White Paper

Secure your Microsoft Azure Arc–enabled environment with Microsoft and Intel

See how to secure your hybrid and multi-cloud environments with Azure Stack HCI powered by Intel technologies.

Today’s threat landscape

In a recent report, IBM Security noted that 83 percent of the organizations it surveyed had had more than one data breach. For the organizations cited in the report, it took on average 243 days to identify a data breach (and another 84 days to contain the breach). Moreover, 60 percent of the organizations’ breaches led to increased prices that they passed on to customers.[1]

But while data breaches can represent some of the costliest and most public security threats that organizations face, they are far from the only one, and new threats continue to emerge. Botnets can be used to control networks of infected private computers. Ransomware has become big business, with hackers providing ransomware-as-a-service on the cloud. Cloud-based attack techniques utilize the increasing computing power of the cloud to create new attacks. Threat-groups are harbored by nation-states, which devote significant resources to attacks against infrastructure, businesses, and military targets in other countries.

At the same time that threats are evolving in new ways, new vulnerabilities are also emerging for organizations. For example, as apps get better secured, attackers are increasingly moving down the stack to lower layers of infrastructure (such as firmware). And today’s distributed workforce increases security risks as users need to access data and other corporate resources from many remote locations, increasing the attack surface that organizations need to secure. In short: the bad actors are continually getting better funded, getting better trained, and evolving the tools they use and their choice of targets.

What security professionals are up against

While malicious actors are developing new techniques for new targets, security professionals face increasing challenges. The labor supply curve for security professionals is negative; there just aren’t enough of them! Security professionals are under-resourced and overwhelmed by the volume of specialized tools they need to use to get their job done. For example, Microsoft’s security operations team uses more than 20 tools.

On the other hand, security teams can’t find the signal in the noise. All good security teams work in two modes: protecting assets proactively, and constantly monitoring for breaches. However, the latter is increasingly challenging, as security teams must wade through a massive volume of security signals to find actual threats. As a result, active attacks can live in environments for more than 50 days before being discovered.[2]

Attacks increasingly traverse many layers and silos of organizations. Security can’t be piecemeal. Attackers will find one weak entry point and then traverse laterally across the organization. Organizations therefore can’t just protect a specific workload; security needs to cover all workloads. Put another way, just some security is no security at all.

Hardening corporate security with Microsoft and Intel

Microsoft and Intel offer enterprises a comprehensive approach to security across their entire IT estate through Azure Stack HCI, a hyperconverged and hybrid solution that uses Azure Arc to bring Azure-based security to hybrid and multi-cloud environments. This is powered by Intel technologies with built-in security, helping create more comprehensive protection from silicon to cloud.

A security-first approach from Microsoft

Azure is the only cloud platform built by a security leader. More than 650,000 customers and 90 companies out of the Fortune 100 trust Microsoft for security. And Microsoft employs more than 8,500 security experts and is committed to investing $20 billion on security over the next five years.

The volume of security signal that Microsoft analyzes is staggering: it processes more than 24 trillion signals every 24 hours. In 2020 alone, Microsoft Defender blocked 9 billion malware threats. For these reasons and others, Microsoft is a leader in security in seven Gartner Magic Quadrant and five Forrester Wave studies.

Security at the core

Intel's security-first pledge aims to keep businesses safe with a defense-in-depth strategy that spans three key priorities:

1. **Foundational security**—critical protection to help verify the trustworthiness of devices and data
2. **Workload and data protection**—trusted execution for hardware-isolated data protection
3. **Software reliability**—platforms that help protect against a range of cybersecurity threats

In addition to building security capabilities into the hardware, Intel created industry-leading programs including the Intel Security Development Lifecycle, which applies privacy and security practices across hardware, firmware, and software, throughout the product lifecycle.

Azure security: Built-in, modern, and holistic tools and controls

Azure security tools and controls are built into the platform, making them easy to discover and turn on. Azure has native controls for DevOps, and tools like Azure Security Center can scale to enable protection and monitoring for all cloud resources and across all layers of the architecture. Azure also offers broad policy support, automation, and actionable best practices.

Azure security tools are modern compared to the popular tools used today on premises. These tools protect, detect, and respond with artificial intelligence (AI) and at cloud scale. Microsoft's use of AI—powered by intelligence from across Microsoft's entire security portfolio—surfaces the most important signals to the security team, so they aren't buried in noise. In addition, cloud scale means that you always have the capacity you need, without investing in infrastructure setup and maintenance.

Azure security is also holistic. Security teams can use these tools to protect their hybrid and multi-cloud environments in addition to Azure, giving them a unified view of their entire environment and enabling them to be more efficient with fewer tools.

For example, Microsoft Defender for Cloud offers an experience for your cloud security posture that spans information from other public cloud providers. Another example is Azure Sentinel, Microsoft's cloud-native security information and event manager (SIEM), which lives within Azure but can protect your organization's entire environment. These solutions also integrate with Microsoft's security portfolio, allowing for a holistic SecOps experience across the entire organization.

Azure and zero trust

Microsoft built Azure on top of industry-standard zero-trust principles:

- Verify explicitly
- Assume a breach

Azure has a consistent Azure Resource Manager layer for managing resources, which combines with Microsoft identity capabilities to deliver least-privilege access and Microsoft networking capabilities spanning micro-segmentation to firewalls to deliver you an architecture literally designed for zero trust.

Microsoft Azure Arc–enabled infrastructure

Azure Arc extends Azure to Azure Arc–enabled infrastructure. Azure Stack HCI benefits from the deep and hardened security benefits of Azure. And because of the integration with Azure, hybrid and multi-cloud environments based on Azure Stack HCI are built with security in mind.

Azure Arc provides a consistent and flexible model for development, operations, and security for both your existing and your new applications. You use the same tools and the same security and governance technologies to create and manage application resources. Azure Arc brings a subset of Azure services for applications, data, and AI to use on new and existing hardware, virtualization, Kubernetes platforms, Internet of Things (IoT) devices, and integrated systems.

Azure Stack HCI is the Microsoft implementation of Azure Arc–enabled infrastructure. It is hybrid by design and delivered as an Azure subscription. It also brings Azure to all your remote offices or other sites that traditionally have not been a good fit for cloud-based services.

Azure Stack HCI provides familiar management and operations. It is built on the foundation of Windows Server and Microsoft Hyper-V and familiar tools like Windows Server Admin Center and Azure portal. It supports Active Directory and Group Policy Objects and is compatible with popular third-party tools such as Altaro, Commvault, Datadog, Veeam, and Veritas (to name a few). Management tasks on Azure Stack HCI are completely scriptable using popular, cross-platform Windows PowerShell framework.

Deployment options

Azure Stack HCI comes with flexible deployment options to meet the specific needs of your organization. One option is to deploy it through integrated systems, solutions that come with services, software, and subscription pre-installed. Integrated systems are offered by leading hardware vendors and support Secured-core server; they enable you to get started with fewer steps for faster time to value. Alternatively, you can deploy Azure Stack HCI through validated nodes, where you or a system integrator builds the solution from a catalog of verified components. This route provides you with the broadest choice of hardware components and can support more diverse configurations for demanding workloads, as well as some customization due to the diversity of solution offerings. In some cases, existing hardware can be repurposed if it matches a current validated node solution in the Azure Stack HCI catalog.

Enabling innovation with foundational security, powered by Intel technologies

Intel provides foundational security, helping ensure a critical base of protection across the platform without sacrificing infrastructure performance. Intel's broad portfolio and integrated accelerators help provide a trusted execution environment for workloads, resulting in increased protection of data in use, in flight, and at rest while providing workload flexibility based on business needs. The suite of technologies includes:

- **3rd Generation Intel Xeon Scalable processors** provide a wide range of SKUs to tailor cores and frequencies to workload requirements with integrated virtualization and security technologies and AI acceleration built into the processor.
- **Intel Optane persistent memory 200 series** can serve as volatile memory or persistent storage, depending on mode, to provide an affordable way to increase memory space and reduce the total amount of DRAM needed while providing hardware security mitigations and automatic data encryption.
- **Intel Optane SSD P5800X drives** are designed for low latency and high performance and provide high endurance, low latency, and high quality of service (QoS) for the cache tier.
- **Intel Ethernet 800 series network adapters** provide flexible and scalable input/output (I/O) virtualization and improved performance using intelligent offloads, and remote direct memory access (RDMA) streamlines and accelerates node-to-node network traffic, all of which delivers greater intelligence and performance for virtualization and network-packet processing.

Azure Arc brings Azure-grade security to your hybrid and on-premises deployments

The new reality of hybrid and multi-cloud environments comes with its own set of challenges, making it even more important to implement a comprehensive and coordinated security and governance strategy. The more you scale your applications across diverse types of environments, the broader the attack surface and potential for security risks. Microsoft and Intel see that most organizations keep large parts of their infrastructure on premises, while also choosing to work across multiple cloud providers.[2]

Azure Arc enables you to secure and govern across environments:

- Harden your security posture and detect threats in order to protect your workloads.
- Monitor your infrastructure and applications end to end in order to proactively detect, diagnose, and resolve issues.
- Conform to key compliance standards and enforce organizational policies.

Layered security is built into Azure Stack HCI and powered by Intel technologies.

Secured-core server

Secured-core server is a collaboration across Microsoft, Intel, and server OEM partners to simplify security enablement. The Windows Admin Center user experience provides easy access to configure the state of the Secured-core features. Secured-core server provides advanced protection; Windows Defender System Guard provides security from the silicon up against firmware attacks while virtualization-based security (VBS) isolates critical parts of the system from even privileged malware.

Secured-core server also supplies preventive defense for Azure Stack HCI environments. VBS features like hypervisor-protected code integrity (HVCI) and credential guard prevent entire classes of vulnerabilities and better protect sensitive assets like credentials. And Trusted Platform Module 2.0 (TPM 2.0) provides hardware root-of-trust as a secure foundation.

Azure Services

Azure Arc brings Azure security services such as Microsoft Defender for Cloud and Microsoft Sentinel to Azure Stack HCI hybrid and multi-cloud environments.

Microsoft Defender for Cloud provides a hardened security posture that spans information from other public cloud providers. Microsoft Defender for Cloud provides you with a secure score that provides a continual assessment of your security posture so you can track new security threats and precisely report on the progress of your security efforts. Microsoft Defender for Cloud also provides step-by-step recommendations so that you can protect your workloads from known security risks. And security alerts from Microsoft Defender for Cloud enable you to defend your workloads in real time so you can react immediately and prevent security events from developing.

Microsoft Sentinel provides both SIEM and security orchestration, automation, and response (SOAR) for both cloud and on-premises environments. It provides a bird's-eye view across your organization and a single solution for attack detection, threat visibility, proactive hunting, and threat response. It also enables you to put large-scale intelligence from decades of Microsoft security experience to work in your environment. Microsoft Sentinel also makes your threat detection and response smarter and faster with AI.

Layered defense

Azure Stack HCI provides a layered defense for all your workloads, wherever they run. The unifying thread running throughout this layered defense is pervasive encryption made possible with minimal performance overhead by Intel technologies.

Network encryption

Security in Azure Stack HCI starts by encrypting network traffic across your hybrid and multi-cloud environment. Software-defined networking (SDN) in Azure Stack HCI provides a way to centrally configure and manage networks and network services such as switching, routing, and load balancing in your environment. You can use SDN to dynamically create, secure, and connect your network to meet the evolving needs of your apps.

Coupled with SDN in Azure Stack HCI is Azure VPN Gateway, which provides site-to-site virtual private networks (VPNs) to secure network connections across your environment using the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). And Azure Stack HCI uses Server Message Block (SMB) encryption to protect data in transit across the network.

This pervasive encryption of data is made possible with minimal overhead by Intel Vectorized Advanced Encryption Standard (AES). The Intel AES New Instructions (Intel AES-NI) in Intel Xeon Scalable processors implement some of the intensive sub-steps of the AES algorithm directly into the hardware, which accelerates encryption. Intel Vectorized AES boosts encryption performance further by enabling Intel AES-NI to perform cryptographic calculations on more data at once, which means that encryption performance can benefit from the large data registers available on Intel Xeon Scalable processors with the Intel Advanced Vector Extensions 512 (Intel AVX-512) instruction set.

Storage encryption

Stored data in Azure Stack HCI also needs to be protected. Azure Stack HCI does this using BitLocker for Storage Spaces, which encrypts the contents of Storage Spaces data volumes in Azure Stack HCI. Encrypting data at rest can help organizations stay compliant with government, regional, and industry-specific standards such as Federal Information Processing Standard (FIPS) 140-2, and the Health Insurance Portability and Accountability Act (HIPAA).

Data encryption in Azure Stack HCI also benefits from the encryption acceleration provided by Intel AES-NI and Intel Vectorized AES. These Intel technologies enable ubiquitous data encryption without the typical performance penalty for applications encrypting data.

Full memory encryption

Encrypting data at rest and in motion is not enough; the data is still vulnerable when it is being used by applications in system memory. To address this vulnerability, Azure Stack HCI uses Intel Total Memory Encryption (Intel TME). Intel TME helps protect platform memory (DRAM) against hardware attacks such as cold boot, freeze spray, or DIMM removal. It is enabled directly in system BIOS with a single CPU-generated key and is compatible with Intel Software Guard Extensions (Intel SGX) application enclave solutions in the Azure public cloud. The encryption engine in Intel TME uses the AES-XTS algorithm and generates only a small overhead on performance (generally 1–2 percent).

Virtual machine (VM) and container isolation

In multi-tenant environments such as Azure Stack HCI, even encrypting hardware memory isn't enough. The sectors of system memory being used by different virtual machines (VMs) and containers also need to be isolated from each other. To accomplish this, Azure Stack HCI uses Intel Total Memory Encryption Multi-Key (Intel TME-MK). This technology enables the VM manager to separately encrypt VMs or containers with unique encryption keys owned by the tenants.

Applications do not need to be refactored to use Intel TME-MK in Azure Stack HCI. It is enabled in the BIOS and encrypts the entire memory by default; no software enabling is necessary.

Intel TME-MK can provide additional security for features in Azure Stack HCI. For example, virtualization-based security in Azure Stack HCI can use Intel TME-MK to create and isolate a secure region of memory from the normal operating system. Azure Stack HCI can then use this secure region of memory to host security solutions or credentials and provide them with increased protection from any vulnerabilities in the operating system. This extra security can prevent attacks on the secured security solutions or credentials by means of a compromised operating system.

On the edge, Intel TME-MK can enable organizations to run workloads of mixed levels of sensitivity on the same platform in Azure Stack HCI. Intel TME-MK protects workloads from each other and permits moving applications, the operating systems, and even the hypervisor outside the trusted computing base.

Confidential computing

For additional security and isolation, workloads running in the Azure public cloud can use Intel SGX. Intel SGX enables developers to partition applications to include hardened enclaves. Data or algorithms running in Intel SGX enclaves are protected from modification and inspection. So, for example, a bank running sensitive AI algorithms could do so in the Azure public cloud without any attackers being able to inspect them.

Figure 1 provides a visual analogy to illustrate the relationship between Intel TME, Intel TME-MK, and Intel SGX. If you were to think of system memory as a large apartment building, Intel TME would be the key to that building: good for keeping out many threats but powerless if a threat were to get into the building. Intel TME-MK would thus be like keys to the respective apartments in the building: each tenant has their own key, and the units remain isolated from each other (and from external threats, which would have to compromise tenants individually). Finally, Intel SGX is like a safe in a given apartment: large enough to protect the most valuable assets for a tenant and able to protect sensitive items if the tenant is compromised.

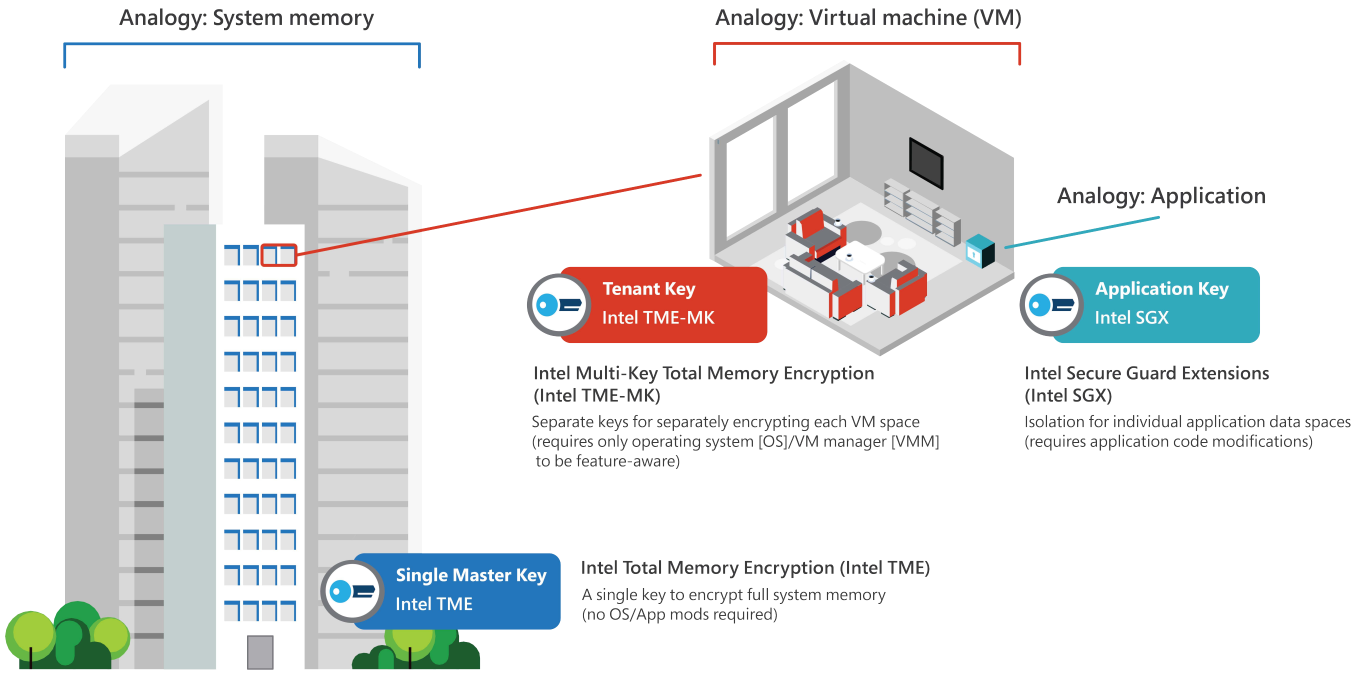
Analogy: System memory
Analogy: Virtual machine (VM)
Analogy: Application
Tenant Key
Intel TME-MK
Application Key
Intel SGX
Intel Multi-Key Total Memory Encryption
(Intel TME-MK)
Separate keys for separately encrypting each VM space
(requires only operating system [OS]/VM manager [VMM]
to be feature-aware)
Intel Secure Guard Extensions
(Intel SGX)
Isolation for individual application data spaces
(requires application code modifications)
Single Master Key
Intel TME
Intel Total Memory Encryption (Intel TME)
A single key to encrypt full system memory
(no OS/App mods required)

Figure 1. Analogy of the relationship between Intel Total Memory Encryption (Intel TME), Intel Total Memory Encryption Multi-Key (Intel TME-MK), and Intel Software Guard Extensions (Intel SGX)

Cryptographic acceleration

In the arms race against malicious actors, Intel is constantly improving the performance of stronger cryptographic algorithms. The new instruction set for cryptography in 3rd Generation Intel Xeon Scalable processors (informally referred to as Crypto-NI) supports the Intel AVX-512 instruction set in order to pack multiple computational operations into a single processor clock cycle. Crypto-NI brings high performance for pervasive encryption in Azure Stack HCI using a variety of algorithms:

- Vectorized AES instructions and "carry-less" multiplication instructions accelerate symmetric algorithms like AES.
- Secure hash algorithmic (SHA) extension instructions accelerate secure hash algorithms that are used to generate random numbers (especially for transport layer security [TLS] handshakes in HTTPS connections).

Conclusion

Azure Arc is designed to deliver the best of Azure security to you in hybrid and multi-cloud environments. Azure security provides built-in, modern, and holistic tools and controls for your entire IT estate and lets you tap Microsoft's extensible pool of experience and expertise in combating modern security threats through Azure security services such as Microsoft Defender for Cloud and Microsoft Sentinel.

Coupled with the powerful security features provided by Azure, Azure Arc–enabled Azure Stack HCI takes advantage of the latest hardware innovations from Intel. Hardware technologies from Intel such as 3rd Generation Intel Xeon Scalable processors and the advanced cryptographic instruction sets and hardware acceleration that come with Intel Xeon Scalable processors enable Azure Stack HCI to make use of encryption across networking, storage, and memory to efficiently secure your workloads without compromising performance.

Learn more

To learn more about how Microsoft Azure Arc–enabled infrastructure can help your organization be more secure, visit www.azure.com/hci.

To learn more about the Intel technologies that power Azure Arc–enabled infrastructure, visit https://www.intel.com/content/www/us/en/security/overview.html.

Microsoft Azure

[1] IBM Security. "Cost of a Data Breach Report 2022." July 2022. https://www.ibm.com/security/data-breach.

[2] Based on internal Microsoft customer research.