Pillar one: Protect critical data and systems.

Fortifying your organization with modern security requires rethinking how you protect data and systems. Dell delivers significant incremental value with intrinsic security features and a holistic presence across the ecosystem.

Intrinsic security

Dell starts with devices and processes designed for security as a baseline. If **intrinsic security features** already exist in the hardware, the firmware and the security control points, the architectural foundation is ahead of the game. Intrinsic security also automates foundational security elements, reducing or even eliminating the need for human involvement and intervention.

Dell delivers incremental value with **intrinsic security** features built into its platforms and internal processes. As a global leader in IT technology for decades, Dell has had many years to drive intelligent innovation for security deep into our product designs and processes. Our customers utilize our hardened devices and processes for an intrinsic advantage.

Endpoint data protection – Dell Trusted Devices

Dell Trusted Devices is a collection of features and offerings that help make Dell the industry's most secure commercial personal computers.[2] Dell Trusted Devices feature embedded technology that protects the device at the BIOS level. Only Dell maintains a protected firmware image and user access credentials off host on a dedicated security chip, hidden from malware that may steal access credentials or hijack the firmware.

Dell SafeData, part of the Dell Trusted Devices feature stack, helps protect data with:

Netskope is a cloud-delivered security platform aligned with Gartner's secure access service edge (SASE) framework that includes network and data security controls for the modern enterprise. Includes zero-trust network access (ZTNA).

Absolute Persistence® technology is embedded in the firmware of Dell laptops and desktops. This technology provides a continuous, tamper-proof connection between devices and data on or off network and self-healing applications (such as VMware Carbon Black and Netskope). The connection is managed via the cloud-based Absolute console.

Dell Managed Detection and Response: The endpoint security portfolio, Dell Technologies Managed Detection and Response, powered by Secureworks® Taegis™ XDR, is a fully managed, end-to-end, *24/7 service that monitors, detects, investigates and responds to threats across the entire IT environment*.

Finally, **APEX Backup Services** is a software-as-a-service (SaaS)-based data protection platform that offers secure, scalable and cost-effective backup, retention, compliance and recovery for SaaS apps, endpoint devices and workloads running in the cloud on-premises.

Dell’s secure supply chain program aligns to and, in places, exceeds US government-promoted best practices and standards, and we’re constantly improving.

Extending security across your full IT infrastructure

Servers

Our Dell PowerEdge servers are designed and built with a cyber-resilient architecture that aims to have security built in at every phase of the server lifecycle. Key components include:

Hardware root of trust. A cryptographic key that Dell embeds into product silicon during hardware production to ensure that the BIOS cannot be tampered with.

Signed firmware, drift detection and BIOS recovery. Built-in data and system protection, reliable detection and monitoring and solutions for rapid recovery should an issue ever arise. A PowerEdge purchaser is not just buying a server, they’re also getting a comprehensive, security-oriented feature set that is intrinsic to the product itself.

Storage

The operating system code in Dell’s storage appliances has been hardened to help ensure that all sensitive data remains secure.

These platforms include features such *as multi-factor authentication, role-based access controls and data at rest or in-flight encryption, among others.*

For **key management,** we offer in-house solutions like CloudLink, options to integrate with a customer’s existing key management and the flexibility to use a local key management store.

Secure Development Lifecycle and Supply Chain Security

Intrinsic security goes beyond technological features built into our products. Dell also manages internal processes designed to ensure the highest level of security for the products that reach our customers.

Dell Secure Development Lifecycle defines security controls for hardware and software development and is governed by an internal team. This team collaborates through several industry standard bodies to ensure best practices. Dell’s suppliers also agree to a set of requirements with Dell to help ensure security throughout the sourcing cycle.

Dell Supply Chain Security ensures that the security, integrity, quality and resilience of our products remains intact. Dell has implemented cutting-edge programs across the full spectrum of supply chain risk—from our threat-informed product designs, to training our tens of thousands of developers on secure development practices, to securing our factories, to logistics security programs, all the way through to post-delivery support and services.