This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

© 2016 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

September 2016 | Rev 1.1
Dell PowerEdge 13G Server Security

Contents
Executive summary................................................................. 4
Introduction........................................................................... 5
Types of enterprise security threats ........................................... 7
Dell PowerEdge 13G enterprise security approach.......................... 8
  Dell Security Development Lifecycle ........................................ 8
  Server platform security layers ............................................... 8
Dell PowerEdge server platform threat mitigation........................ 10
  Adherence to standards and certifications .............................. 12
  PowerEdge 13G server security components ............................ 13
Dell PowerEdge server manageability and security ....................... 14
Conclusion ........................................................................... 16
Glossary ............................................................................. 17

Tables
Table 1. How Dell addresses common threat vectors ...................... 10
Table 2. Modular TPM offerings in 13G PowerEdge Servers .......... 12
Table 3. Dell PowerEdge 13G key enterprise security features ........ 13

Figures
Figure 1. IDC predictions for security products and services to consider in 2016 ............... 5
Figure 2. Enterprise server attack vectors and mitigation strategies ................. 7
Figure 3. Dell Security Development Lifecycle ................................ 8
Figure 4. Layers of security in an enterprise server platform ..................... 9
Figure 5. iDRAC8 high-level functionality .................................... 14
Executive summary

As the business world becomes increasingly digitized, the cost of cyberattacks grows apace. Security-conscious IT executives need servers with a comprehensive security framework, protection against tampering and hardware attacks that render security features inoperative, and complementary solutions that provide protection beyond the server.

The Dell PowerEdge server platform provides a robust server security foundation on which you can build your enterprise strategy. Key features of the Dell approach include the following:

- Server physical security and access control
- Processor technologies with advanced data encryption, chain of trust and attestation features and server identity protection
- Secure server management, configuration upgrades with cryptographically signed firmware and software
- Security Development Lifecycle (SDL) to ensure that hardware is trusted throughout its lifecycle and cannot be tampered with
- Data protection—for data at rest and data in flight
- Proactive Security Monitoring through the Dell Software portfolio
- Adherence to security standards and certifications
- A wide range of professional services that further support securing the IT environment

Read on to learn more about the ways that the Dell PowerEdge server platform delivers the security framework, protection and services your company needs to function securely in an environment of constant threats.
Introduction

Information has become the most important asset for many organizations. Protecting data and the underlying IT infrastructure that supports it is a paramount concern of CIOs, CISOs and IT and datacenter managers alike. Hardware choice is vital to addressing these security concerns.

IDC projects that expenditures in security management and vulnerability assessment will grow to $7.9B in 2019, with a compound annual growth rate (CAGR) of 10.9 percent for the period of the study.1 Faced with these metrics, companies must determine how best to focus their security efforts in the short term. Another IDC study2 predicts the top 10 IT security products and services to consider for 2016, their impact on the enterprise and the number of months it will take each to reach the bulk of enterprises (see Figure 1). The mitigation of supply chain risks and the implementation of tracers and tethers (bubbles 2 and 8 shown in purple in Figure 1) have enterprise-wide impact and are key areas of concern for implementing security infrastructure.

As supply chains have become increasingly complex, it has become dramatically less expensive for malicious agents to devise new threats and implement cyberattacks on them. Managing supply chain

---

security risks is critical for information systems managers, for this increased exposure to more frequent broad attacks on supply chains has the potential to disrupt business very seriously. Nevertheless, as can be seen in Figure 1, the supply chain risk mitigation products and services have the greatest impact on the enterprise as a whole. They are the most complex and costly to address, and yet are at least two years out from mainstream adoption.

As infrastructure becomes highly distributed throughout regions and geographies, traditional security approaches become more difficult to implement consistently. To address this, enterprises turn to centralized management of distributed infrastructure with policy enforcement points (PEPs), using what IDC defines as Tracers and Tethers (TnT). Tracers track data as it flows through the infrastructure while enforcing policies at PEPs. Cryptographic tethers, on the other hand, use remote attestation to validate the integrity of such workloads, data and credentials. They accomplish this using roots of trust based on trusted platform modules (TPMs), hardware security modules (HSMs) and other secure server elements. This change in approach enables the movement from centralized IT architectures to dynamic mesh-like highly distributed architectures with ephemeral zones of trust. Security becomes dynamic, meaning that security policies must be applied in real time as data and workloads move from one location to another.

Servers are the foundation of enterprise security. First, they must be secure and trusted, and they must connect with other servers in a trusted manner by building a solid chain of trust. Second, all upgrades, changes and maintenance made to the servers must preserve this security and chain of trust; this is true from deployment through maintenance and upgrades to decommissioning.

The server security features that enable TnT address the first concern, that servers are secure and trusted. To address the second concern, that the server maintains these attributes over time, vendors must use a security development lifecycle, a set of processes that span the entire server lifecycle. Recognizing these two aspects of security, Dell has adopted a forward-looking proactive approach that incorporates both into its PowerEdge server platforms.

The cornerstone of the Dell security approach is the principle of “chain of trust.” A chain of trust is established when the interconnection of individually trusted components can also be trusted. Dell applies the chain of trust principle both to Dell PowerEdge servers and to the corresponding server supply chain. At the server level, this means that Dell designs servers with security from the bottom up. Server technologies using chain of trust allow remote attestation of servers and enable businesses to create trusted and secure distributed server platforms.

The Dell PowerEdge platform mitigates server supply chain risks while efficiently implementing tracers and tethers—both of which work together to achieve robust enterprise security. Before we explore this in detail, we will first discuss the key aspects of enterprise server security. Doing so will provide a background for Dell technologies that enable servers to be secure and trusted.
Types of enterprise security threats

An attack vector is a path or means by which a threat gains access to an enterprise system to launch attacks, corrupt or gather data or deliver malicious payloads to disrupt or disable system operation. Figure 2 shows typical attack vectors to enterprise servers and mitigation mechanisms for those attacks.

**Figure 2. Enterprise server attack vectors and mitigation strategies**

<table>
<thead>
<tr>
<th>Attack vector</th>
<th>Identity spoofing</th>
<th>Unpatched software</th>
<th>Data breach</th>
<th>Tampered firmware</th>
<th>Physical tampering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigation strategy</td>
<td>Tracers, tethers, attestation</td>
<td>On-time patches</td>
<td>Encryption</td>
<td>Secure, encrypted updates</td>
<td>Intrusion prevention and detection</td>
</tr>
</tbody>
</table>

These attack vectors include the following:

1. the physical server itself and its components (disk drives, devices, etc.), all of which can be tampered with
2. the server’s identity (i.e., where it is and what it is composed of), which can be spoofed
3. rogue firmware that is installed on the server, which can affect the server’s functionality putting applications and data at risk
4. the server’s firmware and software, which may have security holes that can allow breaches and zero-day exploits if not promptly patched
5. the data in the server, which can be corrupted or accessed without permission (whether it resides in a database or in a file system)

Aside from the mitigation mechanisms in Figure 2 (shown in blue text), it is also necessary to mitigate attacks on the operating system stack, infrastructure software (such as databases) and applications. This requires hardening the server hardware, firmware and OS stack and encrypting data stored in the back end.

Next, we explore how Dell accomplishes these objectives.
Dell PowerEdge 13G enterprise security approach

Dell is constantly developing new approaches to server platform security. Rather than taking the traditional reactive approach as to finding solutions to security problems only after they occur, Dell takes a proactive approach, that is, surveying the security landscape continuously, anticipating evolving threats and exploit vectors and providing frequent secure updates to software and firmware to keep the data and hardware safe.

Dell Security Development Lifecycle

Dell has defined as part of its supply chain processes the Dell Security Development Lifecycle, shown in Figure 3, through which server security features are conceived, designed, prototyped, implemented, set into production and deployed. The SDL is a development process, akin to the software development process, that goes from security requirements analysis and definition, through design and implementation in the server platform, to verification/testing and release to end users. Dell uses it to develop the security infrastructure of PowerEdge servers.

More specifically, Dell uses the SDL during server product development and specifically during the development of server firmware to thwart the injection of malicious code during the product development lifecycle. In the case of secure firmware development, threat modeling and penetration testing occur during the design process. Secure coding practices are applied at each stage of firmware development. External audits, for critical technologies, supplements the internal SDL process to ensure that firmware adheres to security-known best practices.

Server platform security layers

As a foundation of your enterprise security strategy, the server platform in your datacenters must provide comprehensive end-to-end security that protects your entire compute and data ecosystem. Achieving this involves the SDL processes mentioned above interacting with several layers of server

---

3 This is why the process phases and their sequence are so similar.
security as shown in Figure 4. Starting with the security of the physical server itself in the bottom layer, each layer builds upon the one below it. The SDL and the security layers work to ensure firmware and server integrity, preserving server security and trust.

Figure 4. Layers of security in an enterprise server platform

6. **Physical server security** protects the physical servers’ enclosure, power supply, components and fabric interconnection from being intentionally damaged or altered.

7. **Firmware and software** enable the server to efficiently carry out complex encryption and cryptographic algorithms to protect both server data and application data in storage devices attached to the server.

8. **Attestation trust features** are built into the server, based on special-purpose processor features and cryptographic on-board elements. These provide a root of trust that enables checking at startup and other points in the server lifecycle whether the server has been altered from its expected configuration. Administrators can set policies to take the server offline and send a notification of the error to IT staff. This ensures that components of the system software stack (hypervisor, OS, applications) are aware the underlying server can be trusted when the server is operational. This layer establishes the foundation for a *chain of trust* between servers, enabling tracers and tethers to create a trusted and secure distributed server platform.
9. **Secure server management** which uses iDRAC—Integrated Dell Remote Access Console, a proprietary remote server management technology from Dell4 to handle server firmware and software updates and other operations for server security, across the data center.

10. At the top is the **process layer**, implemented by the Security Development Lifecycle in the Dell server supply chain, through which security features are developed and deployed as configuration, firmware or software updates for the PowerEdge 13G server installed base. Only duly authorized individuals or processes can modify the server itself by altering its firmware or software, or by changing its configuration or identity. This layer preserves the integrity of server and firmware throughout the lifecycle.

**Dell PowerEdge server platform threat mitigation**

There are many threat vectors in today’s changing landscape. Table 1 summarizes the Dell approach to the most important kinds of backend threats, following the server security layer ordering used earlier, from the bottom up.

<table>
<thead>
<tr>
<th>Security layer</th>
<th>Threat vector</th>
<th>Mitigation strategy</th>
<th>Dell solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical server</strong></td>
<td>Server tampering</td>
<td>Intrusion and tampering detection/prevention</td>
<td>Physical deterrents &amp; Secure management</td>
</tr>
<tr>
<td><strong>Firmware and software</strong></td>
<td>Firmware corruption, malware injection</td>
<td>Secure firmware updates</td>
<td>SDL Cryptographically signed, proprietary firmware</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>Rapid response to avoid zero-day exploits</td>
<td>Eager patching and updating</td>
<td></td>
</tr>
<tr>
<td><strong>Attestation trust features</strong></td>
<td>Server identity spoofing</td>
<td>Attestation, root-of-trust</td>
<td>TPM, TXT, chain of trust</td>
</tr>
<tr>
<td><strong>Server management</strong></td>
<td>Rogue configuration and updates, unauthorized open-port attacks</td>
<td>Security and trust checks on all server management tasks</td>
<td>iDRAC8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security layer</th>
<th>Threat vector</th>
<th>Mitigation strategy</th>
<th>Dell solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data</strong></td>
<td>Data breach</td>
<td>Encryption and access control</td>
<td>Data loss prevention (DLP): encryption, recovery, secure key management, etc.</td>
</tr>
<tr>
<td><strong>Security development process</strong></td>
<td>Supply chain steps</td>
<td>Chain of trust</td>
<td>SDL Trusted, secure steps</td>
</tr>
</tbody>
</table>

Physical server access control
PowerEdge servers provide hardware intrusion detection and logging, with detection working even when no AC power is available. For this, they include lockable bezels and lids, as well as sensors that detect when anyone opens or tampers with the chassis.

From a secure management perspective, iDRAC8 provides secure, robust out-of-band management of servers and all their features. iDRAC8 can be configured to generate notifications or alerts upon detecting an intrusion event. Individual I/O ports can be disabled through iDRAC8, providing highly robust, granular control of all server hardware resources to system administrators.

Cryptographically signed firmware updates
Many key server features are defined in firmware. Many server updates are delivered through updated firmware that a customer can pull on demand or Dell can push to ensure that a server has the latest functional and security fixes. For a server to function properly and conform to its functional specifications, its firmware must be the one designed and delivered by Dell or one of its partners. This means that server firmware is a potential threat vector through which the server hardware itself can be compromised. Firmware can provide attackers access to many facets of the server. It is essential that in the server update process, firmware updates remain identical to the corresponding Dell masters. To this effect, Dell provides securely signed firmware updates that prevent the installation of non-Dell or maliciously modified firmware.

Firmware updates for Dell provided components such as iDRAC, Dell BIOS, PERC RAID controller and other critical components, are cryptographically signed to prove authenticity. During update process, running firmware on the server component verifies the signature of the new firmware update image. Thus, provides protection against any malicious or unsigned firmware being updated on a Dell PowerEdge server.

Dell supports signed firmware in 13G PowerEdge servers for the following server components: System BIOS, iDRAC, Chassis Management Controller (CMC), Management Engine (ME), CPLD, Power Supplies, PERC controller, and the embedded Intel NDC, among others.5 Dell designs conform to the guidelines in the National Institute of Standards and Technology’s BIOS Protection Guidelines for Servers (NIST SP800-147B).

Server identity and trust protection
A subtler type of attack is server identity spoofing, akin to the identity theft that frequently occurs to individuals. Here, a rogue server supplants the identity of an actual datacenter server. To do this, attackers alter the configuration, components and/or location of a physical server, or even replace it with a maliciously modified one while preserving its network identity. To remote users, the rogue server at the expected IP address looks like the real target server opening the possibility of all sorts of security attacks. In all cases, the tampered or spoofed server becomes a potential security attack vector.

5 See Glossary for a definition of these acronyms.
Dell PowerEdge servers support TPM crypto-storage\(^6\) and Intel Trusted eXecution Technology (TXT)\(^7\) to implement tracers and tethers and root-of-trust features\(^8\) that allow them to ensure their own identity. Table 2 features the most important TPM versions in use.

Table 2. Modular TPM offerings in 13G PowerEdge Servers

<table>
<thead>
<tr>
<th>Specification⁵</th>
<th>TPM1.2</th>
<th>TPM2.0</th>
<th>Other TPM2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notable Features</td>
<td>FIPS140-2 certified, Common Criteria Certified</td>
<td>Leading industry in TPM2.0 offerings FIPS140-2 certified, Common Criteria Certified</td>
<td>Specific TPM2.0 module targeted for PRC market with local encryption algorithms</td>
</tr>
</tbody>
</table>

These technologies are compatible with remote attestation solutions such as HyTrust CloudControl. Attestation and remote attestation use the TPM and TXT technologies to take measurements at boot time of a server’s hardware, hypervisor, BIOS and OS, and compare them in a cryptographically secure manner against base measurements stored in the TPM. If they are not identical, the server identity has been compromised and system administrators can disable and disconnect the server either locally or remotely.

Proactive server software updates and patching
New threats appear continually, and can cause previously secure software to become a hidden attack vector. Zero-day exploits, i.e. security holes in software that are unknown to vendor and user, require constant vigilance and quick update turnarounds. Hackers can cause significant damage before those exploits are detected and repaired. Dell limits exposure from such attacks by releasing updates as soon as possible when critical vulnerabilities are discovered.

Data protection everywhere
Data is a major enterprise asset. Dell recognizes this and enables protection of data while at rest using data encryption and data loss prevention technologies as well as self-encrypting drives for storage, and while in transit, by authenticating and encrypting data packets in flight. Data can also be securely erased when a server is decommissioned. Users are ultimately responsible for the security of their data.

Threat monitoring and detection
Finally, in addition to the above Dell PowerEdge security features, Dell offers professional services such as the Dell SecureWorks Advanced Endpoint Threat Detection service, which monitor and gain intelligence that can be used to promote server platform security.

Adherence to standards and certifications
PowerEdge 13G enterprise server security features conform to the NIST 800-155 security recommendations and the Trusted Computing Group (TCG)⁹ TPM specifications. Both are needed for a

---

\(^6\) en.community.dell.com/techcenter/enterprise-client/w/wiki/11849.tpm-1-2-vs-2-0-features
\(^9\) www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/
trusted implementation of TnT security. Many enterprises must adhere to many regulations depending on the type and location of data stored\textsuperscript{10}. The Dell PowerEdge 13G server platform supports these, and provides a number of certifications including Common Criteria EAL4, USGv6 certification, FIPS 140-2 for Dell Self Encrypting Drives (SED), and NIST’s BIOS Protection Guidelines for Servers (NIST SP800-147B).

**PowerEdge 13G server security components**

Dell has designed the PowerEdge 13G server platforms with key industry-standards-driven capabilities and features in mind. The processors used in these Dell servers all have a number of foundational security features intended to enable faster encryption/decryption of data, faster secure key management and control of code that can execute in the processor. These features include Intel AES-NI, Intel Secure Key and Intel Execute Disable Bit, among others.\textsuperscript{11} In addition, as mentioned earlier, Dell provides TPM and Intel TXT.

Hypervisor and OS-level features build on TPM to allow remote attestation\textsuperscript{12} and the creation of trusted, distributed server groups. Third-party solutions use these technologies to increase the trust and security of a solution, e.g., HyTrust CloudControl, to provide secure, trusted cloud deployments, or encryption using Microsoft BitLocker disk encryption based on TPM. Table 3 summarizes some of the key enterprise security features of the Dell PowerEdge 13G platform.

<table>
<thead>
<tr>
<th>Security aspect</th>
<th>The PowerEdge 13G platform provides Dell customers with</th>
</tr>
</thead>
</table>
| **Key industry standards-driven capabilities** | – TCG TPM 1.2, TPM 2.0, TCG Measured Boot, Intel TXT  
  – UEFI Secure Boot (prevents unauthorized device firmware & OS boot loader load during system startup)  
  – Intrusion detection & logging; Granular control of USB and other ports |
| **High assurance & cyber-resiliency against malicious attacks** | – Signed firmware updates (cryptographic authentication by running FW image). Adherence to guidelines in NIST specifications (NIST SP800-147B, NIST SP800-155). Includes all critical FW components, including BIOS, iDRAC, CMC, PERC, NDC, NVMe, SAS Drives, Power Supply and others  
  – SDL during product development lifecycle  
  – Restful API support in iDRAC8 (Redfish); Active Directory and Two/Multi-factor authentication support  
  – Supply Chain assurance |


\textsuperscript{12} That is, performing attestation of a remote server through a secure connection.
The PowerEdge 13G platform provides Dell customers with:

- Data-at-rest (data encryption and DLP/Data-Loss-Prevention) & Data-in-flight support (IPSec)
- FIPS certified SED (self-encrypting-drives); local key management support in PERC; Microsoft BitLocker support
- Secure System Erase for server retirement and decommissioning

Certifications & adherence to standards:

- Common Criteria EAL4+ certified on 13G with RHEL
- USGv6 certification
- FIPS 140-2 for SED drives
- FIPS 140-2 and Common Criteria Certification for TPM 1.2 & 2.0

Dell PowerEdge server manageability and security

During its lifespan, a server may be deployed, repurposed, monitored, upgraded, decommissioned, recommissioned, reconfigured and more. To remotely control these and other tasks, Dell makes iDRAC available on all PowerEdge servers. Figure 5 shows a high-level functionality diagram of iDRAC8, the latest version of the technology.

![iDRAC8 high-level functionality](image)

To avoid in-production tampering of the management platform, iDRAC8 provides many in-place security features. The use of three-factor cryptography and advanced encryption helps protect the iDRAC firmware from rogue firmware and hardware-based attacks. iDRAC8 requires no OS, hypervisor or outside software to function, and runs on a dedicated secure hardware chip.

iDRAC8 provides complete server configuration and firmware update capabilities for all components in the system. Keeping firmware of various components up to date is important for both security and reliability. To ensure firmware is current, iDRAC8 can schedule automatic updates of server firmware.

---

13 Three-factor cryptography includes a 256-bit unique random value burned into each iDRAC chip so flash storage used by the Dell iDRAC firmware is always secure and cannot be decoded. All data is encrypted and cannot be read even if it is loaded from the physical iDRAC chip.
Although iDRAC8 is self-contained, it is not a proprietary, locked solution. In fact, it is compatible and can easily integrate with third-party user account control and management systems. iDRAC8 includes features such BMC server control, integration with Active Directory, RESTful API support and Redfish API. In its latest releases, iDRAC8 supports HTML5 removing Java dependencies.

Dell also provides a lightweight service (iDRAC Service Module) that runs on the OS to provide more thorough monitoring of OS-related attributes, as well as zero-touch automatic server configuration and automated server support functionality.

When the time comes to decommission a server, it’s essential to securely remove all identifiable data so that no malicious party can gain access to sensitive information. iDRAC8 provides options for the secure erase of any settings, data and other sensitive information stored in certain internal hard drives as well as in other kinds of onboard storage, whether iDRAC flash, BIOS settings, internal hard drives or internal SD cards.

Redfish is developed by the Distributed Management Task Force, INC. Information and API documentation can be found at [https://www.dmtf.org/standards/redfish](https://www.dmtf.org/standards/redfish)
Conclusion

Faced with ever-increasing multi-faceted threats, businesses must remain ahead to keep their data safe. Data breaches are extremely costly—both financially and by damaging reputations and valuable consumer trust. Dell has built the PowerEdge 13G platform approach to ensure enterprise security on four major premises: (1) provide security features with standards-based building blocks; (2) design and develop these features with a secure development lifecycle; (3) provide technologies to customers for efficient and secure management of servers in the datacenter and (4) extend supply chain security to third-party suppliers to ensure that Dell products are free of potential threat elements, while providing efficient vulnerability management. To do this, Dell partners with best-in-class vendors to provide platform solutions that are easy to select, deploy, use and manage, while effectively balancing client needs and TCO of their IT investment.

The Dell PowerEdge 13G server family has the capabilities, features and management options to help ensure both the security and integrity of data. From server conception, design and manufacturing to decommissioning, Dell’s Security Development Lifecycle and secure server management tools ensure Dell PowerEdge servers remain secure. Dell technologies, manageability and design minimize the chance of vulnerability at all points in the server lifecycle. Dell’s diligence and timely firmware updates help the PowerEdge platforms stay ahead in today’s threat landscape.

Keeping your IT infrastructure and your data secure are paramount, and the Dell PowerEdge server platform and Dell’s robust security offerings and wide-spectrum enterprise security and server management portfolio can help enterprises adhere to standards, reduce data breaches and stay ahead of the ever-present growing threats companies face today.
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation</td>
<td>The process of verifying something is true or correct</td>
</tr>
<tr>
<td>BMC</td>
<td>Baseboard management controller, the chip that controls the relationship between the hardware and management software, such as iDRAC</td>
</tr>
<tr>
<td>CMC</td>
<td>Chassis Management Controller, a systems management component designed to manage one (or more) Dell systems containing blade servers</td>
</tr>
<tr>
<td>CPLD</td>
<td>Complex programmable logic device</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware security module, a physical device that stores keys for digital cryptography</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and access management</td>
</tr>
<tr>
<td>Identify spoofing</td>
<td>Masquerading as another. A malicious server may spoof another server’s identity to serve malicious websites</td>
</tr>
<tr>
<td>iDRAC</td>
<td>Integrated Dell Remote Access Console</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>Intrusion detection/prevention system</td>
</tr>
<tr>
<td>Intel TXT</td>
<td>Intel Trusted Execution Technology, a technology that attempts to improve the security of servers, processors and other components</td>
</tr>
<tr>
<td>IPMI</td>
<td>Intelligent Platform Management Interface, a platform that provides manageability outside of the computer or server’s processor, BIOS/UEFI or OS</td>
</tr>
<tr>
<td>ME</td>
<td>Intel Management Engine (ME) provides remote management for systems built with Intel vPro technology</td>
</tr>
<tr>
<td>NAC</td>
<td>Network access control, a method of delegating access to certain networks or network functions to certain users, applications or servers</td>
</tr>
<tr>
<td>NDC</td>
<td>Network daughter card</td>
</tr>
<tr>
<td>PS</td>
<td>Dell Power Supply firmware helps improve the effectiveness of power supplies and their monitoring and failover performance.</td>
</tr>
<tr>
<td>SDL</td>
<td>Security Development Lifecycle, a method for developing secure software</td>
</tr>
<tr>
<td>SED</td>
<td>Self-encrypting drive, usually used for data at rest</td>
</tr>
<tr>
<td>Server lifecycle</td>
<td>The stages a server goes through from its purchase through to its decommissioning</td>
</tr>
<tr>
<td>Supply chain risk</td>
<td>The threats presented during product manufacturing, shipping and development</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module, a secure cryptoprocessor that can store and recall encryption keys in hardware</td>
</tr>
<tr>
<td>Tracers and tethers</td>
<td>Tracers track data as if flows through infrastructure. Tethers help validate and attest machines, workloads, etc.</td>
</tr>
</tbody>
</table>