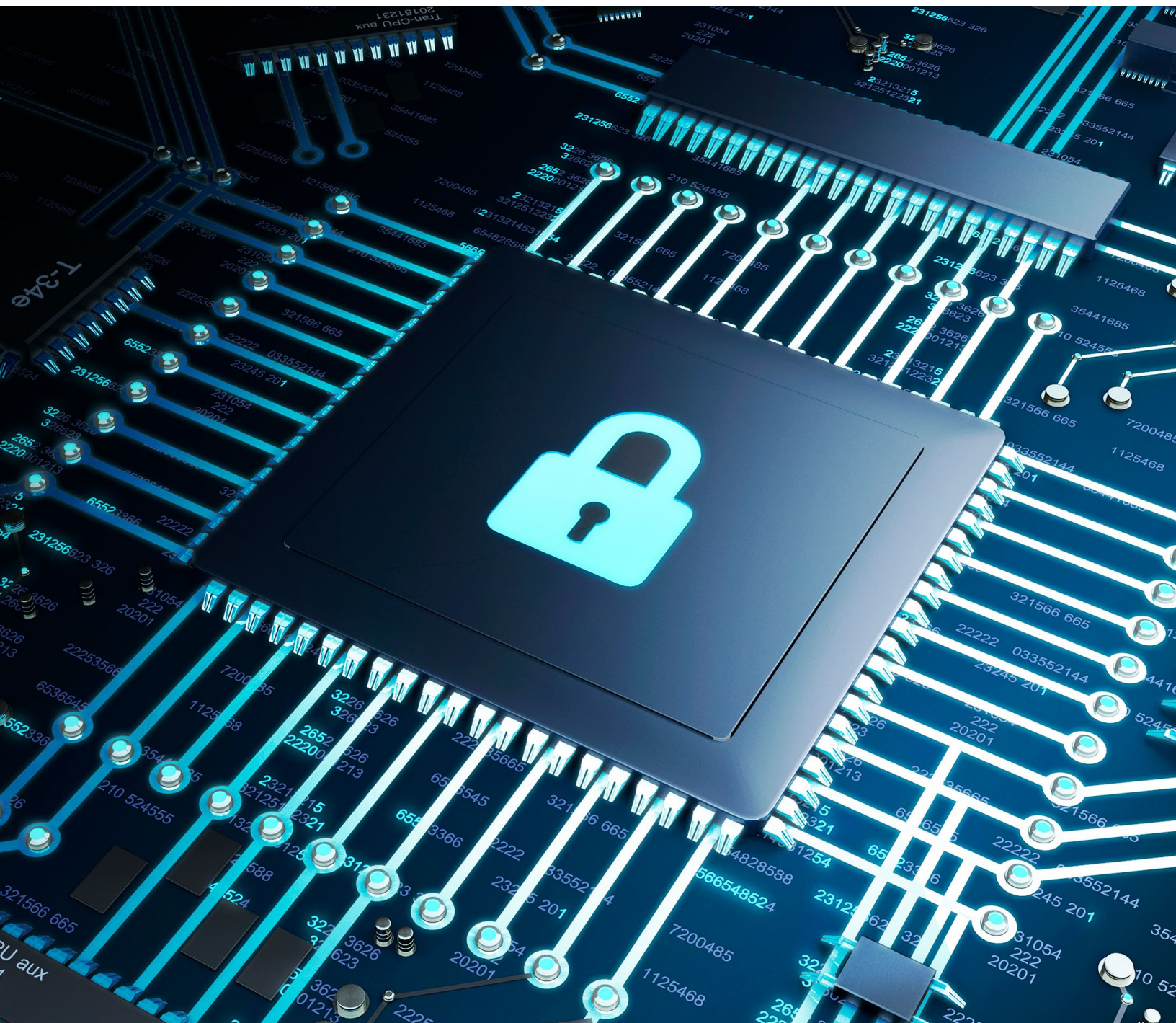


Enhance End-to-End Data Security with Microsoft SQL Server, Dell™ PowerEdge™ Servers and Windows Server 2022





With the huge shift to remote work across many sectors, companies are adjusting to the new normal and making security more of a priority than ever before. In 2021, most business leaders said remote work will continue for the foreseeable future.¹ And with more employees spread out geographically in more areas than ever, with multiple vulnerable endpoints, enterprise IT managers need to take a more holistic approach to security.

88 percent of IT leaders surveyed expect some form of remote work to continue, and the use of multiple content repositories is likely to remain a problem in the short term.¹

IT teams can improve data security across the enterprise by taking a “whole stack” approach in the data center: from hardware to database application to operating system. Modernizing infrastructure and consolidating data on the latest version of Microsoft SQL Server on Dell™ PowerEdge™ servers and Windows Server 2022 gives enterprises a strong foundation to protect data end-to-end in a changing workplace landscape.

Security Challenges Facing Enterprises Today

The rise of remote work has exacerbated the ways that enterprises are already vulnerable to cyberattacks:

- **Content sprawl.** Content sprawl is the natural result of many employees accessing and using enterprise data and applications throughout the day for years. Data ends up being stored in different locations, and across multiple repositories. And data keeps growing. IDC estimates that data will continue increasing at a rate of 24 percent compound annual growth rate (CAGR) over the next five years.² More than half of IT leaders surveyed (52 percent) say their companies have at least 10 file-storage repositories.¹ Just as having a lot of items within a house can lead to clutter and risk of loss, content saved or duplicated across multiple servers and databases can place data at risk.

41 percent of IT leaders say their top concern with content sprawl is the increased risk of data breaches and leaks.¹

- **Bring your own device (BYOD) and shadow IT.** Increased security risks from content sprawl are exacerbated by BYOD policies, in which organizations allow the use of personal smartphones and tablets for work. These devices might not be updated regularly with the latest security patches, and they might be used on unsecured Wi-Fi networks. “Shadow IT,” or the reliance on the self-proclaimed security features of cloud-based apps, is another potential attack vector for hackers due to the inherent lack of internal controls and visibility.
- **Different security patching schedules.** Many organizations use SQL Server as their data platform, but over time they end up with different versions of the database software, complicating data management and security patching. And because patching can slow systems and require server downtime, IT teams must determine the ideal timeframe to patch each version, which can delay updates.
- **Different employee access levels.** IT administrators must try to maintain permission settings as employees are hired or leave an organization. When not set appropriately or updated in a timely manner, someone in the organization can accidentally or intentionally expose company and customer data to ransomware and hackers.

Modernize Data Management on a Secure Foundation

Running SQL Server on Dell PowerEdge servers and Windows Server 2022 helps IT administrators overcome these challenges and secure business-critical workloads on modern infrastructure at the hardware, operating system (OS) and software levels.

65 percent of CIOs and other IT leaders suspect files and documents with sensitive information are saved locally to employees' personal devices.¹

Dell PowerEdge Servers

Dell PowerEdge servers help enterprises defend against the risks inherent in today's environment with a security-enabled infrastructure that supports a full range of modern workloads and objectives. PowerEdge servers are designed to speed deployment and improve performance for database applications, high-performance computing (HPC), virtualization environments and edge compute. And Dell™ OpenManage™ tools help IT administrators manage large clusters easily and effectively.

PowerEdge servers are built on an immutable, silicon-based root of trust, and they enable security functions like end-to-end boot verification, including Unified Extensible Firmware Interface (UEFI) Secure Boot customization, trusted BIOS, firmware chain of trust and verified OS bootloader. Firmware is protected according to National Institute of Standards and Technology (NIST) guidelines, including signed firmware updates, and certificate management is simplified through automatic renewal.

PowerEdge servers also provide data-at-rest protection using Secure Enterprise Key Manager (SEKM) and data-in-use protection with confidential-compute CPU technologies. To mitigate threats like counterfeit components, malware and firmware tampering, Dell Technologies takes a comprehensive approach to supply-chain security with tools for counterfeit avoidance, manufacture chain of custody, code signing, chassis intrusion and tamper-evident packaging. Further, Secured Component Verification (SCV) extends supply-chain security by verifying server component integrity.

As one of Microsoft's largest partners, Dell Technologies has worked closely with Microsoft for nearly four decades to develop industry-leading, security-enabled hardware and software solutions. With this collaboration, Microsoft software, such as Windows Server and SQL Server, runs optimally on Dell PowerEdge servers.

Windows Server 2022

Windows Server 2022 features a secured-core server based on Windows that uses hardware, firmware and OS capabilities to protect against current and future threats. Secured-core servers use processor support for Dynamic Root of Trust for Measurement (DRTM) technology to isolate firmware, so that any breach has less chance of affecting firmware code. In addition, virtualization-based security (VBS) isolates critical parts of the OS, such as the kernel, from the rest of the system to protect applications and data while helping ensure that servers remain devoted to running critical workloads.

This secured-core functionality helps proactively defend against and disrupt many of the paths that attackers use to exploit systems. Multiple Microsoft security technologies are standard or supported on secured-core servers, including hypervisor-protected code integrity in VBS, Trusted Platform Module (TPM) 2.0, BitLocker Drive Encryption, and UEFI Secure Boot.

For more information about the advanced protection capabilities of Windows Server 2022 on Dell PowerEdge servers, read the white paper, ["Gain Advanced Security Protection with the Combined Capabilities of Windows Server 2022 and Next-Generation Dell EMC PowerEdge Servers."](#)

Protect Data at the Database Application Level

SQL Server is built with security in mind. However, as previously mentioned, many enterprises are running several versions of SQL Server, and IT departments are seeking a simpler, consolidated database strategy.

In addition, SQL Server 2012 extended support ends in July 2022, which makes database consolidation on the latest version of SQL Server a more urgent issue. While older SQL Server database versions will continue working, a manufacturer-supported fix will not be available if problems arise. Patches or security updates also will not be provided, which could leave systems vulnerable to malicious attacks.

The most straightforward, practical path to consolidation for many enterprises is upgrading to the latest version of SQL Server and running older versions in compatibility mode. Database administrators can simply back up a legacy SQL Server database, then load and launch it in SQL Server 2019/2022 in compatibility mode. This approach can be a quick and simple way to upgrade if full regression testing isn't necessary. SQL Server 2019 (with a compatibility level of 150) can support versions back to SQL Server 2008 R2 (compatibility level of 100).

Best Security Practices

To further protect data, IT teams might want to ensure they're following security best practices for SQL Server (for more on these best practices and ways to implement them, read the Microsoft blog post, "[Securing SQL Server](#)"). These security best practices apply to all levels of data center infrastructure, including the hardware and OS, and they include:

- **Enhance physical security.** Physical security strictly limits access to the physical server and hardware components. This means using locked rooms with restricted access to servers and networking devices. Access to backup media is limited by storing it at a secure offsite location. Taking a layered approach is recommended: preventing access or requiring a keycard/approval at the facility's perimeter, at the building's perimeter, inside the building and on the data center floor.
- **Keep the OS updated.** OS service packs and upgrades include important security enhancements. Updates and upgrades to the OS can be applied after they are tested with database applications.
- **Use firewalls.** Firewalls increase security at the OS level by providing a chokepoint where security measures can be focused.
- **Reduce the surface area.** Limit the areas that are vulnerable to breaches by turning off or disabling features and components that aren't being used. The surface area of SQL Server can be reduced by running required services that have "least privilege" and that grant services and users rights at the appropriate level.
- **Implement role-based access control (RBAC) to "securables."**³ Securables include components such as the server, database and objects the database contains. Securables are the resources to which the SQL Server Database Engine authorization system regulates access.
- **Encrypt data at all levels.** This includes application and storage data encryption.
- **Create and use certificates.** Certificates are software keys that enable two servers to communicate securely. In SQL Server, certificates enhance object and connection security.
- **Restrict access to OS files used by SQL Server.**
- **Use strong passwords organization-wide.** This is a simple but often underprioritized security practice.
- **Conduct audits.** Ensure recovery after backup works as expected, and that access is applied appropriately.
- **Use Microsoft Defender for SQL Server databases.** Microsoft Defender for SQL Server databases scans databases for vulnerabilities. It detects anomalies that indicate unusual and potentially harmful attempts to access or exploit databases. These anomalies include suspicious database activities, potential vulnerabilities, SQL injection attacks and anomalous database access and query patterns.

Finally, each new version of SQL Server includes new security features that enhance data protection. The new ledger feature, announced for SQL Server 2022, helps protect data integrity by creating an immutable track record of data modifications over time. This can help protect data from tampering by malicious actors, and it's beneficial for scenarios such as internal and external audits.

SQL Server Ledger

- Uses an immutable ledger to protect data from tampering by malicious actors
- Establishes digital trust in a centralized system using blockchain technology
- Attests to other parties that data integrity has not been compromised

Consolidate and Protect from Hardware to Database

The role of IT will only increase along with the growth of data in the digital enterprise. And because that wealth of data is accompanied by smarter and more frequent cyberattacks, IT teams should adopt a data-security strategy that helps protect infrastructure at all levels. Upgrading to the latest version of SQL Server and Windows Server on Dell PowerEdge servers can help businesses protect sensitive company and customer data.

Take a security-first approach to your infrastructure. Learn more about how Dell and Microsoft solutions can help: www.dell.com/en-us/dt/solutions/microsoft-data-platform/index.htm.

Read [“Gain Advanced Security Protection with the Combined Capabilities of Windows Server 2022 and Next-Generation Dell EMC PowerEdge Servers.”](#)

¹ Egnyte. “2021 Data Governance Trends: Predictions, pitfalls and technologies for the future of digital work.” 2021.

www.egnyte.com/sites/default/files/2021-09/2021DataGovernanceTrendsReport.pdf.

² IDC. “Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts.” March 2021. www.idc.com/getdoc.jsp?containerId=prUS47560321.

³ For more on securables, read <https://docs.microsoft.com/en-us/sql/relational-databases/security/securables>.

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.





Get more from Dell EMC PowerEdge R750xs servers with 3rd Generation Intel Xeon Scalable processors

vs. Dell EMC PowerEdge R740xd servers with 2nd Generation Intel Xeon Scalable processors

Maybe the recent launch of next-generation Dell EMC PowerEdge servers has spurred you to look for previous-generation deals or maybe you're considering waiting to see if anything better comes along. In either case, the Dell EMC PowerEdge R750xs is a way for you to have your cake and eat it, too. Not only do these servers support the latest-generation processor, memory, networking, storage, and security technologies, our hands-on testing uncovered some compelling reasons to consider moving to Dell EMC PowerEdge R750xs servers now.

In the Principled Technologies data center, we compared transactional database performance, virtual machine (VM) density, and power efficiency on a Dell EMC PowerEdge R750xs server powered by two Intel® Xeon® Gold 6330 processors to that of a Dell EMC PowerEdge R740xd server powered by two Intel Xeon Gold 6230 processors. We found the Dell EMC PowerEdge R750xs we tested processed 76 percent more orders per minute (OPM), delivered 22 percent more OPM per watt, and supported three more VMs compared to a previous-generation Dell EMC PowerEdge R740xd.



Process 76% more orders per minute



Achieve 37% higher VM density



Handle 22% more OPM per watt



vs. a Dell EMC PowerEdge R740xd powered by 2nd Generation Intel Xeon Scalable processors

What we tested

To compare SQL Server 2019 transactional database performance on the two servers, we first created multiple Windows Server 2019 VMs with 40GB databases in a VMware® virtual environment. Then, we evaluated both servers three ways:

- We compared transactional database performance using the DVD Store 3 benchmark, which uses a simulated OLTP workload to measure performance in OPM.
- We determined VM density by adding VMs until each server reached 100 percent CPU utilization.
- We calculated power efficiency by calculating the performance per watt while the servers were active at 100 percent CPU utilization.

In our tests, the Dell EMC PowerEdge R750xs, powered by 3rd Generation Intel Xeon Scalable processors, processed more OPM, achieved higher VM density, and handled more OPM per watt.

About the Dell EMC PowerEdge R750xs server

This feature-optimized, 2U server is designed for virtualization, VDI, and software-defined storage node workloads. It comes with “full-stack management integration with Microsoft, VMware, ServiceNow, Ansible, and many other tools for on-premise, edge, and cloud environments.”¹



About 3rd Generation Intel Xeon Scalable processors

The Dell EMC PowerEdge R750xs server features Intel Xeon Gold 6330 processors, which are a direct upgrade to Intel Xeon Gold 6230 processors. These processors are, according to Intel, “optimized to power the industry’s broadest range of workloads” and come with integrated AI acceleration (Intel DL Boost technology) and advanced security capabilities (Intel SGX and Intel Crypto Acceleration), which provide built-in data and application code protection.²

Table 1: The dual-socket 2U servers we tested offer the following specifications, according to Dell:

	Dell EMC PowerEdge R750xs ³	Dell EMC PowerEdge R740xd ⁴
Intel Xeon Scalable processors	3 rd generation	2 nd generation
Cores per socket*	Up to 32	Up to 28
Support for PCIe NVMe SSDs	Gen4	Gen3
Memory channels	8	6

To learn more, visit www.dell.com/en-us/work/shop/servers-storage-networking/sf/poweredge-rack-servers.

*In our tests, the Dell EMC PowerEdge R750xs was configured with 28-core processors and the Dell EMC PowerEdge R740xs was configured with 20-core processors. For more details, read the [science behind the report](#).

More VMs without sacrificing transactional database performance

In e-commerce, maximizing the number of orders your servers handle could translate to less waiting for customers retrieving product descriptions, adding items to their carts, and making online purchases. But e-commerce isn't the only sector that relies on speedy database system performance. The ability to support more OLTP transactions per minute could speed up updating patient records, gathering financial data, and catering to clients' needs. When combined with higher VM density, this could translate to lower expenses related to data center power and cooling.

In our DVD Store 3 benchmark comparison, we found the Dell EMC PowerEdge R750xs shot past the previous-generation server in total number of OPM through higher VM density.



Process 76% more OPM per server

Total orders per minute per server

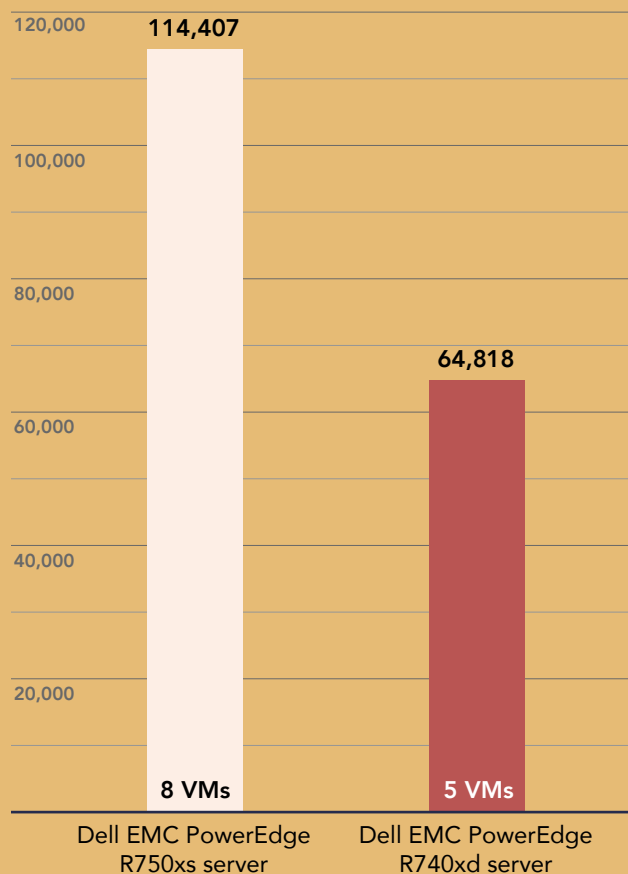



Figure 1: Total OPM per server based on DVD Store 3 benchmark results. Higher is better. Source: Principled Technologies.

The value of higher VM density

Maximizing the number of VMs your on-premises servers support can save your company money by requiring fewer resources, such as IT management, data center space, hardware, and power and cooling. We determined VM density by adding VMs until each system reached 100 percent CPU utilization. Adding more VMs to host servers running at 100 percent utilization in a virtualized environment would negatively impact individual VM OPM processing performance on the system under test.⁵


**Achieve 37%
higher VM
density**

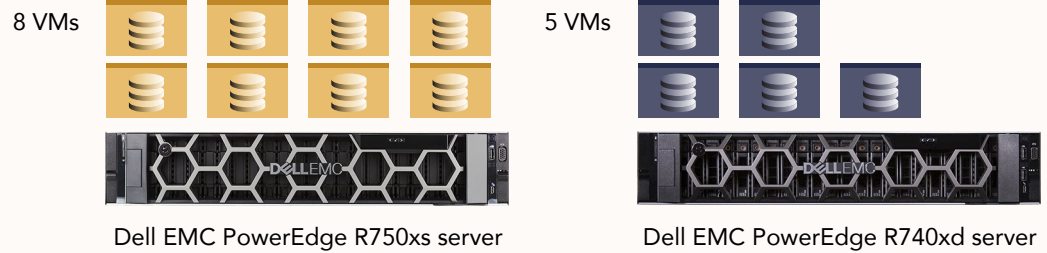


Figure 2: Total VMs per server. Higher is better. Source: Principled Technologies.

The value of better power efficiency

While reliable, high-performance servers are essential to grow your business and keep end-users happy, there is another important piece in the performance puzzle: energy consumption. In addition to its superior transactional database performance and VM density versus the previous-generation Dell EMC PowerEdge R740xd server, the Dell EMC PowerEdge R750xs delivered 22 percent more OPM per watt. This could, when combined with the higher VM density mentioned in the last section, translate to lower data center power and cooling expenses.

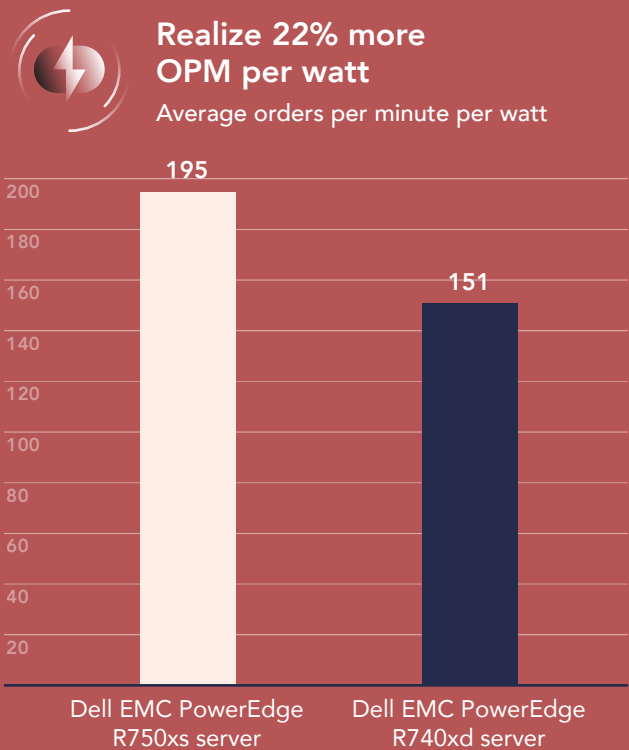


Figure 3: Average OPM per watt based on DVD Store 3 benchmark results. Higher is better. Source: Principled Technologies.



Conclusion

Along with 3rd Generation Intel Xeon Scalable processors, the Dell EMC PowerEdge R750xs server is loaded with next-gen memory, networking, storage, and security technologies. In our hands-on testing, the Dell EMC PowerEdge R750xs server powered by two Intel Xeon Gold 6330 processors processed 76 percent more OPM and supported three more VMs than a previous-generation Dell EMC PowerEdge R740xd server powered by two previous-generation Intel Xeon Gold 6320 processors—all while delivering 22 percent more OPM per watt. Imagine what these server performance increases could do for your company's bottom line.

- 1 Dell Technologies, "Dell EMC PowerEdge R750xs spec sheet," accessed August 2, 2021, https://i.dell.com/sites/csdocuments/Product_Docs/en/r750xs-spec-sheet.pdf.
- 2 Intel Newsroom, "Intel Launches Its Most Advanced Performance Data Center Platform," accessed August 1, 2021, <https://www.intel.com/content/www/us/en/newsroom/news/3rd-gen-xeon-scalable-processors.html>.
- 3 Dell Technologies, "Dell EMC PowerEdge R750xs spec sheet," accessed August 2, 2021, https://i.dell.com/sites/csdocuments/Product_Docs/en/r750xs-spec-sheet.pdf.
- 4 Dell Technologies, "Dell EMC PowerEdge R740xd spec sheet," accessed August 2, 2021, https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/poweredge-r740xd-spec-sheet.pdf.
- 5 Heroix, "Maximizing VMware Performance and CPU Utilization," accessed August 6, 2021, <https://www.heroix.com/blog/vmware-vcpu-over-allocation/>.

Read the science behind this report at <http://facts.pt/6sX26zb> ▶



Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc. All other product names are the trademarks of their respective owners. For additional information, review the science behind this report.

This project was commissioned by Dell EMC.