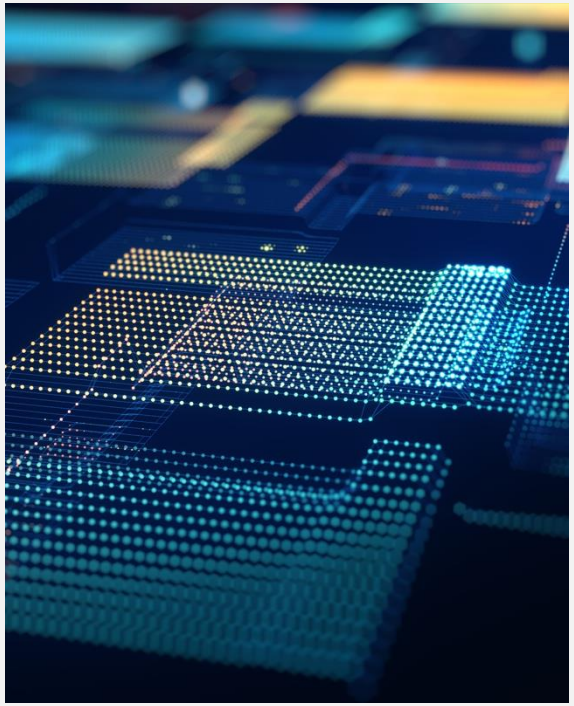
Securing Red Hat workloads on Azure: Leveraging the strength of cloud-native security



February 2025

About our research

To explore how Azure can secure Red Hat® workloads in the cloud, we used publicly available materials and interviews with Microsoft and Red Hat subject matter experts (SMEs).

Our goal was to research the security features that each platform offers and how they intersect to provide enhanced protection for Red Hat on Azure customers.

We found several areas where the two platforms work together to offer a great deal of value, and in our research report, we provide some detail on key security features and benefits available to customers in the Azure and Red Hat ecosystems.

This PowerPoint deck summarizes our report, which you can read at https://facts.pt/G94Mifm.

About PT

Principled Technologies, Inc. (PT) is the leading provider of third-party competitive marketing services for technology.

Our hands-on testing mirrors the way real users work with your product and delivers proof points you and they can count on, while our award-winning competitive marketing contextualizes those claims.

Learn more at www.principledtechnologies.com.

Security principles of Azure

Shared responsibility model

An organization's security team maintains some responsibilities for securing applications, data, containers, and workloads in the cloud, while Azure also takes some responsibility.

Defense in Depth

Azure customers should implement security at many levels to mitigate the risk of any point of failure.

Zero Trust

Zero Trust security always assumes breach and thus requires systems and users to verify every request as though it originated from an uncontrolled network.

Secure Future Initiative (SFI)

SFI is a multi-year commitment that advances the way Microsoft designs, builds, tests, and operates technology to ensure that Microsoft solutions meet the highest possible standards for security.

Types of security we researched

Infrastructure

Azure Boost, Retina, Azure Monitor, and other key tools protect the foundational components of IT environments, including physical and virtual systems, networks, and data centers.

Application

Microsoft Entra ID, Microsoft Defender for Cloud, Red Hat® Insights, and other tools that safeguard software can prevent unauthorized access, data breaches, and malicious exploitation.

Data

Azure uses many approaches to encrypt data at rest and data in transit. Encryption approaches for data at rest include server-side and Azure disk encryption. Encryption approaches for data in transit include transit layer security (TLS) encryption and more.

Code

GitHub Advanced Security for Azure DevOps protects code from vulnerabilities, threats, and malicious attacks to ensure integrity, confidentiality, and availability.

Infrastructure security tools

- Azure Boost
- Azure Monitor
- Retina
- Azure Bastion
- Azure Firewall
- Azure Network Security Groups
- Azure Policy
- Azure Arc

Azure Boost, which offloads server virtualization processes onto purpose-built software and hardware, contains several features that could improve the security of Azure Virtual Machines.

Azure Monitor collects, analyzes, and responds to monitoring data from Azure and on-premises environments.

Retina, the cloud-agnostic, open-source Kubernetes® network observability platform, uses the enhanced Berkeley Packet Filter technology for deep visibility at the kernel level to monitor application and network health and security.

Azure Bastion, a fully managed platform-as-a-service solution, can provide secure access to Azure VMs without exposing them to public IP addresses.

Infrastructure security tools

- Azure Boost
- Azure Monitor
- Retina
- Azure Bastion
- Azure Firewall
- Azure Network Security Groups
- Azure Policy
- Azure Arc

Azure Firewall and Azure Network Security Groups help secure Azure virtual networks by filtering and managing network traffic while offering threat protection.

Change management and policy enforcement

- **Azure Policy (compliance and governance)** can enforce organizational standards while ensuring compliance across large environments.
- **Azure Arc (single-pane management)** provides a centralized platform for managing VMs, Kubernetes® clusters, and databases as if they are part of Azure, enabling consistent management, governance, and security across environments.

Data security tools

- Azure Storage SSE
- Azure-managed disk encryption options
- Data-link layer encryption
- TLS encryption in Azure
- RDP sessions
- Secure access to Linux VMs
- Azure VPN encryption
- Azure Backup and disaster recovery
- Confidential computing

Azure uses many approaches to encrypt data at rest and data in transit. Data at rest encryption approaches include server-side and Azure disk encryption. Data in transit encryption approaches include TLS encryption and more.

Data at rest

For most scenarios, Microsoft recommends using server-side encryption (SSE) features for ease of use in protecting your data.

- **Azure Storage SSE:** Azure Storage uses SSE to “automatically encrypt your data when it is persisted to the cloud.”
- **Azure-managed disk encryption options:** Azure offers Azure Disk Storage SSE, Encryption at host, Azure Disk Encryption, and more.

Client-side encryption refers to data encryption performed outside of Azure. Customers manage keys, helping prevent cloud service providers (CSPs) from decrypting data.

Data security tools

- Azure Storage SSE
- Azure-managed disk encryption options
- Data-link layer encryption
- TLS encryption in Azure
- RDP sessions
- Secure access to Linux VMs
- Azure VPN encryption
- Azure Backup and disaster recovery
- Confidential computing

Data in transit

- **Data-link layer encryption:** Azure encrypts hardware in its data centers to help secure data moving between them.
- **TLS encryption in Azure:** Azure customers can use TLS protocol to protect data in transit between the customer and Azure.
- **Remote Desktop Protocol (RDP) sessions:** Users with Windows or Linux VMs on Azure can sign-in to their systems securely via RDP.
- **Secure access to Linux® VMs with SSH:** Customers can use Secure Shell (SSH), an encrypted connection protocol, to connect to Linux VMs running on Azure.
- **Azure VPN encryption:** Users can create a secure tunnel that protects the privacy of data being sent across the network.

Data security tools

- Azure Storage SSE
- Azure-managed disk encryption options
- Data-link layer encryption
- TLS encryption in Azure
- RDP sessions
- Secure access to Linux VMs
- Azure VPN encryption
- Azure Backup and disaster recovery
- Confidential computing

Azure Backup and disaster recovery

Azure offers Azure Backup and Azure Site Recovery to help customers running Red Hat workloads on Azure with disaster recovery. Azure Backup backs up and restores data on Azure while Azure Site Recovery facilitates seamless disaster recovery for applications, helping organizations maintain business continuity during outages.

Confidential computing

Confidential computing refers to the prevention of unauthorized access to data in use and in memory, rather than at rest or in transit (both of which Azure already encrypts).

Application security tools

- WAF
- Microsoft Entra ID
- Confidential containers
- Microsoft Defender for Cloud
- Microsoft Defender for Endpoint on Linux
- Microsoft Defender for Storage
- Microsoft Sentinel
- Red Hat Insights

Web Application Firewall (WAF) provides security without modifying backend code, which enables organizations to protect their applications seamlessly.

Microsoft Entra ID is a cloud-based identity and access management service allowing users to access both external and internal resources, such as Azure and Microsoft 365 (external) or apps developed within a user's own organization (internal).

Confidential containers, like confidential VMs, provide enhanced data security, privacy, and integrity for workloads in them.

Application security tools

- WAF
- Microsoft Entra ID
- Confidential containers
- Microsoft Defender for Cloud
- Microsoft Defender for Endpoint on Linux
- Microsoft Defender for Storage
- Microsoft Sentinel
- Red Hat Insights

Vulnerability management tools

Microsoft Defender for Cloud, a cloud-native application protection platform (CNAPP), performs continuous security assessments of connected resources and provides security recommendations for any detected vulnerabilities.

Microsoft Defender for Endpoint on Linux provides threat and vulnerability detection and mitigation features.

Microsoft Defender for Storage addresses malicious file uploads, sensitive data accessibility, and data corruption.

Microsoft Sentinel is a cloud-native security information and event management solution for security orchestration, automation, and response.

Red Hat Insights helps organizations better manage and optimize hybrid-cloud environments.

Code security tools

GitHub Advanced Security for Azure DevOps

- Secret scanning push protection
- Repository secret scanning
- Alert system for secrets
- Credential pair detection
- Dependency scanning
- Code scanning

GitHub Advanced Security for Azure DevOps, a CNAPP, enables developer, security, and operations (DevSecOps) teams to protect code with the following:

- **Secret scanning push protection** actively monitors code pushes.
- **Repository secret scanning** analyzes repositories for accidentally committed secrets, generates a single alert per unique credential across branches and commit history, and provides detailed remediation guidance
- **Alert system for secrets** notifies users of detected secrets in repositories from many service providers.
- **Credential pair detection** scans for paired credentials, such as API keys and secrets, to ensure both parts are present.
- **Dependency scanning** detects direct and transitive open-source dependencies, flags associated vulnerabilities, and generates detailed alerts with severity, affected components, and Common Vulnerabilities and Exposures (CVE) information in the build log.
- **Code scanning** uses the CodeQL static analysis engine to identify code-level vulnerabilities and automates security checks with detailed alerts for proactive remediation.

Azure and Red Hat integration points and compatibilities

Red Hat Enterprise Linux® compatibility with Azure confidential VM provides hardware-based isolation, OS disk encryption, and more.

Integrating Microsoft Entra and Red Hat Identity Management enables IT teams to provide and centralize administrative functionality and user maintenance.

Users can leverage Microsoft Defender for Cloud for system auditing, security management, and threat protection. Users can also connect Red Hat on Azure VMs to the Red Hat Insights automatically for monitoring.

See more examples in the report.

How customers win from the Microsoft and Red Hat partnership

Get integrated support for Red Hat workloads on Azure

Red Hat and Microsoft share an integrated, co-located support team that serves as a unified contact point for Red Hat ecosystems running on Azure. This team provides expertise, knowledge, and joint support models.

Follow compliance regulations with Azure Marketplace for Red Hat images

Microsoft and Red Hat engineering teams work closely to build standard images within the Azure Marketplace.

Receive partner architecture guidance

Microsoft and Red Hat have partnered to create a ready-made starting point called Landing Zone for Red Hat Enterprise on Linux.

Principled Technologies®

Facts matter.®

Read the report at https://facts.pt/G94Mifm ▶