DELL EMC

WHITE PAPER

END-TO-END SERVER SECURITY: THE IT LEADER'S GUIDE

A business white paper by the Dell EMC PowerEdge Server Solutions Group

Executive Summary

As enterprises embark on the IT transformation journey, all too often business leaders fail to place sufficient focus on server security. If security is neglected, the datacenter offers a myriad of security vulnerabilities and can become a prime target for malicious attacks. This best practices paper offers business leaders a framework to assess whether their vendors are "Security Leaders" or "Security Laggards." End-to-end security is one of the essential building blocks of a successful IT Transformation and we discuss how 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 ought to inform your decision when choosing a server vendor, particularly if security is a top concern.

PowerEdge Servers come with security built-in, not bolted-on.

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 (or the lack thereof).
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 embarking 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 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 NIST Cybersecurity Framework. On a PowerEdge server, security is a standard, not just a set of features.

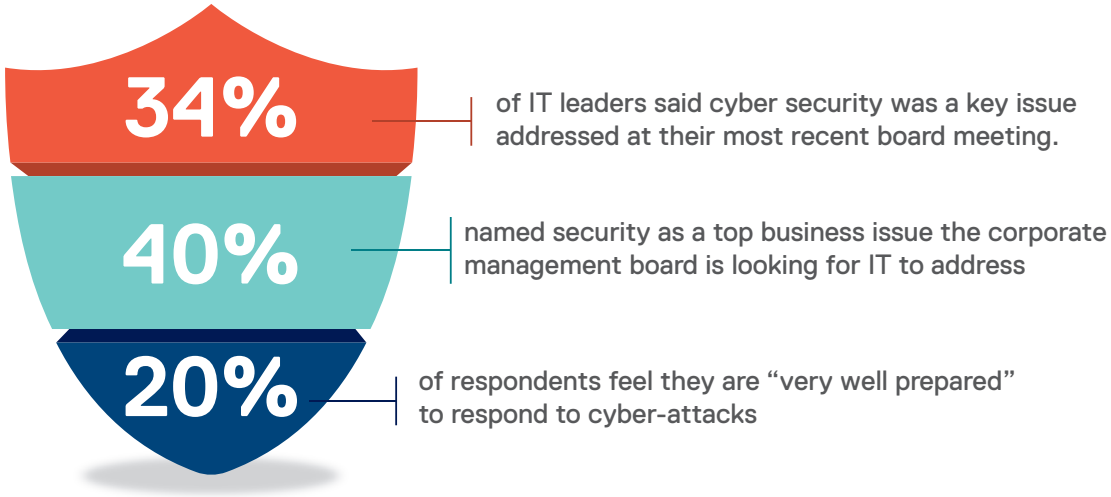
Trust and the Modern IT Infrastructure

Corporate leaders know their organizations must digitize or die. With the proliferation of smart devices, connected sensors and the constant and insatiable 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 continue to support the workloads driving your business today, as well as the new workloads which will drive your business tomorrow. According to Gartner, "A digital business is event-centric, which means it must be continuously sensing and adapting. The same applies to the security and risk infrastructure that supports it, which must focus on deceiving potential intruders and predicting security events."[1]

A digital business is event-centric, which means it must be continuously sensing and adapting.

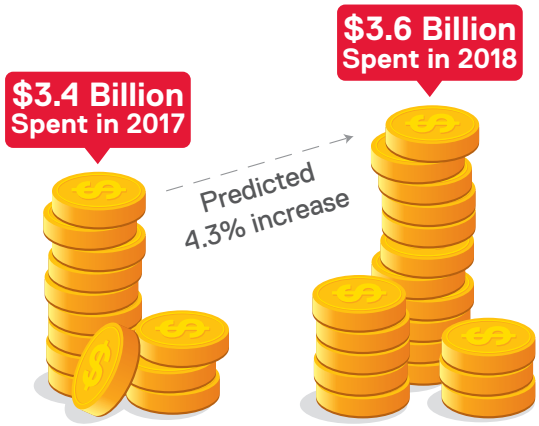
Servers form the foundation of the modern IT infrastructure – running a variety of workloads from databases to software-defined storage. As a result, compute power has become even more central to success in a digital economy. Thus, servers are becoming a prime target for malicious attacks. Servers are also highly subject to inadvertent security mishaps because server security is often overlooked or neglected by businesses. If 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**.

Most businesses realize the importance of security within IT. In a 2017 KPMG survey of 4,498 CIO's and technology leaders, **40%** named security as a top business issue the corporate management board is looking for IT to address. In the same study, 34% of IT leaders said cyber security was a key issue addressed at their most recent board meeting. Yet, only 20% of respondents feel they are "very well prepared" to respond to cyber-attacks.[2] Gartner's most recent IT spending forecast predicted $3.6 billion will be spent on IT resources in 2018, up 4.3% from 2017.[3] However, on average only 5.9% of a company's IT budget is being spent on security.[4] For most businesses, the level of concern does not match the level of preparedness and spending on IT security.



Source: 2017 KMPG survey of 4,498 CIO’s and technology leaders

IT BUDGET 2017

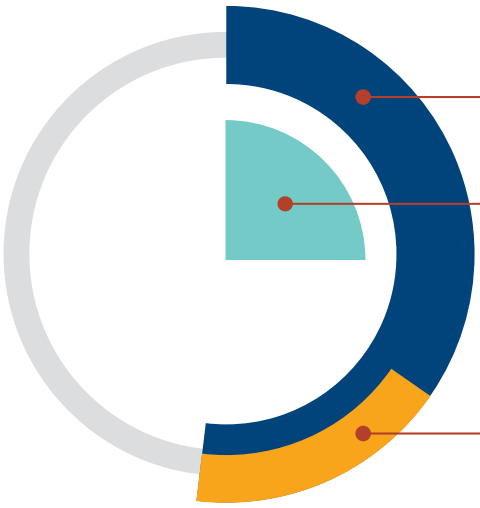


MONEY SPENT ON IT RESOURCES

Source: Gartner’s IT spending forecast

A testament to this neglect is the dearth of industry research related to hardware/firmware security, and in particular server security. In 2016, ISACA conducted a survey of IT security professionals on the topic of hardware and firmware security.[5] They attempted to identify how many firmware attacks are occurring and what is being done to reduce enterprise risks from targeting firmware. The results show most respondents do not have a holistic program to address firmware vulnerabilities within their IT infrastructure. More than 25% are not monitoring, measuring, or collecting firmware data or are unsure if their enterprises are doing so. More than half (52%) of the study’s participants who place a priority on security within hardware life cycle management report at least one incident of malware-infected firmware being introduced into a company system, with 17% indicating the incident had a material impact.

2016
ISACA Survey of IT Security Professionals



52% of the participants who do place a priority on security within hardware life cycle management report at least one incident of malware-infected firmware being introduced into a company system

More than 25% are not monitoring, measuring, or collecting firmware data or are unsure if their enterprises are doing so

17% reveal the incident had a material impact

Source: ISACA survey of IT security professionals on hardware and firmware security, 2016.

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. However, a server with embedded end-to-end security will usually contain the features listed in Exhibit 1. Use this list as a guideline when trying to figure out whether 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

Security Phase	What to Look For	Dell EMC PowerEdge Security Advantage
	Silicon-based security	Dual Silicon Root of Trust: An immutable silicon-based root of trust to securely boot iDRAC and BIOS/firmware.
	Signed Firmware Updates	Cryptographically-Signed Firmware: Allows only Dell EMC approved firmware to be accepted across critical components. Thwarts injection of malicious code along the product lifecycle.
	Always-on Monitoring	iDRAC: Logs events across all server components and provides alerts including recommended actions. Monitoring continues even when the server is powered off.
	Physical Security	Intrusion Monitoring: 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.
	BIOS & OS Recovery Feature	Rapid Recovery: PowerEdge servers have built-in functionality to restore to a Pristine BIOS and to a pre-configured & pre-installed redundant copy of OS image.
	Automatic Configuration Recovery	Easy Restore: Restores server state quickly after a motherboard replacement. Focuses on server configuration, iDRAC licenses, service tag and diagnostics.

Exhibit 1: Key End-to-End Security Features

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 basic input/output system (BIOS) and baseboard management controller (BMC). Security Leaders will also control the customization of the silicon 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. So if you go with one of these vendors, be prepared to shoulder the burden of IT infrastructure security on your own.

Key Security Criteria for the Modern IT Infrastructure

Now let's move on to **HOW** you ensure your datacenter is 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 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. Hardware and firmware are less-frequent targets, but given the current state of hardware/firmware security, it's only a matter of time before malicious players wise up to the fact that many of these components contain vulnerabilities.

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

Dell EMC is on the forefront of informing the market about vulnerabilities in server firmware and hardware security.

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. Still, 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 utilizes an immutable, dual silicon root of trust to cryptographically assure BIOS and iDRAC firmware integrity and booting on all 14th generation PowerEdge servers.
  - 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 14th generation of PowerEdge servers contain innovative features which offer new ways to protect and recover the BIOS, ensuring platform integrity throughout the full server lifecycle.
  - Intel Boot Guard[6] and BIOS Recovery are a demonstration of our engineering commitment to the security and stability of your enterprise infrastructure.
- **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 disablement 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.

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.[7] 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 sever 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.

IT infrastructure security is not a destination, it's a never-ending journey.

Dell EMC 14th generation 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.
- **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.

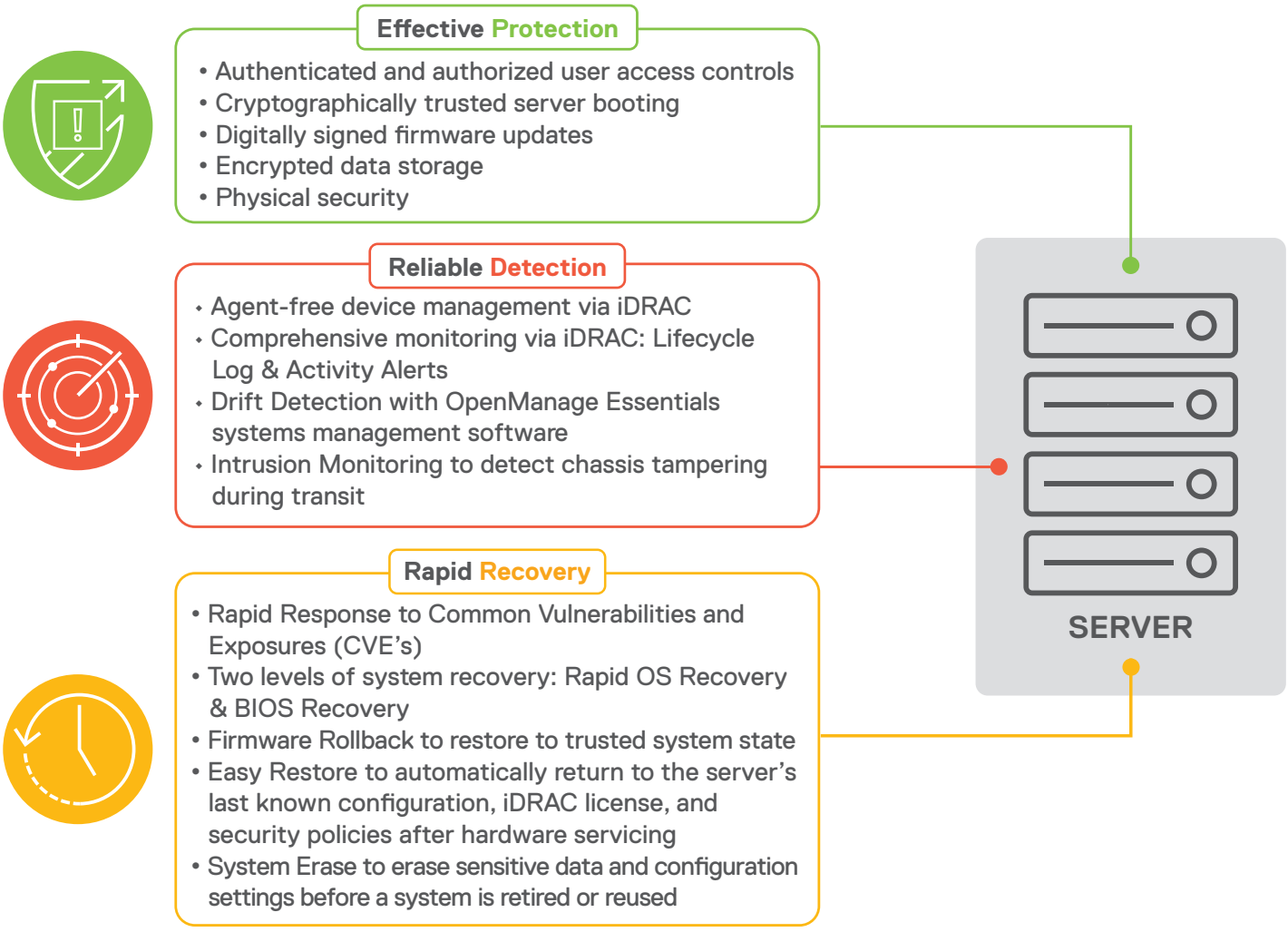


Exhibit 2: Dell EMC Cyber Resilient Architecture

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 criteria
- 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

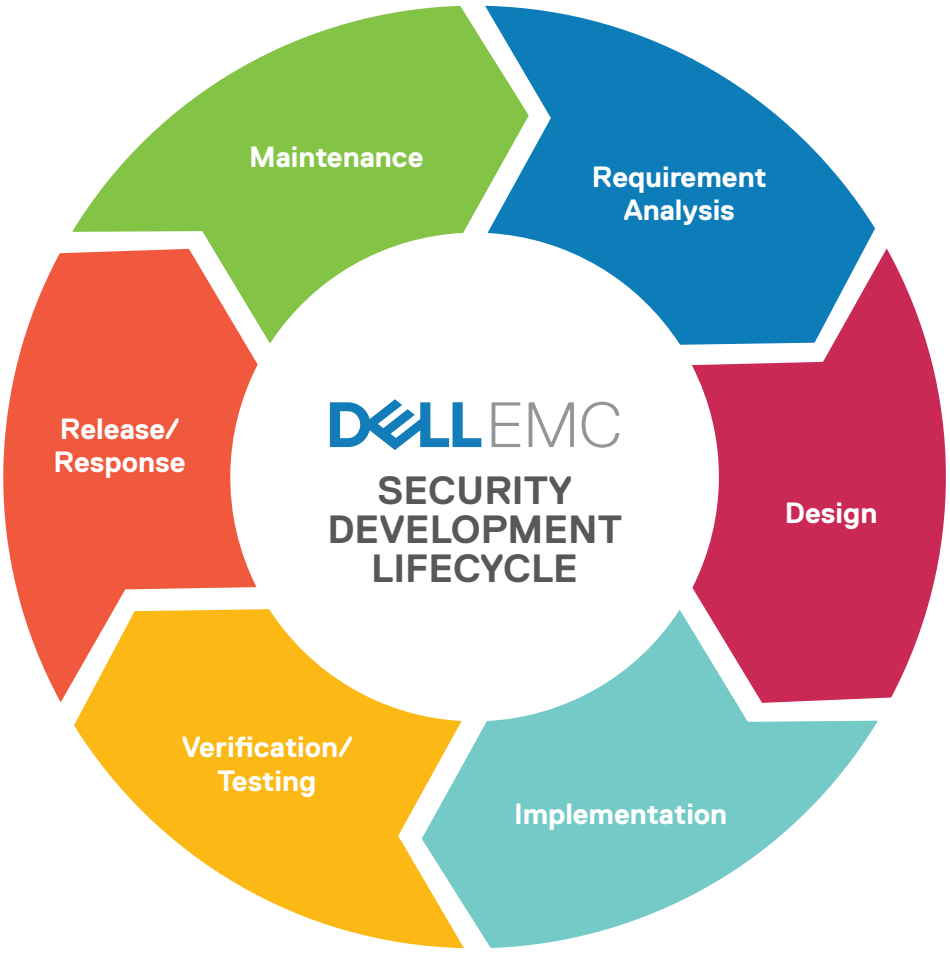


Exhibit 3: Dell EMC Security Development Lifecycle

Question #4: How do you price key security features?

This is admittedly a trick question. For Dell EMC, security is not a set of features to be licensed, but a constantly-evolving set of priorities which our engineers build into every PowerEdge server. Dell EMC believes security is fundamental to everyone who uses PowerEdge servers. We do not ask companies to pay a security licensing fee in order to benefit from the Cyber Resilient Architecture. What if auto manufacturers charged a yearly fee for airbags and seatbelts? Dell EMC only manufactures servers that go through the Security Development Lifecycle and meet the standards of the Cyber Resilient Architecture. The problem is, not all server vendors treat security in this way.

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

Dell EMC advises IT leaders to read the fine print. Will these servers be secure even if I don't purchase an additional security license? CIO's and CISO's need to ask this question specifically before signing on to any server purchase or refresh agreement. The end-to-end security features summarized in Exhibit 1 are base-level features that come standard on every PowerEdge server. Know how your server vendor charges for security features. Then consider carefully whether you're comfortable signing on with a vendor who doesn't provide standard security features – from Protect, to Detect, to Recover – for all customers, by default.

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?"
2. "Are your servers secure across the security lifecycle?"
3. "Is security embedded in the product development process?"
4. "Do I need to pay a licensing fee to benefit from key security features?"

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

- Enterprise Management Associates (EMA) White Paper – Dell EMC PowerEdge Servers: The Integrated Security Architecture
- Dell EMC Technical White Paper: End-to-end Security in Dell EMC 14th Generation PowerEdge Servers
- Dell EMC Direct from Development Tech Note: System Erase on PowerEdge 14G 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

[1] "Top 10 Strategic Technology Trends of 2018," Gartner, 03 October 2017:
https://www.gartner.com/document/3811368?ref=ddrec
[2] "Harvey Nash/KPMG CIO Survey 2017," Harvey Nash/KPMG, 23 May 2017:
http://www.kpmg-institutes.com/content/dam/kpmg/advisory-institute/pdf/2017/cio-survey-harvey-nash-2017-us.pdf
[3] "Forecast Alert: IT Spending, Worldwide, 3Q17 Update," Gartner, 29 September 2017:
https://www.gartner.com/document/3810569
[4] "IT Key Metrics Data 2017: Key IT Security Measures: by Industry," Gartner, 12 December 2016:
https://www.gartner.com/document/3524617?ref=solrAll&refval=194212569&qid=c3e5998670a94b9eee7d2a4d5222ea60
[5] "Firmware Security Risks and Mitigation: Enterprise Practices and Challenges," ISACA, 18 October 2016:
http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/firmware-security-risks-and-mitigation.aspx
[6] 14th Generation PowerEdge servers also support AMD Secure Boot
[7] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 10 January 2017:
https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

Learn more about Dell EMC PowerEdge solutions

Contact a Dell EMC Expert

View more resources

Join the conversation on Twitter @DellEMCServers with #PowerEdge