PowerEdge Product Group

Direct from Development

Security in Server Design

Tech Note by:
Rick Hall
Mukund Khatri
Tad Walsh

SUMMARY

Server security is critical for securing the IT infrastructure. While much customer focus on cybersecurity concerns protecting the OS and applications, less attention is devoted to the underlying server infrastructure including hardware and firmware.

The importance of server security can't be overstated: Cyber intrusions and attacks can result in system and business downtime, lost revenue, lost customers, corrupted data, the inability to comply with government regulations for data protection, and damaged corporate reputation.

To protect, detect and recover from cyber attacks, security is built into the PowerEdge server design, not bolted on after the fact.

PowerEdge server security: Built-in, not bolted on

User conversations, the trade press, and market research all indicate that IT security is a key and growing area of concern among customers ranging from IT Administrators to the C-suite. The potential for system downtime, lost productivity, lost revenue, corrupted data and damaged corporate reputation are all reasons for the increased concern. However, while cybersecurity is increasingly top of mind for many IT managers, most of the focus is on protecting the OS and applications from malicious attacks; little thought or planning is given to how secure the underlying server infrastructure is including the hardware and the firmware as shown in Figure 1:

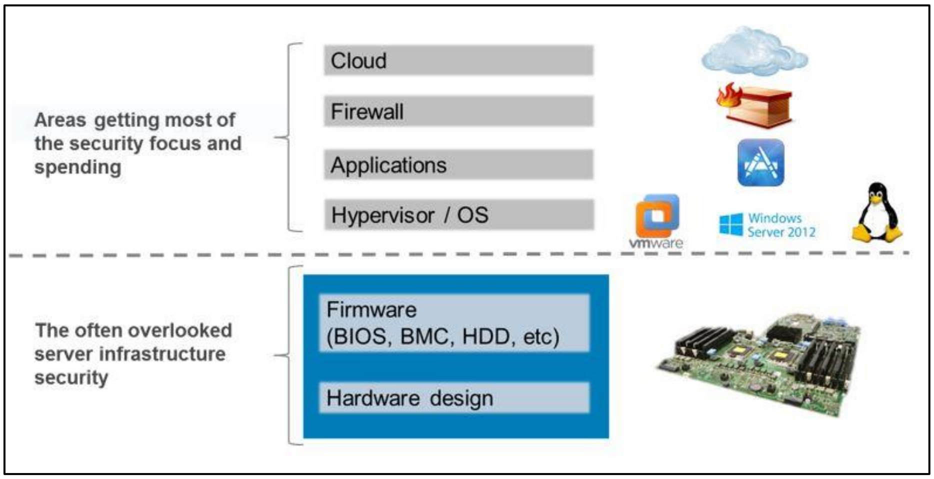
Areas getting most of the security focus and spending
Cloud
Firewall
Applications
Hypervisor / OS
vmware
Windows Server 2012
The often overlooked server infrastructure security
Firmware (BIOS, BMC, HDD, etc)
Hardware design

Figure 1: Server Infrastructure is Critical to Data Center Security

The overlooked reality is that server infrastructure is also key to data center security, since cyber attacks targeting firmware can be persistent, stealthy and very damaging. Thus, in addition to the above areas of focus, IT security strategies should consider critical areas of server hardware design, on one hand, and firmware, on the other. In this context, server firmware includes several components, including BIOS, the baseboard management controller (iDRAC in the case of PowerEdge), hard drives and networking adaptors as examples.

Enhanced Cyber Resilient Architecture

PowerEdge servers have featured robust security for several generations, including the innovation of using silicon-based security and cryptographic root of trust to authenticate server booting and firmware updates. These features align with security standards such as NIST SP800-147B and UEFI Secure Boot. Dell EMC 14th Generation PowerEdge servers feature an enhanced **Cyber Resilient Architecture** that provides a hardened server design to protect, detect and recover from cyber attacks. Some of the key aspects of this architecture are:

Effective Protection	○ Silicon-based Hardware Root of Trust ○ Signed Firmware Updates ○ System Lockdown ○ Secure Default Passwords
Reliable Detection	○ Configuration and Firmware Drift Detection ○ Persistent Event Logging including user activity ○ Secure Alerting
Rapid Recovery	○ Automatic BIOS Recovery ○ Rapid OS Recovery ○ System Erase

Figure 2: Key aspects of the PowerEdge 14G Cyber Resilient Architecture

Security Development Lifecycle

Delivering the Cyber Resilient Architecture requires security awareness and discipline at each stage of development. This process is called the Security Development Lifecycle (SDL) model, in which security is not an afterthought but is rather 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 Figure 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
  - ○ Threat modeling and penetration testing coverage during the design process
  - ○ 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
- 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 (CVEs) including recommended remediation measures if warranted

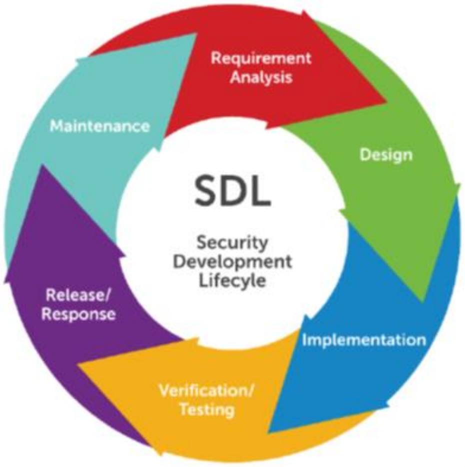

Figure 3: Dell EMC's Security Development Lifecycle

Innovative Security Features

A compelling example of Dell EMC's innovation in server security is the use of a **hardware root of trust** based in silicon. This feature anchors our Cyber Resilient Architecture that validates both iDRAC and BIOS firmware as each module is booted in a chain of trust. All firmware for critical components (NICs, HBAs, RAID, CPLD, storage drives, PSUs, etc.) is likewise validated using cryptographic signatures to ensure that only authentic firmware is running in the server.

PowerEdge servers also support **UEFI Secure Boot** which checks the cryptographic signatures of UEFI drivers and other code which is loaded prior to the OS running. These include:

- Operating System boot loaders
- UEFI drivers that are loaded from PCIe Cards
- UEFI drivers and executables from mass storage devices

In addition, 14th Generation PowerEdge servers offer customers the unique flexibility of using a customized boot loader certificate not signed by Microsoft. This is primarily a feature for Linux environments that want to sign their own OS boot loaders.

Another example of a new security feature of PowerEdge 14G servers is **System Lockdown**.

- System Lockdown helps prevent change (or “drift”) in system firmware image(s) and critical configuration data
- Lockdown mode provides a level of protection yielding higher protection against inadvertent or malicious modification of server firmware and configuration
- Lockdown mode is a feature included with the iDRAC Enterprise license
- Dell tools or interfaces that support/enforce lockdown mode are: iDRAC GUI, RACADM, WS-MAN, Redfish, DUPs, OMSA/OMSS, BIOS F2, DTK, and IPMI.
- Certain key operations such as power capping, power operations, etc. are allowed when the system is in lockdown mode
- Some 3rd party vendor tools may be able to configure their respective server components such as networking adaptors though their use is not recommended

As another example, highly relevant for hosting providers, 14G PowerEdge servers provide additional security via **Domain Isolation**, an important feature for multi-tenant, hosting environments. In order to secure the server's hardware configuration, the hosting providers may desire to block any re-configuration by the tenants. Domain isolation, new with PowerEdge 14G servers, is a configuration option that ensures that management applications in the host OS have no access to the out-of-band iDRAC service processor or to the chipset functions like Management Engine (ME) or Innovation Engine (IE).

Securing server operations via Automation

Table 1 below briefly summarizes some key actions users can take to provide additional server security. With Dell EMC OpenManage systems management tools, many of these routine tasks can be automated, which eliminates the configuration errors and security vulnerabilities that manual processes can introduce. For example, iDRAC provides robust APIs such as WS-Man or the new RESTful Redfish API to script automated deployment of hardware security features. Security policies that are not automated will typically result in errors and possible security breaches.

Table 1: Key actions users can take to provide additional server security

Control Access	Monitor	Update	Maintain
• Employ LDAP or AD for user & role authorization and authentication • Set up 2-Factor Authentication • Customize the iDRAC log-on security notice to your company's policy • Enforce stronger encryption • Restrict users to a specific source IP address range • Set a BIOS password	• Alert for unplanned configuration or firmware changes • Use SNMP v3 or Redfish eventing for secure alerting • Monitor for chassis intrusion events • Monitor mobile device ID logs associated with Quick Sync 2 usage • Monitor iDRAC logs for tracking suspicious user access behavior	• Use only Dell EMC signed firmware updates • Select HTTPS (instead of CIFS & NFS) for file transfers from update repositories • Use System Lockdown to prevent inadvertent or malicious changes to firmware	• Use the iDRAC Direct dedicated USB port to locally and securely remediate server or OS issues • Use HTML5 mode instead of Java for remote console • Use System Erase to securely and quickly wipe all user data from drives and embedded non-volatile memory • Reset configurations to factory defaults

Conclusion

Data center security is paramount to business success and the security of the underlying server infrastructure is critical. Cyber intrusions and attacks carry with them the potential for system and business downtime, lost revenue, lost customers, corrupted data, the inability to comply with government regulations for data protection, and damaged corporate reputation. To protect, detect and recover from cyber attacks, security needs to be built into server hardware design, not added on after the fact. Dell EMC PowerEdge servers are designed from the ground up according to the Security Development Lifecycle (SDL), a robust methodology that is an integral part of our overall hardware and firmware design. Many new features and capabilities that enhance and harden security are available with PowerEdge 14G servers, making them trustworthy servers that form the bedrock of the modern data center.