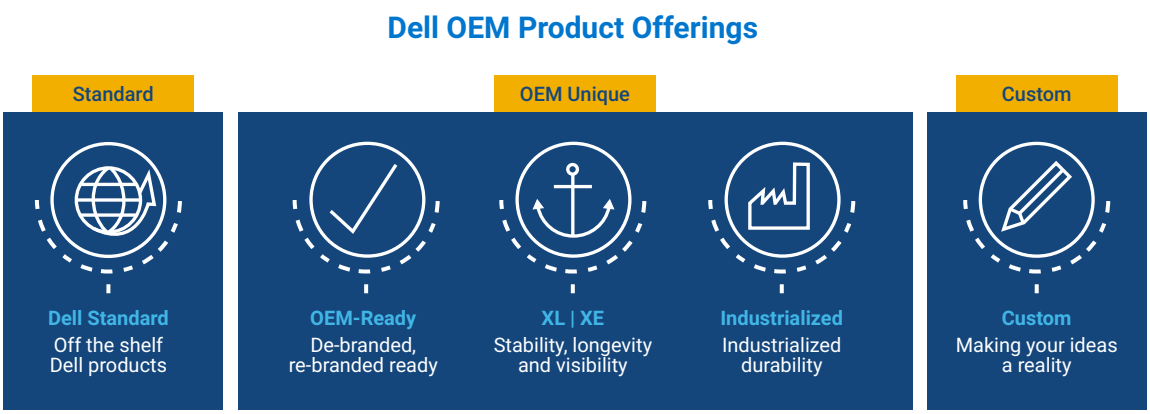


Figure 5. Dell Technologies OEM Solutions offers Standard, OEM Unique and Custom solutions

Dell Technologies OEM Solutions supports customers globally. Dell Technologies offers 24/7 global support from a dedicated OEM queue, which results in fast response times and quick resolution of issues from highly trained technicians.

Dell Technologies OEM Solutions has a broad ecosystem of partners who extend the capabilities of the OEM Solutions group at Dell. They provide additional design, integration and deployment capabilities as well as access to third party components. Partners also streamline last mile customization, final product recertification, and more.

Conclusion

Your customers rely on your solutions to help keep their data secure and their business processes running in the face of an ever-evolving threat landscape. You can count on Dell Technologies OEM Solutions and Intel as your trusted technology partners to help you design and deliver solutions built on trusted infrastructure and Zero Trust principles.

Dell Technologies and Intel offer a broad portfolio of cyber resilient technologies to meet the needs of a wide variety of use cases across 40+ verticals. This portfolio includes servers and clients, storage and data protection appliances, networking and HCI, and solutions for the edge. Dell Technologies OEM Solutions can enable you with solutions tailored to your environment and unique usage scenario including off-the-shelf products, OEM-ready platforms or solutions custom-designed with the help of Dell Technologies expertise.

The Dell Secure Development Lifecycle ensures that cyber resilience is top of mind at every stage of product development, deployment and maintenance. And the Dell Technologies secure supply chain ensures that your customers receive the correct, untampered versions of the hardware, firmware and software that your solutions call for.

Dell Technologies OEM Solutions is a partner you can trust to drive business growth and enable better business outcomes for your organization and for the customers you serve, all while ensuring security and cyber resilience.

Learn more about Dell Technologies OEM Solutions at Dell.com/OEM.

[1] Check Point Software Technologies. “Businesses Suffered 50% More Cyberattack Attempts per Week in 2021.” *Cyber Security Intelligence*. January 2022. www.cybersecurityintelligence.com/blog/corporate-cyber-attacks-up-50-last-year-6069.html.
[2] NIST. “Computer Security Resource Center | Glossary.” Accessed April 2023. https://csrc.nist.gov/glossary/term/cyber_resiliency.
[3] Based on Dell internal analysis, September 2022. Not all features available with all PCs. Additional purchase is required for some features.
[4] This applies to select products in Dell Technologies OEM Solutions portfolio.

© 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.