Edge Security Essentials

Edge Security and How Dell NativeEdge Can Help

August 2023

H19591

White Paper

Abstract

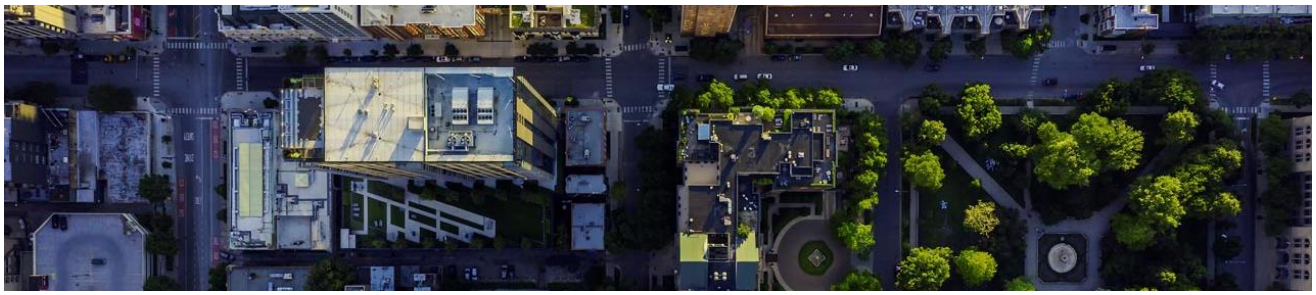
This technical white paper describes how vulnerable edge locations and industrial computer systems are to attacks by malicious actors and how critical public functions are thereby jeopardized. It details how dependent we have become in our daily lives on edge critical infrastructure and why the attack surface at the edge is so much higher than the traditional parameters of a datacenter. Considering cyberthreat advancements, political instability, and regulations, this document gives an insight into how the Dell Technologies edge offerings, and NativeEdge specifically, are helping to establish a safer environment for all of us.

Dell Technologies Solutions

Copyright

Contents

Executive summary



Security threats are everywhere and since the exposure and attack surface at the edge is larger compared to tradition enterprise environments, this brings additional complexities when deploying edge infrastructure.

- The US National Cybersecurity Strategy 2023 is shifting from consumers to suppliers when it comes to liability for security incidents.
- The EU GDPR rules dictate that data breaches must be reported to authorities within 72 hours after the detection. Failure to comply with data protection rules may result in disciplinary sanctions for EU businesses. These rules all focus on accountability, and that means that institutions and companies are liable for the data they process.

Security investments are rising, but the attack surface is also getting bigger and the understanding for many enterprises as not being “if”, but more “when” a breach happens.

Security incidents in operational technology (OT) and other industrial control systems (ICS) have three main motivations for the attackers: actual harm, commercial vandalism (reduced output), and reputational vandalism. The effect of breaches against these systems can result in reputational damage.

In the US, Executive Order (EO) 14028 introduced new regulations for companies supplying products or services containing software to U.S. government agencies and the Cybersecurity Act currently under development strengthens the EU Agency for Cybersecurity (ENISA). Both pieces of legislation establish a cybersecurity certification framework for products and services that reduce damage to consumers and enterprises.

This white paper introduces the key features and design considerations needed to enhance security for edge assets. It explains how Dell Technologies is approaching edge security in designing Dell NativeEdge—an edge operations software platform. This white paper explains how Dell NativeEdge will comply with industry standards and legislation to reduce customers vulnerability to security breaches and threats.

Security threats specific to the edge

Edge locations

Edge systems are often deployed by organizations where security is difficult or impossible to ensure, such as on factory floors or on top of communication towers where it would be too dangerous or expensive to station security guards and where controlling physical access is challenging. Some edge systems may be locked inside a cabinet or hidden away in hard-to-access places, but these protections are not ideal or reliably secure. As a result, the threat landscape for edge deployments is significantly greater than traditional data center deployments of enterprise information assets. The absence of IT or other security protecting resources like camera surveillance or physical guards protecting the assets at these locations brings additional challenges such as physical access, remote access, and disconnected or loosely connected scenarios.

In manufacturing, there is an electrical cabinet in many cases, but workers and service staff usually have unrestricted access to it and therefore its exposure is a security threat.

Figure 1. Electrical cabinets in manufacturing

Physical access

Physical access to the assets is one of the major threats at the edge. Defense mechanisms like video surveillance, tamper seals, or even in-person security guards are often not an option for cost and practical reasons. Locking devices in a cabinet is a form of protection, but since these are unmanned in many locations, it gives malicious actors all the time they need to plan and execute a breach. A keylock gives extremely limited protection as the theft of the whole cabinet in many cases is the biggest worry in these scenarios. Alternative methods are required to defend against physical access.

Scale

Many companies in their cloud and edge journey start with PoCs where they initially have one to 10 units to proof the solution. Once the solution is installed, SSH is the primary way of accessing these remote devices at the edge. Once that PoC is brought to mass production, SSH does not scale and a management plane is required to do this at massive scale.

Loosely connected sites

Often these edge locations are fully disconnected and occasionally check in, for example over a 4G connection, to send their information to higher-layered information systems or the cloud. This complicates security measures and could lead to incidents being reported late. To prevent the data being exposed to malicious users, alternative measures are required.

Skilled staff

Lack of skilled staff at the edge or having staff at these locations is challenging. Some sites are so remote that sending a skilled person to the location can be extremely expensive.

Edge breaches

Edge requires a different approach than traditional datacenter best practices as breaches have a direct effect on:

- People's quality of life: Edge infrastructure drives critical infrastructure, for example, digital cities, power grids, factories, hospitals, ships, buildings, and airports.
- Business continuity: Edge infrastructure drives critical applications that run, for example, cash registers, advanced optical inspection (AOI), operator equipment efficiency (OEE), energy efficiency, telco base station monitoring, and patient care.

This infrastructure requires the highest level of security and might involve dark sites, strict compliance, or regulatory constraints. The data processing at these sites often needs the highest level of confidentiality.

Security best practices at the edge

With cyber security threats becoming a part of both the assets we are working with and the way they are produced, maintained, and managed, novel approaches are needed to secure them. These threats can come from a variety of sources, whether from the equipment supply chain, assets, the network, users, or even the data itself.

Zero-trust

The diverse platforms of edge computing pose a challenge when attempting to consolidate them into a single security stack. Consequently, networks become vulnerable to unforeseen endpoint attacks. However, edge and IoT platform providers have recently shifted away from the "trust but verify" philosophy and have started incorporating technology that treats every endpoint and identity as a new security perimeter.

The truth is that most of today's edge and IoT platforms were not designed with sufficient security measures to withstand endpoint attacks. Companies struggle to integrate these platforms into a unified security stack because legacy edge and IoT platforms rely on server and operating system security. The lack of enforcement of least-privileged access through interdomain trust relationships leaves a wide range of endpoints vulnerable to intrusion and breach attempts.

To prevent devastating breaches, companies need to secure edge computing and IoT platforms across their entire stack. This includes hardware, operating systems, application platforms, data, and network security. Companies must explore how zero-trust can address the challenge of securing complete technology stacks for edge computing and IoT networks.

Zero-trust is described in the National Institute of Standards and Technology Special Publication (NIST SP) 800-207 as a new approach for trusting IT resources.

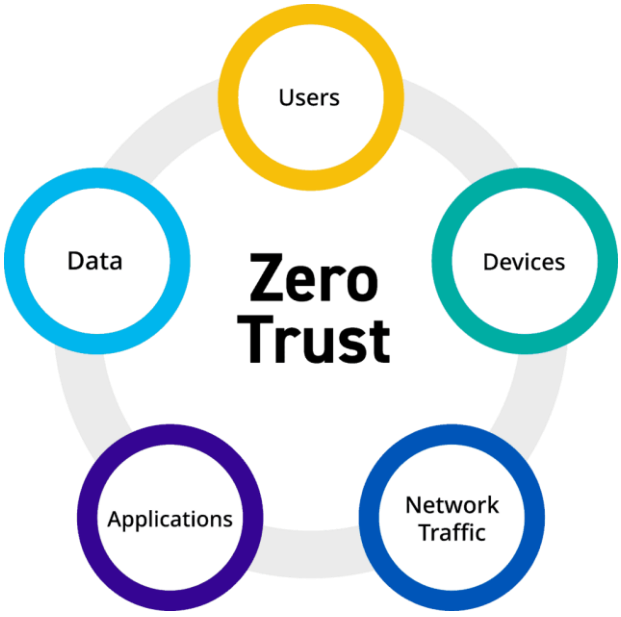


Figure 2. Zero-trust data points

Zero-trust is an integrated, end-to-end security strategy based on three core principles:

- Never trust, always verify—Always authenticate and authorize based on all available data points, including user identity, location, device, data sources, service, or workload. Continuous verification means there are no trusted zones, devices, or users. Instead, zero-trust treats everyone and everything as a potential threat.
- Assume breach—By assuming your defenses have already been infiltrated, you can take a stronger security posture against potential threats, minimizing the impact if a breach does occur. Limit the "blast radius"—the extent and reach of potential damage incurred by a breach—by segmenting access and reducing your attack surface, verifying end-to-end encryption, and monitoring your network in real time.
- Apply least-privileged access—Zero-trust follows the principle of least privilege (PoLP), which is the practice of limiting access rights for any entity and only permitting the minimum privileges necessary to perform its function. In other words, PoLP prevents users, accounts, computing processes, and so on, from having unnecessarily broad access across the network. Such access leaves your network vulnerable and creates a higher attack surface in case of a breach.

John Kindervag developed the original zero-trust model in 2010, and as a principal analyst at Forrester Research, he realized that traditional access models operated on the outdated assumption that organizations should trust everything within their networks. The thinking was that perimeter-based security (in other words, firewalls) would be enough to validate user access and secure the network entirely. But as more workers started remotely accessing systems through all types of devices and all kinds of connections, this trust structure proved insufficient to effectively manage a distributed workforce. Kindervag recognized this vulnerability and developed zero-trust in response.

A few major tenets:

- Network segmentation—Traditional networks exposed direct access to all data assets, servers, and applications. The zero-trust model segments various subsets of these resources and removes the ability for users to directly access them without first going through a tightly controlled gateway. This is sometimes referred to as "network isolation." Micro segmentation takes this concept further by isolating workloads from one another so that administrators can monitor and control the flow of information between different servers and applications rather than just between client and server.
- Access control—Regardless of whether users are physically located in an office or working remotely, they should only be able to access the information and resources that are appropriate for their respective roles. Each segment of the network should authenticate and validate authorization to ensure that traffic is being sent from authenticated and authorized users regardless of the location or source of the request.
- Visibility—Network boundaries should inspect and log all traffic, and admins should regularly monitor logs to ensure that users are only attempting to access systems that they are permitted to access. Administrators often use cloud access security broker software to monitor traffic between users and cloud applications and warn when they see suspicious behavior.

Identity and assurance

A crucial part of a zero-trust environment is identity and assurance, as this is where trust is created.

By implementing robust identity-proofing mechanisms, NativeEdge ensures that individuals accessing the platform are who they claim to be. This process establishes trust, reduces the risk of unauthorized access, and protects the integrity and confidentiality of data within the platform. It forms a fundamental part of the overall zero-trust architecture, safeguarding the users, devices, network applications, and data.

Secure component verification

Dell secure component validation (SCV) is a process used by Dell Technologies to ensure the authenticity and integrity of the hardware components used in its products. It involves a series of verification steps to validate that the components used in Dell systems are genuine, free from tampering, and meet the required quality standards.

The SCV process typically includes the following steps:

Supply chain integrity—Dell works closely with trusted suppliers and manufacturers to establish a secure supply chain. This includes verifying the identity and authenticity of the components throughout the manufacturing and distribution process.

Component verification—Dell validates the components used in its systems to ensure that they are genuine and not counterfeit. This may involve inspecting unique identification markers, serial numbers, holographic labels, or other security features specific to the components.

Firmware validation—Dell verifies the integrity and authenticity of the firmware or software embedded in the components it uses. This helps ensure that the firmware has not been modified or tampered with, safeguarding against potential security vulnerabilities.

Testing and quality assurance—Dell conducts rigorous testing and quality assurance procedures to verify that the components meet the specified performance and reliability standards. This includes functional testing, stress testing, and compatibility testing.

Security measures—Dell incorporates additional security measures, such as secure boot processes and cryptographic signatures, to protect against unauthorized access or tampering of the components.

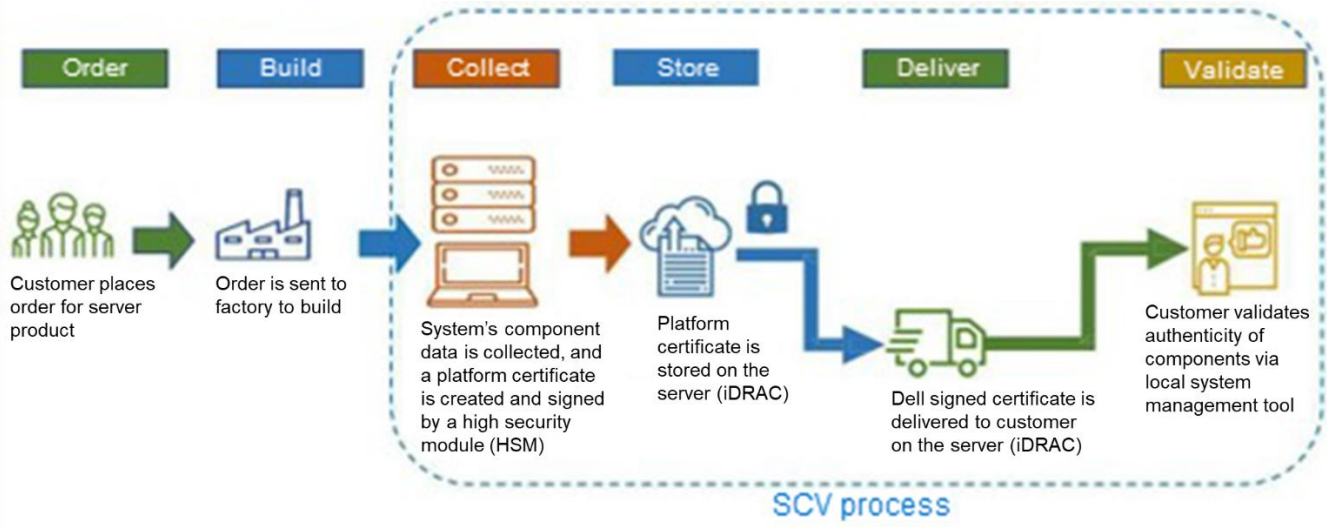


Figure 3. Secured component verification

By implementing SCV, Dell Technologies ensures that the hardware components used in its products are genuine, trustworthy, and meet the required standards. This helps to enhance the overall security, reliability, and performance of Dell systems, giving customers peace of mind when using Dell products.

Piece-part identification

To enable appropriate traceability, all key components are uniquely identified by a serial number label or marking, a Dell-prescribed piece-part identification (PPID) label, or an electronic identifier that can be captured during the manufacturing process. PPID provides a foundation for the downstream component verification capabilities offered by Dell.

Software bill of material

The software bill of material (SBOM) ensures that the software supply chain is known and trusted. The security and validity of software and its source has taken on renewed importance in response to the increase in supply chain attacks. The SBOM has become an integral part of the Dell lifecycle management and the secure development lifecycle of the software components of Dell offerings.

To learn more about the Dell secure supply chain, see A Partnership of Trust: Dell Supply Chain Security.

Public key infrastructure

The public key infrastructure (PKI) is the set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public keys.

A PKI consists of:

- A certificate authority (CA) that stores, issues, and signs the digital certificates.
- A registration authority (RA) that verifies the identity of entities requesting that their digital certificates be stored at the CA.
- A central directory—A secure location in which keys are stored and indexed.
- A certificate management system managing the access to stored certificates, the delivery of the certificates to be issued, and so on.

- A certificate policy stating the PKI's requirements concerning its procedures. The purpose is to allow outsiders to analyze the PKI's trustworthiness.
- Dell is uniquely positioned by owning the hardware design, the firmware design, and the OS runtime environment. NativeEdge can assure the five key pillars under the zero-trust architecture asset trust (devices, network, applications, users, and data), NativeEdge can become an integral part of that PKI. With this, it assures these entities can cryptographically signed and protect trustworthiness of these assets.

Secure boot

Secure boot (SB) is a security feature implemented in modern computer systems to ensure the integrity and authenticity of the boot process. It is designed to prevent the execution of unauthorized or malicious software during system startup.

When SB is enabled, the system firmware, typically the unified extensible firmware interface (UEFI), verifies the digital signatures of the bootloader and the operating system kernel before allowing them to run. These digital signatures are generated by trusted entities, such as the PC manufacturer or operating system vendors, and indicate that the software components are genuine and have not been tampered with.

If the digital signatures are valid and match the trusted signatures stored in the firmware, the system proceeds with the boot process. However, if the signatures are invalid or missing, secure boot prevents the execution of the software, alerting the user or administrator to a potential security threat.

By enforcing the use of trusted software, secure boot helps protect the system against rootkits, bootkits, and other forms of malware that attempt to hijack the boot process and gain control over the system. It establishes a chain of trust from the firmware to the operating system, enhancing the overall security of the computer system.

For NativeEdge-enabled hardware, this means that only Dell-signed firmware can execute on the supported platforms.

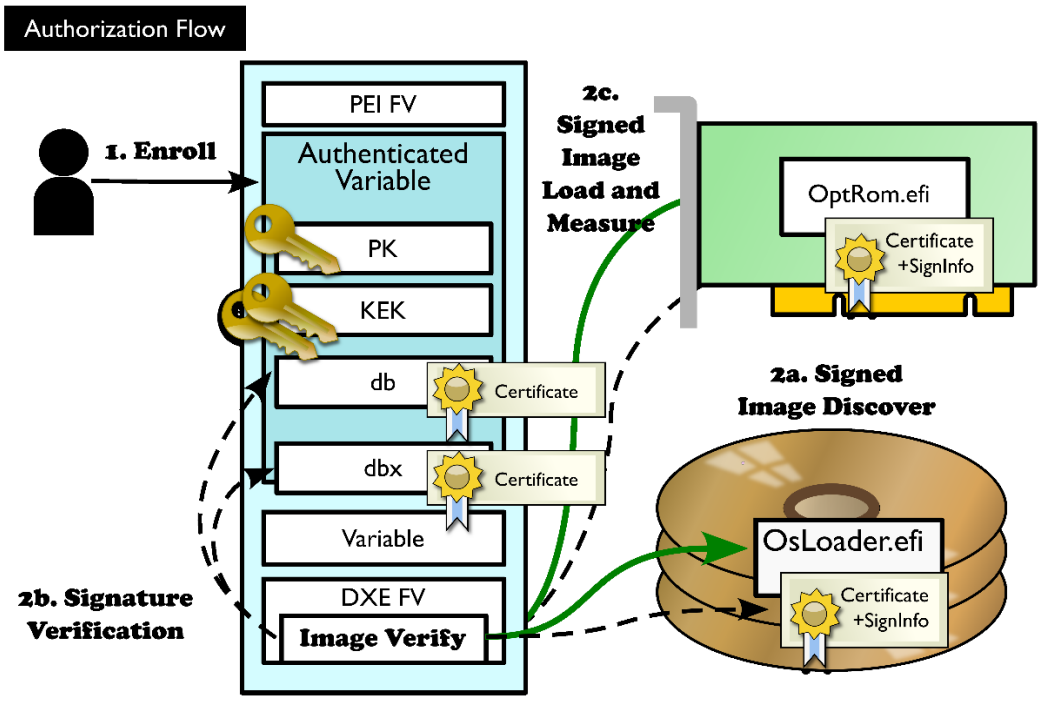


Figure 4. Secure boot authorization flow

Signed/resilient firmware

One potential threat to any supply chain is the risk of unauthorized code or data modifications. Dell engineers add a cryptographic digital signature to software, applications, and firmware—a process known as code signing—to enable confirmation of authenticity and integrity at runtime. The code signing makes the firmware resilient to malicious code being introduced and thus prevents it from being compromised.

Restricted BIOS access

NativeEdge-enabled Devices have restricting access to BIOS functionality by the user further decreases the attack surface. Firmware settings cannot be altered by the user in any way, as this access is confined the control plane.

FIDO device onboarding

Fast IDentity Online (FIDO) is the organization that has established the FIDO device on-boarding (FDO) specification which solves two key IoT security challenges: supply chain security and passwords without physical users. Historically, devices have been manually added to servers and controls. This is expensive and insecure as the trust is provided by the installers or SIs provisioning the devices. FDO allows the device to prove its trust (attestation) from the device initialization in factory and therefore can be automatically onboard without the need for human intervention. The FDO was developed by the FIDO Alliance based on the same guiding principles of convenience, security, and privacy used for FIDO authentication.

FDO and Dell's unique position of owning the hardware, firmware, and the operating environment provides a secure supply chain from point of ordering to point of delivery for NativeEdge-enabled Devices. All that customers need to care about is the eventual application that will be running at these endpoints. Dell Validated Designs for the edge can be delivered to endpoints in a trusted manner.

The following figure shows how devices and ownership vouchers are sent to customers along different paths to ensure security from manufacturing all the way to receipt and installation of the device:

- A logistical path where the device is shipped from Dell manufacturing to the end location.
- An IT path where the ownership voucher travels from manufacturing to the end location.

When the two join again, trust is enabled by the combination of the device, the authenticity of which is validated by SCV, and the ownership voucher which confers ownership. Only if trust has been verified can workloads be trusted. This assures confidence that this device was built by Dell and is allowed to run the workload assigned to it by its trusted owner.

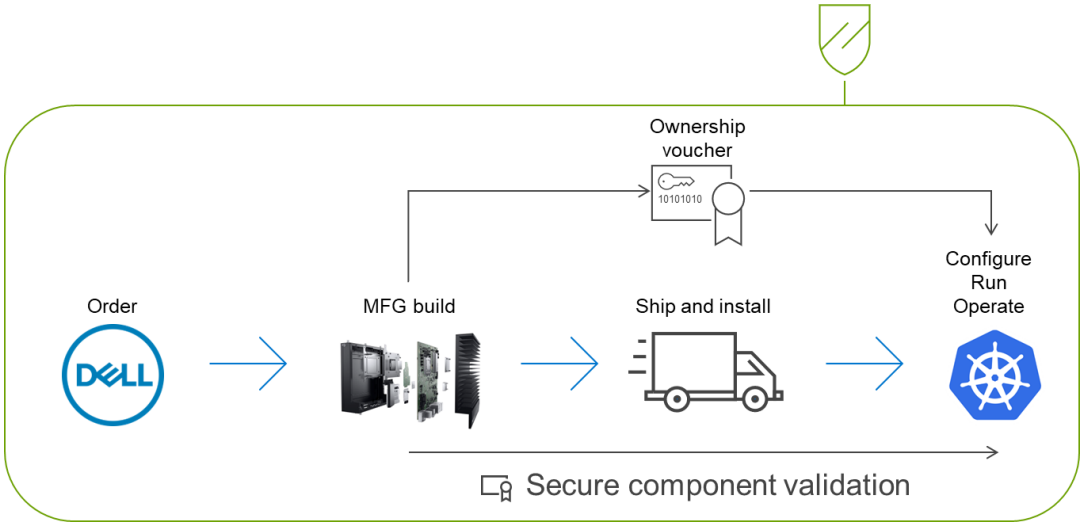


Figure 5. Ensuring security from manufacturing all the way to receipt and installation of the device

Multi-factor authentication

Talking to our customers, we found that weak passwords are one of the major sources of security breaches. Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. The NativeEdge Orchestrator provides robust tools to define the complexity and chronology of password usage throughout the NativeEdge secure environment

Root of trust

Root of trust (RoT) provides a means of assuring that each entity in the boot process is reviewed for integrity in a chain of trust. Each BIOS module contains a hash of the next module in the chain.

The key modules in BIOS are:

- Initial boot block (IBB)
- Security (SEC)
- Pre-EFI initialization (PEI)
- Memory reference code (MRC)

- Driver execution environment (DXE)
- Boot device selection (BDS)

In PowerEdge servers, the RoT is provided through the integrated dell remote access controller (iDRAC). The iDRAC boot process uses its own independent silicon-based root of trust that verifies the iDRAC firmware image. The iDRAC root of trust also provides a critical trust anchor for authenticating the signatures of Dell Technologies firmware update packages (DUPs).

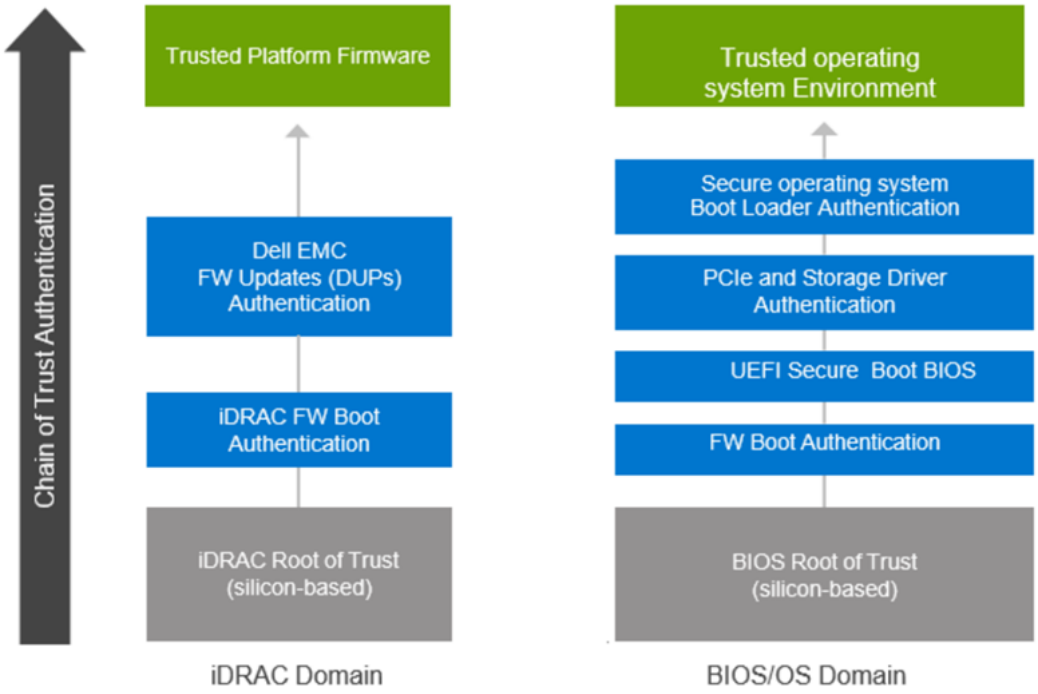


Figure 6. Chain of trust authentication

Trusted platform module

All NativeEdge-enabled Devices carry a root of trust (ROT) in the form of a trusted platform module (TPM) which is a chip that resides inside a computer and is soldered to the system board on Dell computers. The primary function of a TPM is to securely generate cryptographic keys, but it has other functions as well. Each TPM chip has a unique and secret RSA key that is embedded into it during production.

The main components of the TPM are:

- Cryptographic processing
- Persistent and versatile memory

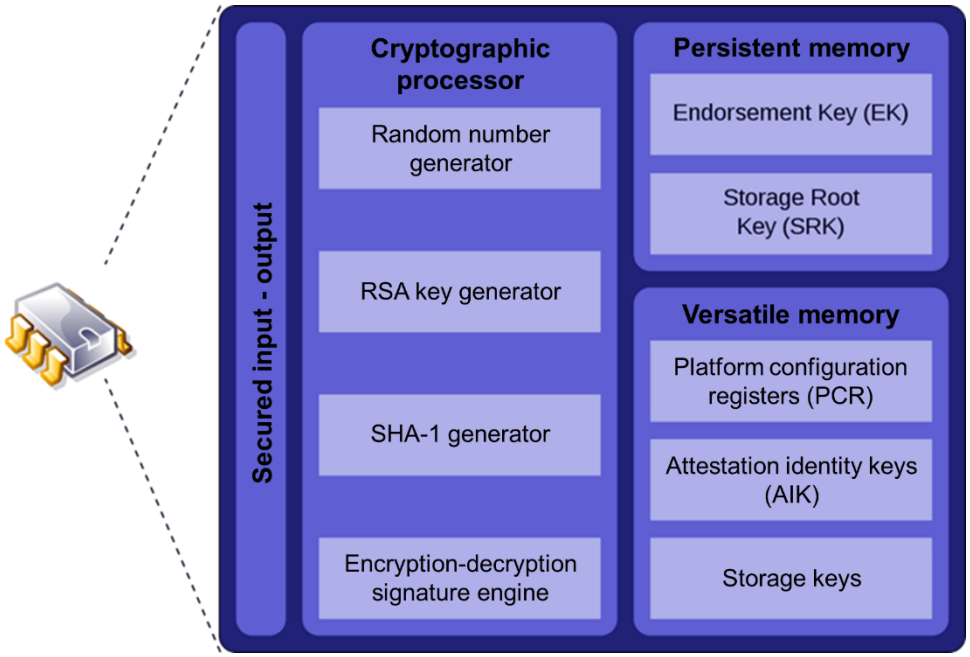


Figure 7. Main components of the TPM

NativeEdge-enabled Devices have a root of trust either in the form of an iDRAC or a TPM to hold platform secrets securely.

Data at rest encryption

NativeEdge provides data at rest encryption (DARE), which is a requirement for federal and industry regulations and ensures that data is encrypted when it is stored. DARE is provided through self-encrypting drives (SEDs) and a key management system. The data on SEDs is encrypted, and the data may not be accessed if the SED is stolen or removed from the device.

Data at rest encryption is designed to prevent an attacker from accessing the unencrypted data by ensuring the data is encrypted when on disk. If an attacker obtains a hard drive with encrypted data, the data is inaccessible unless the attacker gets access to the encryption keys. Data at rest encryption is applied automatically to NativeEdge-enabled Devices. For PowerEdge, it does not matter if SED or non-SED drives are used. The platform automatically assures the data is secured against physical tampering or theft.

DARE uses SEDs and AES 256-bit encryption keys. The algorithm and key strength meet the NIST standard and FIPS compliance.

NativeEdge encrypts the drives whether they are SED or standard drives to provide assurance data stays untouched even in the event of devices being stolen or accessed by unauthorize or nefarious persons.

Role-based access control

NativeEdge provides role-based access control (RBAC), which is a method of restricting NativeEdge system access based on the roles of individual users within an enterprise. Organizations use RBAC—also called role-based security—to parse levels of access based on an employee's roles and responsibilities.

Compliance and hardening

Dell security standards

NativeEdge also targets our federal customers and will eventually carry the right certifications to serve these markets.

Dell standards for the security of IT systems and product development provide a strong posture for the security of data and information. They are based on industry-recognized best practices and guidelines such as those found in the ISO 27000 series (for example, ISO 27001, 27002, 27034, and so on).

The information security management system for Dell Technologies encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solution Group (ISG) and supporting functions inclusive of the security and resiliency organization (SRO), IT, facilities management, human resources, and legal.

Security development lifecycle

Delivering a cyber-resilient architecture requires security awareness and discipline at each stage of development. The security development lifecycle (SDL), which is the Dell approach for secure product and application development, is a key part of the overall system design process. This design process encompasses a view of security needs throughout the entire system lifecycle:

- Features are conceived, designed, prototyped, implemented, set into production, deployed, and maintained with security as a key priority.
- Server firmware is designed to avoid, detect, and mitigate the injection of malicious code during all phases of the product development lifecycle.
  - Threat modeling and penetration testing are executed during the design and validation processes.
  - Secure coding practices are applied at each stage of firmware development.
- For critical technologies, external audits supplement the internal SDL process to ensure that firmware adheres to known security best practices.
- Ongoing testing and evaluation of new potential vulnerabilities using the latest security assessment tools takes place.
- There is a rapid response to severe common vulnerabilities and exposures (CVEs), including security updates, and remediation measures are recommended as needed.

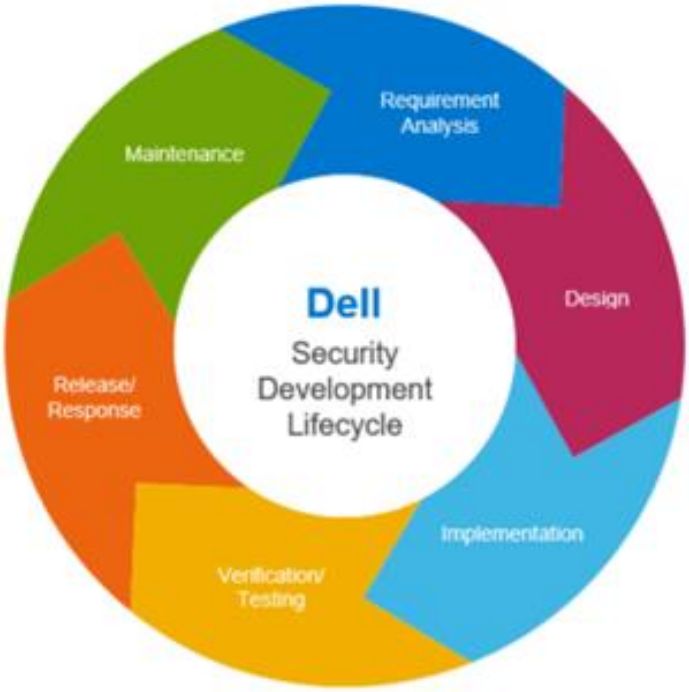


Figure 8. Phases of the security development lifecycle

Common vulnerabilities and exposures

Common vulnerabilities and exposures (CVE) is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that has been assigned a CVE ID number. We ensure that this is part of the SDL, and when CVEs are found post-release, the Dell products security incident response team (PSIRT) mitigates the situation.

See Dell Vulnerability Response Policy.

Port security

For enhanced security, NativeEdge allows all physical ports to be disabled. This reduces the attack surface for any nefarious user to insert, for example, USB drives or key generators.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is a federal agency within the United States Department of Commerce. It is responsible for promoting and maintaining measurement standards, including those related to technology and cybersecurity. NIST plays a crucial role in developing guidelines, frameworks, and best practices to enhance the security and resilience of information systems.

NIST provides numerous publications and resources that are widely recognized and followed in the cybersecurity community. One of the most well-known publications is the NIST Special Publication (SP) 800-53, which outlines security and privacy controls for federal information systems and organizations. NIST guidelines often serve as a foundation for other security standards and frameworks, both nationally and internationally.

Key points about NIST:

- Exists as a federal agency within the United States Department of Commerce.
- Develops guidelines, frameworks, and best practices for information system security.
- Publishes NIST Special Publications that outline security controls.
- Is widely recognized and influential in the cybersecurity community.
- Creates standards often serve as a foundation for other security standards and frameworks.

IEC 62443

Dell NativeEdge has the ability to host IEC62443 compliant workloads as some of the Dell Validated Designs comply with this standard. For example, Dell Technologies Validated Design for Manufacturing Edge with Litmus does comply with this standard where they can. This allows customers easy access to compliance.

IEC 62443 is a series of standards and technical reports that are developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC).

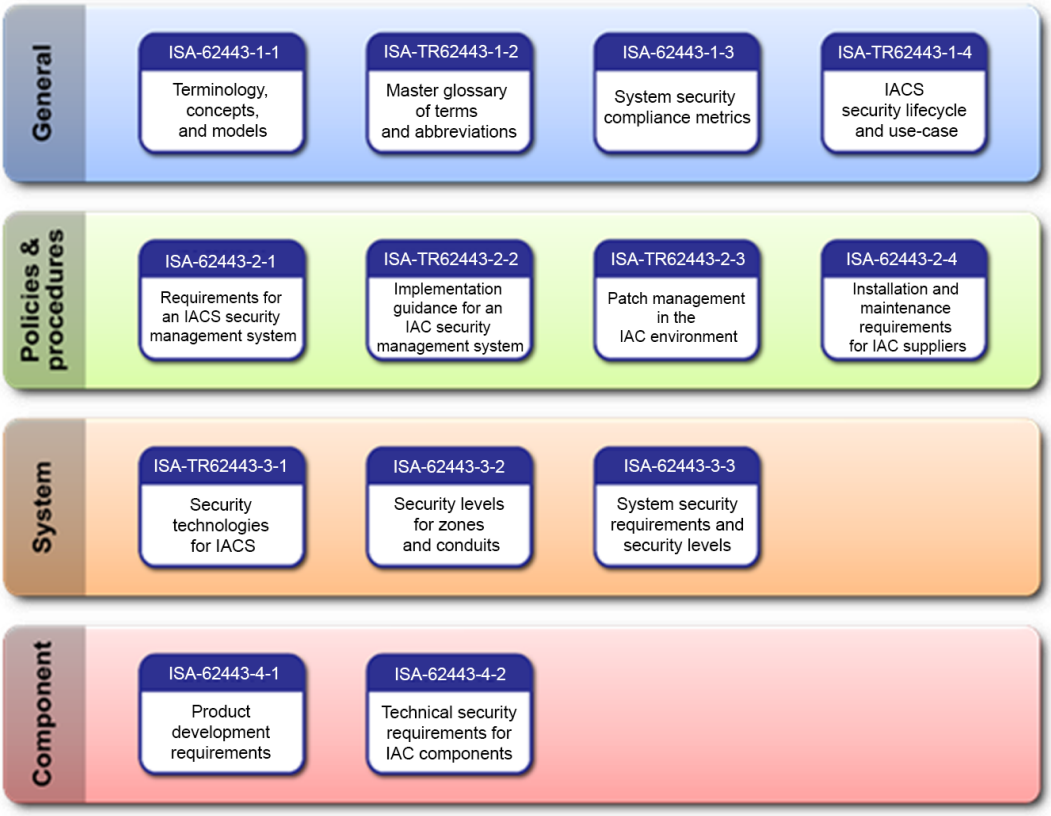


Figure 9. IEC 62443 standards and technical reports

For a more detailed explanation, see IEC 62443 Overview. Some of the validated designs that will be hosted inside NativeEdge will be validated against IEC-62443. One example is Dell Technologies Validated Design for Manufacturing Edge with Litmus, which carries this certification.

Automation

Secure zero touch runtime environment provisioning

Secure zero touch environment provisioning is an automated and secure process for deploying and configuring network devices. In the context of NativeEdge, this enables the seamless provisioning of devices without the need for manual intervention. It late binds the OS and runtime environment, and the desired pre-defined settings.

The process involves the following steps:

- Device enrollment—Network devices are registered with the NativeEdge Orchestrator, which manages their provisioning.
- Pre-configuration—Devices are initially configured with basic settings.
- Device discovery—Devices are connected to the network and are discovered automatically.
- Authentication and authorization—The server verifies the identity of the device and authorizes it for provisioning.
- Configuration delivery—The server pushes device-specific configurations to the device, including the runtime OS and environment.
- Configuration verification—The device verifies the integrity and authenticity of the configurations.
- Configuration application—The device applies the configurations to its operational settings.
- Post-provisioning operations—The device may perform additional tasks like connectivity testing and reporting provisioning status.

NativeEdge ensures efficient and secure deployment of network devices. It reduces manual effort, enhances network security, and maintains consistent configurations across devices. This automated provisioning process contributes to the overall success and effectiveness of NativeEdge network infrastructure.

Life cycle management

By introducing lifecycle management into NativeEdge, the platform allows to reduce 0-day exploits by automating the task of hardware, firmware, and software patching. Dell provides upgrade bundles which are cryptographically signed and validated during the uploading to NativeEdge Orchestrator and when applied to the NativeEdge-enabled Devices. Further, Dell provides a checksum for enhanced validation of consultancy when downloading the individual bundles.

In accordance with Dell Vulnerability Response Policy, Dell actively participates in various community efforts including the Forum of Incident Response and Response Teams (FIRST) and the Software Assurance Forum for Excellence in Code (SAFECode). Our processes and procedures align with the FIRST PSIRT Services Framework, as well as other standards including ISO/IEC 29147:2018 and ISO/IEC 30111:2019.

Micro segmentation

NativeEdge provides software micro segmentation, and it is a security technique used to enhance the security of virtual machines (VMs) and containers within a network environment. It involves dividing the network into smaller segments or zones to create isolated and highly controlled communication paths between VMs or containers.

For VMs:

In the context of VMs, micro segmentation works by implementing security policies at the virtual network level. Each VM is assigned to a specific microsegment, and communication between VMs is tightly controlled based on predetermined rules. These rules can define which VMs can communicate with each other, what types of traffic are allowed, and the specific ports and protocols that can be used. By segmenting the network at a granular level, micro segmentation limits the lateral movement of threats and contains potential security breaches to a specific segment, minimizing the overall risk.

The benefits of micro segmentation in NativeEdge for VMs include:

- Enhanced security—Micro segmentation reduces the attack surface by isolating and restricting communication between VMs or containers. It helps contain potential threats and prevents unauthorized access to critical resources.
- Granular control—By implementing specific security policies for each microsegment, administrators have detailed control over the flow of network traffic. They can define and enforce policies based on the specific requirements and sensitivity of the applications and data.
- Compliance and regulatory requirements—Micro segmentation can assist organizations in meeting compliance standards by ensuring the isolation and security of sensitive data. It helps enforce data privacy and protection regulations.
- Simplified management—Micro segmentation allows for centralized management of security policies and rules. Administrators can define, monitor, and update policies from a single management interface, making it easier to maintain and adapt to changing security requirements.

Overall, micro segmentation provides a powerful security mechanism for protecting VMs and containers by isolating and controlling network traffic. It strengthens the overall security posture and helps organizations mitigate the risks associated with potential breaches and the lateral movement of threats within virtualized environments.

If the same workloads were to run on the same bare metal system, the attack surface would likely be broader and harder to secure.

Secure NativeEdge-enabled Device communication

In many edge locations there is separation, routing, and proxying in place to communicate from user endpoints. Placing a new system inside these environments can be challenging as it might affect proxy and firewall routing. By using a port 443 reverse proxy on the end nodes, it allows secure HTTPS communication on one side and in many cases already available means for IT clients to communicate to the outside world. All services in the NativeEdge environment use mutual transport layer security (mTLS) communication to mutually authenticate each entity in the environment. This assures that each service has to be granted access as part of the PKI environment. To further enhance the security of this communication, NativeEdge includes mutual TLS as a means of communicating between all services inside the environment. mTLS ensures that the parties at each end are who they claim to be by verifying that they both have the correct private key. The information within their respective TLS certificates provides additional verification.

Conclusion

Dell NativeEdge is an edge operations software platform that helps businesses securely scale their edge management across all locations. Its API-based architecture facilitates seamless communication and integration between software systems and applications. It acts as a bridge that enables developers to connect, share data, and leverage functionalities across various software components.

The main features and characteristics of the NativeEdge are:

- Integration—The platform enables seamless integration between disparate software systems, allowing them to work together and share data effectively. It simplifies the process of connecting different applications, eliminating the need for custom integration solutions.
- Data exchange—NativeEdge enables the secure and efficient exchange of data between systems. It provides standardized methods for retrieving, updating, and synchronizing data, ensuring consistency and accuracy across applications.
- Functionality extension—Developers can leverage the capabilities of existing software systems by accessing their functionalities through the NativeEdge platform. This allows for the extension of application capabilities without the need for extensive custom development.
- Scalability and flexibility—The platform is designed to scale and adapt to changing business needs. It accommodates the integration of new applications and services, ensuring flexibility and futureproofing for evolving software ecosystems.
- Security and governance—NativeEdge prioritizes data security and governance. It provides authentication, authorization, and encryption mechanisms to ensure secure communication and protect sensitive information.

In summary, the NativeEdge enables seamless integration, data exchange, and functionality extension across diverse software systems. It promotes scalability, security, and developer collaboration, making it a valuable tool for building interconnected and robust software ecosystems.

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Solutions team by email.

Author: Jeroen Mackenbach

Note: For links to additional documentation for this solution, see Dell Technologies Solutions Info Hub for NativeEdge.

References

Dell Technologies documentation

The following Dell Technologies documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- *Dell NativeEdge Security Configuration Guide – under the documentation tab on the NativeEdge Orchestrator support page*
- *Dell NativeEdge Orchestrator User's Guide – under the documentation tab on the NativeEdge Orchestrator support page*
- *Dell NativeEdge Orchestrator Deployment Guide – under the documentation tab on the NativeEdge Orchestrator support page*
- *Additional resources on the NativeEdge page of the Dell Technologies Info Hub*