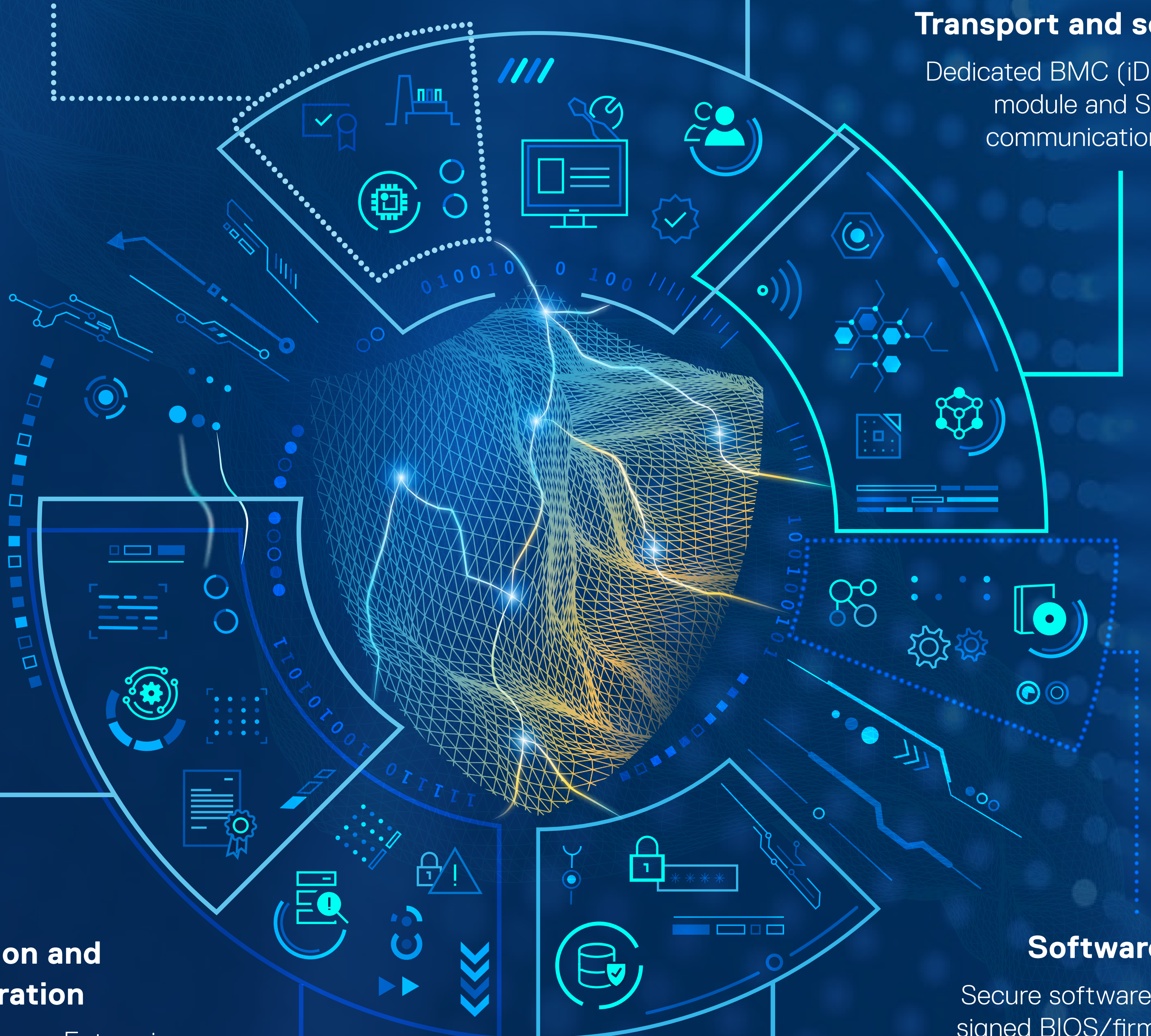
DELL Technologies

Zero Trust. Verified Trust.

Meet the challenge of ever-changing threats
with the new standard in cybersecurity.

The complexity of the modern IT infrastructure along with the sophistication of today's threat landscape requires a trust model that validates at every point in the IT environment before permissions are granted.



Device trust

A silicon-based hardware root of trust — the foundation of device trust and part of a deliberate cyber-resilient architecture. Supply chain security from design through manufacturing to delivery is now enhanced with component verification.

User trust

Multifactor authentication (MFA) via the Integrated Dell Remote Access Controller (iDRAC) using RSA SecureID, Active Directory or LDAP integration with SSO support along with role-based access control and auditing

Transport and session trust

Dedicated BMC (iDRAC) network module and SSH/TLS communication options

Software trust

Secure software development, signed BIOS/firmware updates, secure E2E boot and UEFI boot capabilitie, and drift detection plus automatic BIOS and OS recovery

Data trust

Data-at-rest encryption, scalable key management and confidential compute with data-in-use protection

Visibility and analytics

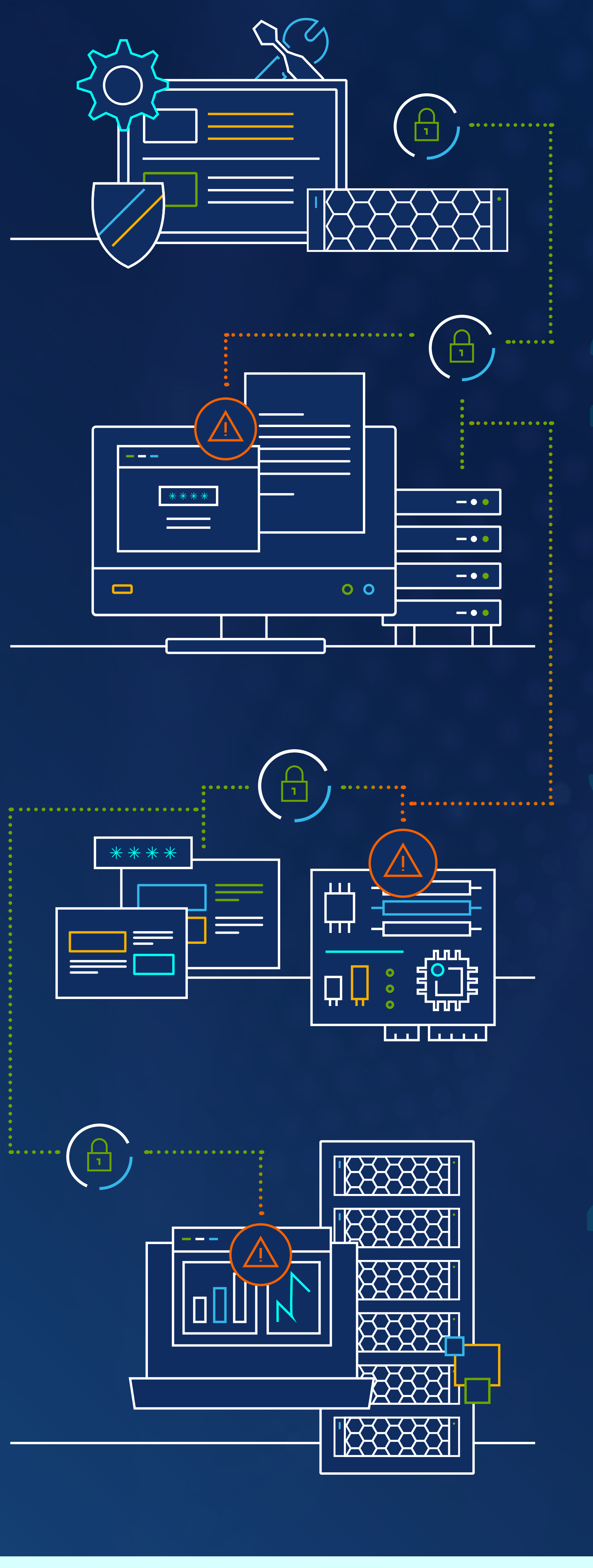
Persistent event logging/auditing and security alerts along with the Dell vulnerability responses team provides timely mitigations to any vulnerabilities found in the wild.

Automation and orchestration

Dell EMC OpenManage Enterprise drift detection and firmware rollback, centralized updates, automatic SSL certificate renewal and automated deployments for security configuration consistency

Zero trust is integral to the Dell Technologies infrastructure end-to-end lifecycle.

The Dell Technologies approach to security is intrinsic in nature — it is built in, not bolted on. It is integrated into every phase of the server lifecycle — from design to manufacturing through use and end of life. We continue to innovate to meet the ever-growing threat landscape.



1 Design and develop

Dell Technologies Security Development Lifecycle (SDL) prioritizes cyber resilience and zero trust from the time features are conceived and designed through production and maintenance. This provides assurance to the customer that servers are resilient at their foundation.

2 Manufacture and deliver

The 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.

With the newly released Secured Component Verification program, customers augment zero trust with cryptographic verification of devices. This ensures that a system built in a Dell Technologies factory has the same components as the one that arrives at the customer's site.

3 Deploy and maintain

Security controls and comprehensive management tools enable zero trust deployments using robust layers of security across hardware and firmware in the areas of:

- Expanded root of trust: immutable platform root of trust, integrity attestation
- End-to-end verified boot: cryptographically-verified trusted boot
- Advanced data protection: encryption and key management of data at rest, data in flight and data in use
- Secure server lifecycle: multifactor authentication, system lockdown, drift detection, comprehensive event logging and vulnerability rapid response

4 Retire and repurpose

Zero trust should extend all the way to system end of life. Systems need to be taken out of production securely to avoid data compromise and misuse. System erase eliminates nonvolatile stores in memory and storage devices including, logs, configuration data, storage data and cache so that no confidential information is compromised. Customers can also take advantage of Dell Technologies Data Sanitization Services.

Tenets of zero trust

Zero-trust architecture is built around a set of principles that presumes the network is always vulnerable to compromise — in some way — and sets out to safeguard access to critical data and resources.[1]

- ✓ **Assume every user and device is a potential threat**.
- ✓ **Apply the principle of "least privilege"** to restrict users (and their devices).
- ✓ **Apply multifactor authentication models** and authorization rights that are time based, scope based, role based, etc.
- ✓ **Authenticate and authorize** at communication intersections of the infrastructure.
- ✓ **No entity is inherently trusted**, and verification is required to access all assets.

Don't be a victim.

Ransomware is malware that identifies critical data in your network and encrypts it until a ransom is paid. Variants threaten to release the sensitive data to the public. This is cyber-extortion, and it has organizations moving to a zero-trust model to secure their IT infrastructure.

But not all threats are malware. Threats can come from anywhere, and it is critical to secure all aspects of the enterprise network from the edge to the endpoint, data center and cloud. Dell Technologies has security built into our industry-leading servers, storage, HCI and data protection appliances to help protect data wherever it is stored, managed or used.

Zero trust: The new standard in cybersecurity

In the wake of a rash of bold cyberattacks and ever-evolving risks that have targeted everything from the national energy grid to the food supply chain, organizations are going back to the fundamentals of information security. Unlike trust-then-verify frameworks, **the zero-trust approach performs verification before it trusts a user, or device, and grants access**. The Dell Technologies zero-trust approach has been refined to align with the U.S. Department of Defense (DoD) standards and, in the near future, government agencies, their vendors and those in heavily regulated industries — like infrastructure, transportation, energy, healthcare and banking — can expect more scrutiny to be placed on them to comply with zero-trust security specifications.

Learn more about cyber-resilient Dell PowerEdge servers.

Visit DellTechnologies.com/Servers or our Infohub.

[1] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly, Zero Trust Architecture, NIST Special Publication 800-207, August 2020.

Published in the USA 01/22 Infographic

Dell Technologies believes the information in this document is accurate as of its publication date. The information is subject to change without notice.