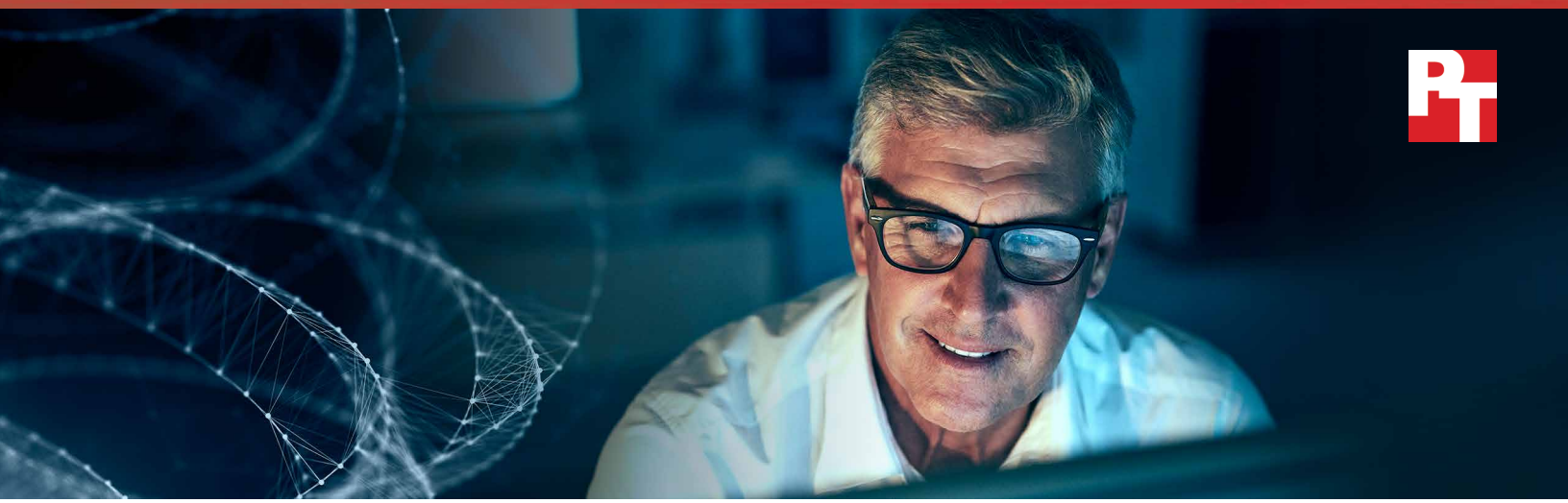


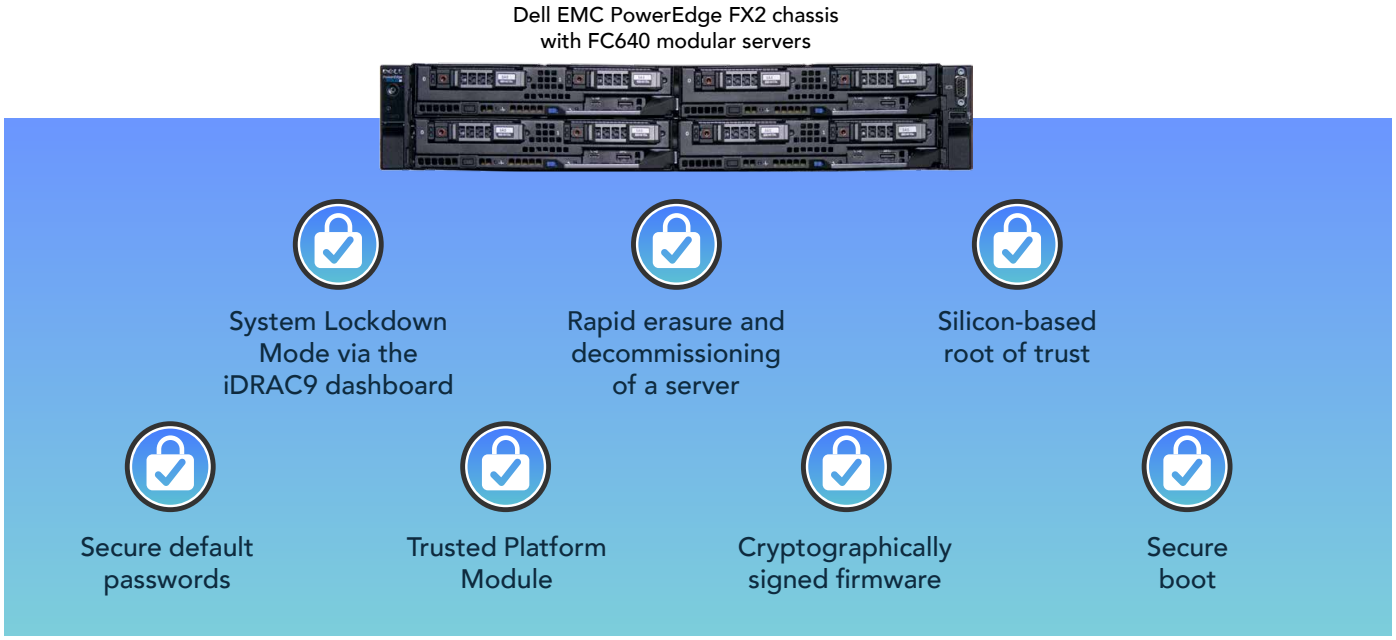
Dell EMC PowerEdge FX2 solutions offer enterprise-class server security features integrated within the platform

The security features of a Dell EMC PowerEdge FX2 solution compared favorably with those of an HPE Synergy solution

Each security feature of a datacenter solution provides a new layer of data protection that can prevent costly server downtime. Systems administrators can configure these features and use them to prevent breaches at many infrastructure points.

In our hands-on security analysis of the Dell EMC™ PowerEdge™ FX2 with Dell EMC OpenManage™ Systems Management solutions and HPE Synergy with embedded HPE OneView, we found the Dell EMC solution shared six critical security features with HPE Synergy and included one that HPE did not. In this analysis, we examined only the availability of features within each platform; we did not perform penetration or security testing on either vendor's solution.

This report explains the features we tested and how they can help secure your infrastructure.



Included features	Dell EMC	HPE
System Lockdown Mode	✓	✗
Cryptographic erase	✓	✓
Root of trust	✓	✓
Secure default passwords	✓	✓
Trusted Platform Module	✓	✓
Cryptographically signed firmware	✓	✓
Secure boot	✓	✓

Differentiating protective and restorative capabilities

Working with Dell EMC, we chose to verify a subset of six protection features and one recovery feature. The table on the left summarizes which features each solution had. To learn how we tested and what documentation we used, see the appendices at the end of this report.

System Lockdown Mode

We found the Dell EMC solution with OpenManage allows admins to enable System Lockdown Mode via the iDRAC9 dashboard. The HPE solution we tested did not have a similar feature. System Lockdown Mode prevents unauthorized changes to configuration settings and firmware, ensuring systems maintain their desired configurations while protecting the system itself and data stored on it.

System Erase

Both solutions offer rapid erasure and decommissioning of workloads running on the server. The Dell EMC solution offers a set of features within Dell Lifecycle Controller that allow IT admins to wipe configuration information, user data, and drives, rendering them unreadable by subsequent users. In addition, the Dell EMC solution features Secure Erase, which wipes the system and returns it to a default state. Secure Erase leverages Cryptographic Erase, which directs self-encrypting storage drives to destroy the current encryption key, rendering data unreadable. These features are compliant with NIST standards, and require no additional cost or license.

The HPE Intelligent Provisioning module gives IT admins the option to erase hard drives, perform a U.S. Department of Defense-compliant multi-pass wipe, and purge the system of all configuration information, including warranty and license information. HPE, however, also offers other disk erasure options within the Storage Manager application in Intelligent Provisioning. HPE SSDs offer Sanitize Block Erase, while HPE HDDs use Sanitize Overwrite, both of which meet the requirements of the NIST Guidelines for Media Sanitization. Disk encryption for HPE requires a separate license on a per-drive basis, but with it, IT admins can perform a cryptographic erase of drives. In addition, the HPE feature doesn't leverage self-encrypting drives; instead, the array controller and each disk in the array establish encryption.

Validating protection features of both solutions

The Dell EMC solution with OpenManage and the HPE solution with OneView both had comparable versions of the following security features to help protect data, applications, and users:

Silicon-based root of trust

Chains of trust validate hardware and software. Dell EMC and HPE offer a silicon-based root of trust for their firmware. Silicon-based roots ensure firmware updates originated with the vendor, rather than from a malicious third party.

Secure default passwords

Both solutions offer secure default passwords from the factory, as opposed to generic, well-known administrative credentials. For secure environments, this decreases the attack surface for an off-site attacker to gain access to sensitive servers.

Trusted Platform Module

From boot to OS execution, Trusted Platform Module (TPM)-based systems utilize a known and trusted combination of hardware and software, ensuring that unknown components have no access to low-level system code. Dell EMC and HPE leverage TPM 1.2 and 2.0 for assuring the integrity of their respective platforms.

Cryptographically signed firmware

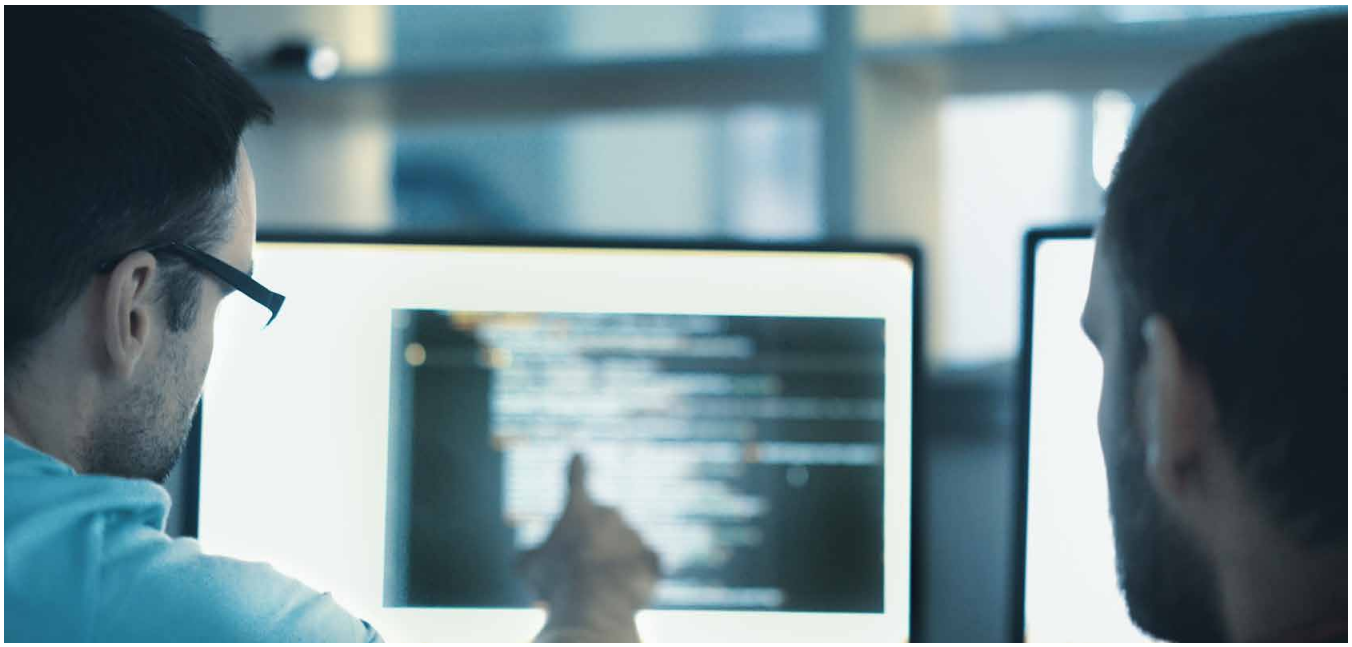
Dell EMC and HPE use cryptographically signed firmware, which ensures the system boards validate firmware using private key-based algorithms. This determines whether a firmware package is from the vendor or some malicious third party. The system will reject packages that do not have matching keys.

Secure boot

Secure boot allows firmware to check each piece of boot code, including firmware drivers, applications, and the operating system, for valid signatures prior to operation. Secure Boot systems will only boot and pass control to the operating system once they have validated all signatures. Dell EMC and HPE offer this feature.

Assessing HPE security claims

On the HPE website, HPE claims their Gen10 servers are "the world's most secure industry standard servers,"[1] citing a May 2017 paper from independent security consulting firm InfusionPoints. Because testing for that paper occurred in or before May 2017, however, InfusionPoints could not have assessed the security capabilities of Dell EMC 14th generation servers, which Dell EMC announced in May 2017 and released in July 2017.[2, 3] Given that it's based on testing that excluded the latest Dell EMC servers—and given the many security features we found in our assessment of the PowerEdge FX2—we believe the HPE claim is no longer verifiable.



Conclusion

Protecting data, applications, and users is of the utmost importance for any business. The more security features datacenter solutions can provide, the harder it can be for hackers to gain access to infrastructure. In our hands-on analysis, we found a Dell EMC PowerEdge FX2 solution and an HPE Synergy solution shared many security features. In addition, the FX2 solution offered one feature that the Synergy solution did not.

---

1 "HPE Gen10 Servers," accessed April 17, 2018, https://www.hpe.com/us/en/servers/gen10-servers.html

2 "Dell EMC Announce 14th Generation PowerEdge Servers," accessed April 17, 2018, http://www.storagereview.com/dell_emc_announce_14th_generation_poweredge_servers

3 "Press Release: Dell EMC Launches Next Generation of the World's Best-Selling Server Portfolio," accessed April 17, 2018, https://www.emc.com/about/news/press/2017/20170711-01.htm

On January 15, 2018, we finalized the hardware and software configurations we tested. Updates for current and recently released hardware and software appear often, so unavoidably these configurations may not represent the latest versions available when this report appears. For older systems, we chose configurations representative of typical purchases of those systems. We concluded hands-on testing on May 15, 2018.

Appendix A: System configuration information

Server

Server configuration information	Dell EMC PowerEdge FC640	HPE Synergy 480 Gen10
BIOS name and version	Dell 1.2.11	I42 v1.22 (09/29/2017)
Non-default BIOS settings	Legacy Boot Enabled	N/A
Operating system name and version/ build number	Windows Server® 2016 and ESXi-6.5U1 v6765664	Windows Server 2016 and ESXi-6.5U1 v6765664
Date of last OS updates/patches applied	01/15/18	01/15/18
Power management policy	Balanced	Balanced
Processor		
Number of processors	2	2
Vendor and model	Intel® Xeon® Gold 5120	Intel Xeon Gold 5120
Core count (per processor)	14	14
Core frequency (GHz)	2.20	2.20
Stepping	M0	1
Memory module(s)		
Total memory in system (GB)	16	384
Number of memory modules	2	24
Vendor and model	Hynix HMA81GR7AFR8N-VK	HPE SmartMemory 840757-091
Size (GB)	8	16
Type	PC4-2666V	PC4-21300
Speed (MHz)	2,666	2,666
Speed running in the server (MHz)	2,666	2,666
Storage controller		
Vendor and model	Dell PERC H330 Mini	HPE Smart Array P416ie-m SR G10
Cache size (GB)	2	2
Firmware version	25.5.4.0006	1.04
Driver version	N/A	N/A

Server configuration information	Dell EMC PowerEdge FC640	HPE Synergy 480 Gen10
Local storage (type A)		
Number of drives	8	1
Drive vendor and model	Dell SSDSC2BB120G7R	HPE VK000480GWCFE
Drive size (GB)	120	480
Drive information (speed, interface, type)	6Gbps, SATA, SSD	6Gbps, SATA, SSD
Network adapter		
Vendor and model	Broadcom® GbE 4P 5720 bNDC	Synergy 3820C 10/20Gb Converged Network Adapter
Number and type of ports	4 x 1 GbE	2 x 20 GbE
Driver version	25.6.52	N/A

Server enclosure

Server enclosure configuration information	Dell EMC PowerEdge FX2	HPE Synergy 12000 Frame
Number of management modules	1	2
Management module firmware revision	2.0	2.01.01
KVM module firmware	N/A	1.15
Midplane version	1.0	N/A
First type of I/O module		
Vendor and model number	Dell E14M001 1Gb Pass-Through Module	Synergy 12Gb SAS Connection Module
I/O module firmware revision	1.0	1.2.4.0
Number of modules	1	2
Occupied bay(s)	1, 2	1, 4
Second type of I/O module		
Vendor and model number	N/A	Synergy 20Gb Interconnect Link Module
I/O module firmware revision	N/A	1.08
Number of modules	N/A	2
Occupied bay(s)	N/A	3, 6
Power supplies		
Vendor and model number	Dell D1600E-S0	HPE 798095-B21
Number of power supplies	2	6
Wattage of each (W)	1,600	2,650
Cooling fans		
Vendor and model number	Dell 06ww82 Dell 0X4GJ2	Synergy Fan Module 809097-001
Number of fans	8	10

Appendix B: How we tested

Security lockdown and prevention

For this feature, we performed hands-on analysis and gathered information from publicly available documentation. Both solutions allow IT admins to manually disable Secure Shell (SSH), the web console, Simple Network Management Protocal (SNMP), and other tools. IT admins can configure both solutions for certificate mappings. IT admins activate System Security Lockdown for Dell EMC solutions in iDRAC. We confirmed for the Dell EMC solution that BIOS is inaccessible and that iDRAC won't push firmware changes while this feature is enabled.

We used the following references:

- http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/Direct_from_Developmen_Dell_EMC_PowerEdge_Security_in_Server_Design.pdf
- http://en.community.dell.com/techcenter/extras/m/white_papers/20444292/download
- https://support.hpe.com/hpsc/doc/public/display?docId=c05212310

Changing security settings on the Dell EMC PowerEdge FC640

1. Turn on or off System Lockdown Mode.
2. Log into the iDRAC of the FC640.
3. Enable or disable services.
   - To enable, select More Actions→Turn on the System Lockdown Mode.
   - To disable, select More Actions→Turn off the System Lockdown Mode.
4. Log into the iDRAC of the FC640.
5. Navigate to iDRAC Settings→Services.
6. Expand the desired service, SSH for example.
7. Change the status to Disabled or Enabled, and click Apply.

Changing security settings on the HPE Synergy 480 Gen10

1. Log into the iLO.
2. Navigate to the Security page.
3. Toggle the on/off switch to enable or disable the desired service, and click Apply.

Secure instant erase

For this feature, we performed hands-on analysis and gathered information from publicly available documentation. We could not confirm the instant System Erase feature on the Dell EMC solution because our PowerEdge FC640 modules used the PERC H330 Mini Monolithic RAID Controller, which does not support instant erase or RAID-level drive encryption. We saw no noticeable difference between the System Erase feature of Dell EMC PowerEdge servers and the similar secure erase option of the HPE Synergy. Dell EMC claims System Erase works on NVMe drives, but we were not able to confirm this as our neither our PowerEdge FC640 blades nor our FD332 storage supported NVMe drives.

We used the following references:

- http://www.dell.com/support/article/hk/en/hkbsd1/sln307626/m2-nvme-drive-does-not-complete-secure-erase-operation?lang=en
- http://en.community.dell.com/techcenter/extras/m/white_papers/20440600/download

Erasing the Dell EMC PowerEdge FC640

1. Boot the PowerEdge FC640 into Lifecycle Controller.
2. Click Hardware Configuration.
3. Click Repurpose or Retire System.
4. Select Secure Erase Disks, and click Next.
5. Click Finish, and confirm the erasure to start the operation.

Erasing the HPE Synergy 480 Gen10

1. Boot the PowerEdge FC640 into Intelligent Provision.
2. Select Perform Maintenance.
3. Select System Erase and Reset.
4. Select All Hard Drives and Wipe Hard Drives.
5. To begin the erasure, click Submit.

Root of trust

For this feature, we performed hands-on analysis and gathered information from publicly available documentation. Both solutions had certificate-based root of trust. We were not able to distinguish a difference between the features of the two solutions from a high-level view.

We used the following references:

- https://www.hpe.com/us/en/resources/servers/root-of-trust.html
- https://news.hpe.com/hpe-unveils-the-worlds-most-secure-industry-standard-servers/

Secure default passwords

For this feature, we performed hands-on analysis. Our PowerEdge FC640 modules came with default passwords, but more recent Dell systems come with individually generated passwords. The Synergy blades each had individually generated passwords.

Other features

Both solutions offered the following features, and we performed hands-on analysis for each.

- TPM 1.2/2.0 options
- Cryptographically signed firmware
- Chassis intrusion alert
- Secure boot

Changing secure boot settings on the Dell EMC PowerEdge FC640

1. Log into the iDRAC of the PowerEdge FC640.
2. Navigate to Configuration→BIOS Settings.
3. Expand Security Settings.
4. Adjust the Secure Boot settings as desired, and click Apply.

Changing Secure Boot settings on the HPE Synergy 480 Gen10

1. Boot the Synergy into the BIOS settings.
2. Navigate to Server Security→Secure Boot Settings.
3. Enable or Disable Secure Boot.
4. For advanced settings, click Advanced Secure Boot Options.
5. After configuring the desired settings, press F12.

HPE Gen10 Security Reference Guide

We referenced this HPE document during our analysis of the HPE solution:

https://support.hpe.com/hpsc/doc/public/display?docId=a00018320en_us

This project was commissioned by Dell EMC.

Facts matter.®