Solution Brief

Network-Optimized 5th Gen
Intel® Xeon® Scalable Processors
Confidential Computing

Secrets Management with HashiCorp Vault and Intel® Trust Domain Extensions (Intel® TDX)

HashiCorp Vault protects and manages private encryption keys, credentials and other secrets, reducing the attack surface of network security functions. With Intel TDX hardware protection, Vault is further isolated and protected from other virtual machines (VMs) and system software. Intel TDX is now generally available on 5th Gen Intel® Xeon® Scalable processors.

The complexity and cost of cybersecurity are higher than ever before, as are the potential damages from attacks not warded off successfully. IBM reports that the global average cost of a data breach in 2023 has reached $4.45 million, an amount that has risen 15.3% over the last three years and continues to grow.[1] The immediacy and scale of these threats make it imperative for businesses not only to follow best practices, but to innovate where they can as they protect their vital core data. In fact, 51% of organizations report that they are planning to increase security investments as a result of a breach.[1]

Many companies look to increase their security postures with only modest cost and disruption by increasing the use of data encryption in their operations. Security-oriented networking solutions such as zero-trust network access (ZTNA) together with secure access services edge (SASE) are also gaining ground, further increasing use of encryption. Accordingly, secrets-management systems are becoming more important than ever, to provide protected storage for private encryption keys and other credentials such as passwords and certificates. In all these cases, encrypting data at rest and in transit reduces the attack surface and helps protect sensitive data.

Even so, data including encryption keys and other secrets is generally unencrypted while in use, making it vulnerable to potential compromise. The processes that expose such secrets in the shared memory space are conventionally isolated from each other using software measures, but those can be susceptible to escalation-of-privilege attacks and vulnerable in the event that the operating system, hypervisor or other system software is breached.

Confidential computing improves on that isolation using measures that are rooted in hardware, below the system software level and out of reach from software-based attacks. Reduced vulnerability and the novel ability to protect data while it is in use have set the stage for rapid uptake of these technologies, which has only just begun.

CONFIDENTIAL COMPUTING MARKET SIZE

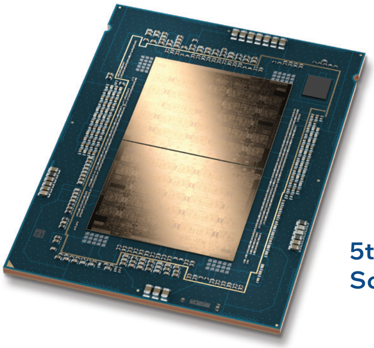
94.4% CAGR
2023-2026[2]

$53.31 BILLION
By 2026[2]

HashiCorp is at the leading edge of advancing and enabling confidential computing for the enterprise with its Vault secrets-management system. The combination of Vault and Intel® Trust Domain Extensions (Intel TDX) can benefit customers who need confidential computing environments for their sensitive workloads. Intel TDX, which has broad general availability for the first time in 5th Gen Intel® Xeon® Scalable processors, isolates Vault at the VM level to protect secrets while they are in use: from other VM tenants, the hypervisor, other system software and administrators.

Platform leadership for performance and workload isolation

The 5th Gen Intel Xeon Scalable processors uniquely provide the hardware foundation for confidential computing with HashiCorp Vault. In addition to Intel TDX, the platform offers outstanding performance and energy efficiency. Execution resources include high per-core performance on up to 64 cores, with built-in accelerators for AI, encryption and other critical workloads. The balanced platform also provides up to 16 percent memory bandwidth improvement[3] and up to 3x increased last-level cache (LLC) vs 4th Gen Intel Xeon processors.[4]



5th Gen Intel® Xeon® Scalable processors.

The platform includes two processor SKUs optimized for network security workloads, engineered for high throughput, low latency and high energy efficiency on workloads including next-gen firewalls, SD-WAN and SASE, with applicability also to general cloud compute.

- **Intel Xeon Gold 6548N processors** (two-socket, 32 cores, 2.8 GHz) are tuned for mid-tier security implementations.
- **Intel Xeon Platinum 8571N processors** (one-socket, 52 cores, 2.4 GHz) are tuned for high-end security implementations and feature up to 3x larger last-level cache (LLC).

The combination of HashiCorp Vault and 5th Gen Intel Xeon Scalable processors makes it possible to pursue new business models that demand protection for shared sensitive data and intellectual property, with performance to help maximize value and energy efficiency to help reduce operating costs. In addition, the platform supports Optimized Power Mode, which is user configurable in the platform BIOS to help achieve incremental power savings for select workloads.

Confidential computing isolates sensitive or regulated data from privileged third parties — as well as unauthorized software and users — based on a low-level hardware root of trust that extends upward through the solution stack. That root of trust enables a trusted execution environment (TEE), with a low-level hardware foundation that eliminates software dependencies and associated vulnerabilities. The TEE protects Vault and the integrity of operations performed on it. Unlike software-based measures, the TEE is protected against unauthorized access by users or software, regardless of privilege level.

5th Gen Intel Xeon Scalable processors improve dramatically on the confidential computing technologies of predecessors with the general availability of VM-level TEE in addition to application-level isolation, which can be utilized independently of each other. Intel Trust Domain Extensions (Intel TDX) offers isolation and confidentiality at the virtual machine (VM) level. Within an Intel TDX confidential VM, the guest OS and VM applications are isolated from access by the cloud host, hypervisor and other VMs on the platform. It offers a simple migration path for existing VMs to move to a TEE, with a projected performance overhead of less than 5% on HashiCorp Vault.[5]

5th Gen Intel Xeon Scalable processors also provide Intel Total Memory Encryption (Intel TME) as an enabling technology for Vault's confidential computing implementation based on Intel TDX. Intel TME enables the hypervisor to separately encrypt multiple VMs (or containers) with unique encryption keys owned by the tenants. This hardware-enabled inline encryption technology requires no application changes and delivers high performance. Co-engineering by HashiCorp and Intel has helped Vault lead the market with next-generation confidential computing.

Secret and encryption management: HashiCorp Vault

Protecting application secrets such as encryption keys, passwords, tokens, certificates and other sensitive data is a core goal of confidential computing. HashiCorp Vault is a widely adopted secrets-management system that runs encryption, authentication and authorization services to enable secure storage, management, control and auditability of secrets.

Protected data can be securely stored and managed in Vault, where access and control are tightly restricted with robust support for auditable governance measures. Vault provides both graphical and command-line interfaces to access its contents, as well as programmatic access using an HTTP API. Before allowing access, Vault validates, authenticates and authorizes clients such as users, machines and applications, helping maintain a robust and consistent security posture. Those mechanisms are critical for understanding and controlling access patterns to critical data.

Vault uses client tokens that govern access based on individual client policy rules that constrain what resources can be accessed and what actions can be performed on them. Tokens can either be created manually and assigned to clients, or they can be generated in a self-service modality using a software service. The Vault repository guards against their unintended exposure. It also handles authentication and authorization for robust access control.

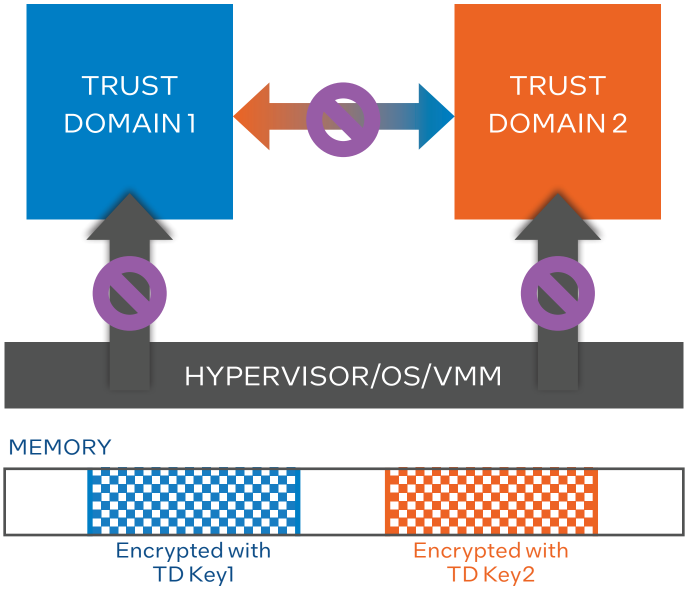
Beyond protecting access, Vault also provides monitoring and management capabilities that make it possible to understand and govern what parties, applications and services are accessing specific secrets, across platforms. Key features of Vault include the following:

- **Secure secret storage**. Vault encrypts secret key/value pairs before writing them to storage, providing an added layer of protection beyond protecting the storage itself.
- **Dynamic secrets**. Vault can generate short-lived secrets on demand, such as credentials for a database or storage volume, and automatically revoke them after use.
- **Live data encryption**. Vault can encrypt and decrypt data without storing it, enabling developers to store encrypted data in databases or other conventional data stores without defining encryption schemes.
- **Leasing and renewal**. Vault maintains leases for each secret to govern automatic revocation of the secret at end-of-lease; built-in APIs provide the mechanism for clients to renew secrets.
- **Built-in secret revocation**. Vault automates revoking sets of secrets, such as all secrets of a given type or that have been accessed by a given user, which is valuable for both key rolling and intrusion response.

To further harden the cryptographic isolation of secrets, Vault can be deployed in a VM protected by confidential computing based on Intel TDX. This approach is well suited to HashiCorp's development of the Vault solution in part because it allows for the existing Vault platform to be adapted to confidential computing without changes to code or disqualifying performance impacts.

Isolating and protecting Vault with Intel TDX

Intel TDX extends confidential computing with a new kind of VM guest called a trust domain (TD). Each TD maintains its own protection barrier, running with encrypted memory that is isolated by means of unique, dedicated private encryption keys. That independence is a critical enabler for defense-in-depth, providing hardened secret protection based on Vault. It helps remove barriers to enterprises as they evolve their security postures for today's highly distributed networks, including implementations of new security models such as ZTNA and SASE.



Tenants are isolated using trust domains, each of which is encrypted using a unique key.

Because Intel TDX places the entire VM within a single trust domain, Vault reduces calls to services outside the trust boundary. The entry and exit cycles associated with the calls each require the hardware to perform operations to protect cache and memory when control flow passes outside the trust boundary. Reducing the need for such operations is key to the low overhead and high performance of HashiCorp Vault's confidential computing implementation based on Intel TDX.

Conclusion

The general availability of Intel TDX in 5th Gen Intel Xeon Scalable processors provide HashiCorp Vault with memory protection at the VM level, without requiring code changes or creating untenable performance impacts. As application secrets continue to proliferate, this protection will safeguard the authentication, encryption, authorization and access mechanisms that cybersecurity depends on, especially for sensitive workloads including those protected by regulations such as PIPA, GDPR and HIPAA. Ongoing co-engineering by HashiCorp and Intel will continue to build on this foundation to expand the future promise of confidential computing.

Learn More

Intel® Trust Domain Extensions (Intel TDX)

HashiCorp Vault

Solution provided by:

intel xeon + HashiCorp

[1] IBM, "Cost of a Data Breach Report 2023." https://www.ibm.com/reports/data-breach.

[2] Fortune Business Insights, "Confidential Computing Market Size, Share & COVID-19 Impact Analysis." https://www.fortunebusinessinsights.com/confidential-computing-market-107794.

[3] See [G12] at intel.com/processorclaims: 5th Gen Intel Xeon Scalable processors. Results may vary.

[4] See [G11] at intel.com/processorclaims: 5th Gen Intel Xeon Scalable processors. Results may vary.

[5] See [N27] at intel.com/processorclaims: 5th Gen Intel Xeon Scalable processors. Results may vary.

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel technologies may require enabled hardware, software or service activation.

1123/LH/MESH/353954-001US