End-to-End Server Security: The IT Leader’s Guide for the Next Decade

A business white paper by the Dell EMC PowerEdge Server Group
Executive Summary

As enterprises continue on the IT transformation journey, all too often business leaders struggle to place sufficient focus on server security. If server security is not prioritized higher, the datacenter offers a myriad of security vulnerabilities and will become a prime target for malicious attacks. This best practice paper offers business leaders a framework to assess whether their vendors are “Security Leaders” or “Security Laggards.”

End-to-end security is the essential foundation of a successful IT Transformation and we discuss how Dell EMC PowerEdge servers are uniquely designed to support this. Further, we provide key questions every CIO, CISO, and IT leader should pose to their server vendor. These questions will inform your decision when choosing a server vendor, particularly where security is a top concern.

This paper is organized into sections describing the importance of IT infrastructure security and presents essential criteria IT leaders should use to identify end-to-end server security.

1. **Trust and the Modern IT Infrastructure**
   Why you should be concerned about server security and the pitfalls of lax security.

2. **End-to-end Server Security**
   How Dell EMC defines end-to-end server security.
   In this section, we also provide crucial characteristics business and IT leaders can use to classify prospective server vendors.

3. **Key Security Criteria for the Modern IT Infrastructure**
   The security questions every IT leader should ask of their server vendor before investing more on an IT transformation.

4. **Conclusion & Additional Resources**

The objective of this paper is to highlight the Dell EMC comprehensive approach to server security. PowerEdge servers come with security designed and built-in, not bolted-on. Using a Cyber Resilient Architecture, Dell EMC commits to end-to-end server security on all PowerEdge servers. That means we focus on often-overlooked security features at the firmware and hardware level. In addition, PowerEdge servers come with standard-setting security spanning the IT security lifecycle according to the most current NIST Cybersecurity Framework. On a PowerEdge server, security is a standard, not just a set of features.
Trust and the Modern IT Infrastructure

Corporate leaders know their organizations must digitize or die. With the proliferation of smart devices, connected sensors and the constant need for data-driven insights, IT has moved from back office functionality to executive strategy. IT Transformation begins with a modern IT infrastructure. Modernizing IT is about building from the foundation up. It’s about building new types of infrastructures which will securely support the workloads driving your business today, as well as the new workloads driving your business tomorrow. According to Forrester, “As malicious invaders develop new ways to bypass security systems, organizations must adapt their security strategies to avoid vulnerabilities to hardware-level security breaches.”

Servers form the foundation of the modern IT infrastructure – running a variety of workloads from databases to software-defined storage. As a result, compute power has become even more central to success in the digital economy. Thus, servers are becoming a prime target for malicious attacks. Servers are also highly subject to inadvertent security mishaps because server security is often overlooked or neglected by businesses. While your company is in the midst of an IT transformation, it is critical to consider how your IT provider is ensuring end-to-end server security BEFORE entering into any economic agreement. Even if you’re simply adding additional compute capacity or refreshing your servers, security needs to be a top consideration. But before exploring the HOW of IT infrastructure security, let’s first examine the WHY.

Many businesses realize the importance of security within IT. In the most recent Harvey Nash / KPMG CIO survey of 4,219 CIO’s and technology leaders, 52% report being ‘very’ or ‘extremely’ effective at embedding risk and security in their IT projects, yet 47% named security & privacy as a top area of technology investment their corporate management board is looking for IT to address. In the same study, 35% of the respondents consider cyber-security as the scarcest skill in their available workforce.2

...Organizations must adapt their security strategies to avoid vulnerabilities to hardware-level security breaches.”
– Forrester

---

Source: 2020 Harvey Nash/KPMG survey of 4,219 CIO’s and technology leaders
Aligned with these concerns are key statistics from customers and companies focused on digital experiences. In the 3rd edition of the State of the Connected Customer by Salesforce Research, conducted with 8000 consumers and business buyers worldwide, 41% of consumers don’t believe that companies care about the security of their data, while 84% of the same consumers said they are more loyal to companies that have strong security controls. This is very telling, considering that 63% of companies have experienced a data compromise or breach within the past 12 months due to an exploited vulnerability in hardware- or silicon-level security. The impact of COVID-19, particularly in the United States, is raising the awareness of data privacy, data security, and will certainly have a long standing effect on end-to-end server security in the datacenter.

What is End-to-End Server Security?

A secure server is difficult to identify if you don’t know WHAT you’re looking for. In fact, the server and its security features don’t offer adequate information to determine whether or not the server is protected with end-to-end security. Determining the server’s security level is more about the vendor or manufacturer and how their design, engineering, and manufacturing processes integrate security. It’s also about whether the supply chain is secure from end-to-end and can be validated in some manner. A server with embedded end-to-end security will typically contain some, if not all, of the features listed in Exhibit 1. Use this list as a guideline when trying to determine if your servers are adequately secure. To fully understand whether your IT infrastructure is secure, you need to evaluate not only the server itself, but also your chosen IT partner or server vendor.

The server and its security features don’t offer adequate information to determine whether or not the server is protected with end-to-end security.
**Key End-to-End Security Features**

<table>
<thead>
<tr>
<th>Security Phase</th>
<th>What to look for</th>
<th>Dell EMC PowerEdge Security Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect</td>
<td>Dual Silicon Root of Trust: An immutable silicon-based root of trust to securely boot iDRAC and BIOS/firmware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cryptographically Signed Firmware: Allows only Dell EMC approved firmware to be accepted across critical components. Thwarts injection of malicious code along the product lifecycle. Can be customized for higher security requirements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iDRAC: Logs events across all server components and provides alerts including recommended actions. Monitoring continues even when the server is powered off.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion Monitoring: On-board sensors detect when the server chassis is opened or tampered with. Physical security events are reported in the iDRAC Lifecycle Log once power is applied. Secured Component Verification: Validation of “as-built” hardware configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rapid Recovery: PowerEdge servers have built-in functionality to restore to a Pristine BIOS and to a pre-configured &amp; pre-installed redundant copy of OS image.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Easy Restore: Restores server state quickly after a motherboard replacement. Focuses on server configuration, iDRAC licenses, service tag and diagnostics.</td>
<td></td>
</tr>
</tbody>
</table>

**The two categories of server manufacturers**

Server vendors can be defined in two categories, in category A is what we’ll call the “Security Leaders.” You may also see Security Leaders labeled as Hardware Partners. Security Leaders are companies who have been focused on IT infrastructure security before it was even on the radar of IT professionals or corporate boards. Security Leaders are keenly aware and hyper-focused on the issue of firmware and hardware security, discussed above. They understand that firmware and hardware vulnerabilities, while often overlooked by end users, represent a dangerous entry point for would-be hackers. Therefore, they will have direct control over critical firmware like the Unified Extensible Firmware Interface (UEFI) and baseboard management controller (BMC). Security Leaders will also control the customization of the silicon where these features run on. Security Leaders control the server development process from design to manufacturing and provide integrated security features across the security lifecycle – in every server. Finally, Security Leaders believe server security and peace of mind should come standard.

**Security Leaders:**
- Focused on firmware and hardware security
- Direct control over critical firmware
- Use customized silicon chips from vetted manufacturers
- Control server design and development process
- Provide security features across the security lifecycle

**Security Laggards:**
- Tend to be followers in feature innovation
- Few to zero security features
- Little to no control over the supply chain
- Depend on third-party non-customized silicon chips
- May charge a licensing fee for standard security features
In category B are the “Security Laggards,” also known as a Hardware Provider. Server vendors within this category can often be found following Security Leaders in terms of security feature innovation.

Or, in the interest of cutting costs, they may not even bother with security features at all. A Security Laggard will have little to no control over the manufacturing supply chain, which introduces hardware and firmware security vulnerabilities into the server ecosystem. Original design manufacturer (ODM) server vendors fall within this category. They depend on third-party software and third-party off-the-shelf chips – so by definition Security Laggards do not control the server development process from design to manufacturing. Ultimately, you can identify a Security Laggard because they view and treat security as the responsibility of the end-user. They’ll often charge a security licensing fee for security features that should be standard. If you go with one of these vendors, be prepared to shoulder the entire burden of IT infrastructure security.

**Key Security Criteria for the Modern IT Infrastructure**

Now let’s move on to **HOW** you ensure your datacenter is fully secure, from end-to-end, from silicon to system. Dell EMC has identified four key questions every CIO, CISO, or IT leader needs to ask of their server vendor when continuing or embarking on an IT transformation. If you get the right answers back, then your IT infrastructure is secure enough to support a successful IT transformation. But if your IT partner can’t answer these questions or doesn’t conform to the standards listed below, it’s time to consider making a change.

**Question #1:**

**How are you ensuring server security at the firmware and hardware level?**

Many IT organizations focus on cybersecurity concerns such as protecting the network, data, operating system and applications, but less attention is devoted to the underlying server infrastructure including hardware and firmware. In addition, as IoT devices proliferate, firmware, operating system and app functionality become intimately intertwined; the differentiation starts to blur.

Dell EMC is on the forefront of informing the market about vulnerabilities in server firmware and hardware security. We’ve been focused on firmware and hardware security going back many years. IT security professionals know that no system is completely foolproof, thanks to the endless ingenuity of would-be hackers. Every server in your IT infrastructure should be equipped with the following in order to protect against attacks on the server’s hardware and firmware.

- **Silicon root of trust**
  - Dell EMC has chosen a dual approach to the silicon root of trust; the BIOS/OS domain is independent from the iDRAC domain.
  - In contrast to Security Laggards, Dell EMC works with extensively vetted silicon chip manufacturers to customize the chip and build in this root of trust technology.
• Basic Input/Output System (BIOS) security
  » The Dell EMC PowerEdge servers contain innovative features which offer new ways to protect and recover the BIOS, ensuring full integrity throughout the server lifecycle.
  » Intel Boot Guard and BIOS Recovery are a demonstration of the Dell EMC engineering commitment to the security and stability of your enterprise infrastructure.
  » PowerEdge UEFI Secure Boot Customization is the latest innovation to ensure only authorized firmware and operating system bootloaders are initialized.

• Physical security
  » PowerEdge servers provide hardware intrusion detection and logging, with detection working even when no AC power is available.
  » Physical I/O ports such as USB inputs can be dynamically disabled via iDRAC. This permits the disableness of these ports for production use but also temporarily grants access for crash cart debugging without rebooting the server.
  » PowerEdge servers come with lockable bezels and lids, as well as sensors that detect when anyone opens or tampers with the chassis. Servers that have been opened while in transit generate a log in the iDRAC lifecycle log once power is applied.
  
    PowerEdge servers also have an embedded hardware inventory, cryptographically signed at the factory, that can be used to verify the “as-built” hardware configuration upon delivery.

**Question #2:**
**How are my servers protected throughout the security lifecycle?**

IT infrastructure security is not a destination, it’s a never-ending journey. There’s an ongoing life cycle to every organization’s IT security journey. The National Institute of Standards and Technology (NIST) defines five core security lifecycle phases. Dell EMC maintains and simplifies the NIST framework into three key phases: Protect, Detect, and Recover. It is important for IT leaders to understand how their IT infrastructure is protected across all phases of the security lifecycle. If your server vendor is not intimately familiar with the security lifecycle, be worried. Every single server in your datacenter needs to come with dedicated security features designed for each phase: Protect, Detect, and Recover.

Dell EMC PowerEdge servers feature an enhanced Cyber Resilient Architecture that provides a security-hardened server design to Protect, Detect and Recover from server-targeted attacks. Key aspects of the Architecture are shown in Exhibit 2 and outlined below:

• **Protect:** The underlying philosophy at the Protect phase is that infrastructure assets should provide robust protection against unauthorized access to resources and data as well as tampering of critical components like embedded firmware. This includes the ability to securely verify that the as-built hardware configuration matches the inventory at delivery.
• **Detect:** It’s critical to have a detection capability providing complete visibility into the configuration, health status, and change events within the server system. Once a security event is detected, the ability to send alerts for any and all events is also essential. And these capabilities need to cover ALL server components. Dell EMC PowerEdge servers achieve comprehensive detection capabilities via the security features in Exhibit 2.

• **Recover:** IT security incidents are inevitable. However, the magnitude of such incidents is diminished when the right recovery protocols are in place. Server infrastructure must support recovery to a known, consistent state in response to a variety of events. The Cyber Resilient Architecture means PowerEdge servers are designed to quickly and effectively recover from a variety of security events, as outlined in Exhibit 2.

---

**Effective Protection**

- Authenticated and authorized user access controls
- Cryptographically trusted server booting
- Digitally signed firmware updates
- Digitally signed “as-built” hardware configuration
- Encrypted data storage
- Physical security and alerting

---

**Reliable Detection**

- Agent-free device management via iDRAC
- Comprehensive monitoring via iDRAC: Lifecycle Log & Activity Alerts
- Drift Detection with OpenManage Essentials systems management software
- Intrusion Monitoring to detect chassis tampering during transit

---

**Rapid Recovery**

- Rapid Response to Common Vulnerabilities and Exposures (CVE’s)
- Two levels of system recovery: Rapid OS Recovery & BIOS Recovery
- Firmware Rollback to restore to trusted system state
- Easy Restore to automatically return to the server’s last known configuration, iDRAC license, and security policies after hardware servicing
- System Erase to erase sensitive data and configuration settings before a system is retired or reused

---

Exhibit 2: Dell EMC Cyber Resilient Architecture
Question #3: How does your product development process integrate security?

For server vendors in the “Security Laggards” category, you may get a blank stare when you ask this question. Delivering the Cyber Resilient Architecture requires security awareness and discipline at each stage of development and it isn’t cheap or easy. At Dell EMC, this process is called the Security Development Lifecycle (SDL) model, in which security is not an afterthought but is an integral part of the overall server design process. This design process encompasses a view of security needs through the entire server lifecycle, as bulleted below and as depicted in Exhibit 3:

• Features are conceived, designed, prototyped, implemented, set into production, deployed and maintained, with security as a priority criterion
• Server firmware is designed to obstruct, oppose and counter the injection of malicious code during all phases of the product development lifecycle
• For critical technologies, external audits supplement the internal SDL process ensuring firmware adheres to known security best practices
• Continuous testing and evaluation of new potential vulnerabilities using the latest security assessment tools
• Rapid response and reporting to customers of critical Common Vulnerabilities and Exposures (CVE’s) including recommended remediation measures if warranted

Security is not an afterthought but is an integral part of the overall server design process.
Conclusion

Business leaders charged with implementing IT transformation must begin with modernizing their IT infrastructure. A critical step in this modernization is to implement a secure IT infrastructure. Investing in a modern IT infrastructure that’s not secure from end-to-end is equivalent to buying a new Ferrari and leaving it unlocked in the driveway instead of locked and protected in the garage. PowerEdge servers are the bedrock of the modern data center and security on a PowerEdge server is built-in, not bolted on. Dell EMC commits to end-to-end security on every PowerEdge server – beginning at the firmware and hardware level and spanning the IT security lifecycle.

The stakes for IT leaders are high, and the risks of inadequate IT infrastructure security include job insecurity, reputational damage, and monetary damage. Because of this, every IT leader or CIO needs to challenge their server vendor to ensure end-to-end security. Here are the four questions to ask your server vendor.

1. “Are your servers secure at the hardware and firmware level throughout the supply chain?”
2. “Are your servers secure across the security lifecycle?”
3. “Is security embedded in the product development process?”

By asking these questions, IT leaders and CIO’s can set themselves on a path for successful IT transformation.

Additional Resources
Dell EMC PowerEdge Server Security – In Depth

- Dell EMC Direct from Development Tech Note: Data Security by using the System Erase feature of iDRAC9 on PowerEdge Servers
- Dell EMC Direct from Development Tech Note: Security in Server Design
- Dell EMC Direct from Development Tech Note: Cyber-Resiliency Starts at the Chipset and BIOS

4 “Match Present-Day Security threats with BIOS-Level Control” Forrester Consulting, Thought Leadership Paper commissioned by Dell, 2019
5 Note: 14th Generation PowerEdge servers also support AMD Secure Boot: https://www.delltechnologies.com/en-us/servers/amd.htm

Discover more about PowerEdge servers

Learn more about our systems management solutions
Search our Resource Library
Follow PowerEdge servers on Twitter
Contact a Dell Technologies Expert for Sales or Support