INCREASE SECURITY OF PUBLIC CLOUD WORKLOADS WITH RED HAT AND MICROSOFT

PARTNER TECHNOLOGY OVERVIEW

More than

7.1 billion

identities were exposed in data breaches during the past eight years.[1]

Red Hat Enterprise Linux is the world's leading open source operating system trusted by

90%

of the Fortune 500.[2]

CONNECTED ENVIRONMENTS INCREASE SECURITY RISKS

Businesses worldwide continue to add highly connected public cloud resources to their IT environments, with 64% planning to move more than 100 applications to public cloud platforms.[3] Cloud adoption has many benefits, including improved resilience, reduced cost of ownership, and greater infrastructure and business agility. Even so, many organizations remain concerned about providing adequate security and privacy for applications and data in cloud environments. The Cloud Security Alliance (CSA) identified some of the top security threats to cloud computing as:[4]

- Insufficient identity, credential, and access management.
- Data breaches.
- Advanced persistent threats.
- Shared technology vulnerabilities.
- System vulnerabilities.
- Insecure interfaces and application programming interfaces (APIs).

Application and data protection in cloud environments depends on the underlying hardware and software. Choosing the right cloud infrastructure can alleviate security threats and help protect your applications and data. Together, Red Hat and Microsoft deliver a production-ready cloud foundation that effectively addresses these security concerns.

INCREASE CLOUD SECURITY WITH RED HAT AND MICROSOFT

Red Hat® Enterprise Linux® and Microsoft Azure form an enterprise-grade platform for modern, cloud-based applications. With built-in security and management technologies, Red Hat Enterprise Linux offers a consistent, open source foundation across bare-metal, virtualized, container, and public and private cloud resources. As the most-deployed commercial Linux distribution in public cloud environments, it delivers performance and stability to cloud workloads.[5] Microsoft Azure is a global network of some of the world's largest datacenters. It provides cloud services and built-in management tools using a trusted foundation based on intelligent insights, certifications, and physical, operational, and infrastructure security.

[1] *"Internet Security Threat Report." Symantec. April, 2017.* symantec.com/security-center/threat-report.

[2] *Red Hat client data and Fortune 500. 2017.* fortune.com/fortune500.

[3] *"Cloud Migration Is Actively Embraced, But Not For Everything." Forrester. October, 2017.* redhat.com/en/resources/cloud-migration-embraced-analyst-paper.

[4] *"The Treacherous Twelve." Cloud Security Alliance. 2017.* downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf.

[5] *"The state of Linux in the public cloud for enterprises." Red Hat. February 2018.* redhat.com/en/resources/state-of-linux-in-public-cloud-for-enterprises.

> *“The fact that Azure supports various Red Hat solutions including Red Hat Enterprise Linux, as well as Windows Server, was one of the key criteria for selecting cloud vendors.”*[6]
>
> TOMOHIRO KATABIRA, BUSINESS STRATEGIES DIVISION, CLOUD BUSINESS DEVELOPMENT DEPARTMENT, VISIONARTS, INC.

Red Hat and Microsoft help protect your cloud environment and manage threats. Comprehensive and effective best practices minimize the presence and limit the impact of vulnerabilities. A rich set of security-related features hardens and safeguards your most sensitive applications and data.

This technology overview will detail how the combination of Red Hat Enterprise Linux and Microsoft Azure alleviate top cloud security threats faced by enterprises today.

INSUFFICIENT IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

Identity, credential, and access management—using techniques such as multi-factor authentication, strong passwords, and automated key, password, and certificate rotation—is the first line of defense in preventing data breaches and cyber attacks. Red Hat Enterprise Linux and Microsoft Azure offer a variety of control mechanisms to help limit access to your data and applications.

Enabled by default, Security-Enhanced Linux (SELinux) is a core component of Red Hat Enterprise Linux. The SELinux mandatory access control (MAC) architecture enforces separation of information based on confidentiality and integrity requirements. With the identity management feature set in Red Hat Enterprise Linux, you can centrally define, administer, and audit access control policies and privileges for users, machines, and services. Microsoft Active Directory integrates with this feature set to serve as your identity hub across both Linux and Windows environments.

Microsoft Azure Multi-Factor Authentication (MFA) is a two-step verification solution that provides a simple sign-in process. Strong authentication via multiple methods—phone call, text message, or mobile application—helps protect data and applications and reduces the likelihood of access for a compromised credential. Role-based access controls (RBAC)—provided in both Red Hat Enterprise Linux and Microsoft Azure—assign specific permissions to users, groups, and applications to establish least privileges and maintain separation of duties between users with different roles.

DATA BREACHES

Data breaches—the unauthorized or unlawful loss, alteration, destruction, disclosure, or acquisition of sensitive, protected, personal or confidential information—may be the result of a targeted attack, human error, application vulnerabilities, or poor security practices. If a data breach occurs, advanced encryption technologies in Red Hat Enterprise Linux and Microsoft Azure help keep your data safe, both at rest and in motion, across your on-premise and cloud resources.

Red Hat Enterprise Linux includes a Federal Information Processing Standards (FIPS)-certified implementation of the Linux Unified Key Setup (LUKS) specification for full-disk encryption. This solution increases protection for cloud data at rest. The Network-Bound Disk Encryption (NBDE) feature decrypts LUKs encrypted boot or root volumes without manual intervention. Microsoft Azure Disk Encryption guards the operating system and data at rest by encrypting Windows and Linux Infrastructure-as-a-Service (IaaS) virtual machine disks. Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols and virtual private networks (VPNs) offer increased security for data exchange between your on-premise and Microsoft Azure infrastructures.

[6] *“Sony Global Manufacturing & Operations support service combines the cloud with open source software to reduce costs.” Microsoft. September 2017.* customers.microsoft.com/en-us/story/sony-visionarts.

Red Hat Enterprise Linux is Common Criteria and FIPS 140-2 certified. It is the first operating system to be Common Criteria-certified with Linux Container Framework Support.[7]

ADVANCED PERSISTENT THREATS

Advanced persistent threats (APTs) are cyberattacks in which an unauthorized person accesses a network for an extended period of time. The intention of an APT is not to cause damage, but to steal data. APTs often adapt to changing security measures to avoid detection. Together, Red Hat and Microsoft help defend systems and networks from cyberattacks and preserve data and application integrity.

As a critical, security-focused component of Red Hat Enterprise Linux, ExecShield provides mechanisms and technologies that can disrupt entire classes of vulnerabilities. Advanced technologies—including No eXecute (NX) memory permission, address space layout randomization (ASLR), and GNU Compiler Collections (gcc) and GNU C Library (glibc) hardening—can stop automated attacks from worms and viruses. To protect the host file system, SELinux blocks read and write access to host files by unauthorized processes.

Additionally, the web application firewall (WAF) in the Microsoft Azure Application Gateway helps safeguard applications from common web-based attacks and defends against bots, crawlers, and scanners.

SHARED TECHNOLOGY VULNERABILITIES

In public cloud environments, multiple tenants often share physical servers and infrastructure resources. While this increases scalability and reduces cost, it introduces the risk of running sensitive applications on resources shared with malicious users. Red Hat and Microsoft offer increased security, confidentiality, privacy, and integrity for workloads in multitenant cloud environments.

Microsoft Azure compute instances offer isolation at multiple levels to increase data protection without reducing configuration flexibility. All customer applications run in Microsoft Hyper-V virtual machines. A hypervisor isolates all Microsoft Hyper-V virtual machines from both physical resources and from each other. In addition, the Microsoft Azure Active Directory architecture segregates customer data by issuing each subscriber a distinct, dedicated, and separate directory service. These features offer protections against users of one directory service accidentally or maliciously accessing data in another directory.

SYSTEM VULNERABILITIES

System vulnerabilities are exploitable software bugs that allow unauthorized access to resources. Susceptibilities within public cloud foundations, including operating systems and virtualization software, pose security risks for all applications and data. Red Hat and Microsoft have well-established processes and best practices—administered by dedicated teams of experts working together and in collaboration with customers, partners, and the open source community—to identify and resolve system vulnerabilities.

[7] *"Red Hat Achieves Common Criteria Security Certification for Red Hat Enterprise Linux 7." October, 2016.* redhat.com/en/about/press-releases/red-hat-achieves-common-criteria-security-certification-red-hat-enterprise-linux-7.

Learn more about the Red Hat Product Security team at access.redhat.com/security/overview.

Working closely with upstream projects, the Red Hat Product Security team identifies and monitors potential security issues and ensures the integrity of recommended remediation processes. In 2016, the team investigated more than 2,600 potential vulnerabilities across all Red Hat products and addressed 1,346 issues through more than 600 security advisories.[8] The team releases security patches for currently supported versions of Red Hat products. Red Hat Enterprise Linux versions 5, 6, and 7 include 10 years of support in Production Phases 1, 2, and 3 followed by an Extended Life Phase, unless otherwise noted.[9] Red Hat Enterprise Linux versions 5 and 6 offer Extended Life-cycle Support (ELS) annual subscriptions to extend limited services beyond Phase 3.[9]

Red Hat also helps reduce vulnerabilities through comprehensive management tools. OpenSCAP—Red Hat's National Institute of Standards and Technology (NIST)-certified scanner—automates detection and remediation of vulnerabilities and configuration security baselines for Red Hat Enterprise Linux systems. Red Hat Satellite delivers complete life-cycle management for your Red Hat infrastructure, keeping it up to date and simplifying compliance with applicable corporate and regulatory standards.

The Microsoft Security Response Center (MSRC) identifies, monitors, and resolves security incidents and vulnerabilities in Microsoft software. When an incident occurs, the MSRC leads the worldwide Software Security Incident Response Process (SSIRP). Through the SSIRP, security teams across Microsoft quickly and effectively investigate, analyze, and resolve issues. As a core Microsoft Azure security feature, alerts and recommendations from Microsoft Azure Security Center—including actionable recommendations from the MSRC, prioritized alerts from integrated partner solutions, and virtual machine update notifications—help remediate vulnerabilities. Microsoft Azure Security Center adaptive application controls block malware and other unwanted applications by applying whitelisting recommendations tailored to your specific workloads.

INSECURE INTERFACES

In public cloud environments, customers manage and interact with cloud resources through software user interfaces (UIs) and APIs. Bad actors can potentially exploit these interfaces to circumvent cloud security policies. Red Hat and Microsoft design, build, and test UIs and APIs to defend against both accidental and malicious attempts to bypass security measures.

Red Hat Enterprise Linux implements open APIs that adhere to industry standards. Working with the open source community, Red Hat builds security features into the operating system core. Furthermore, every release of Red Hat Enterprise Linux undergoes extensive quality assurance testing to help prevent potential vulnerabilities.

Microsoft Azure includes tools to create and analyze security-focused applications. The Threat Modeling Tool, part of the Microsoft Security Development Lifecycle (SDL), helps identify and mitigate possible issues. Microsoft performs penetration testing on Microsoft Azure and allows end-user application testing through multiple methods, including endpoint fuzz testing and port scanning as well as vulnerability testing based on the Open Web Application Security Project (OWASP).

[8] *"Red Hat Product Security Risk Report: 2016." Red Hat. 2017.* redhat.com/cms/managed-files/su-2016-security-risk-report-f6404cw-201703-v2-en.pdf.

[9] *For further details on the Red Hat Enterprise Linux support policy, see:* access.redhat.com/support/policy/updates/errata/#exceptions.

LEARN MORE

As organizations move critical applications and sensitive data to public cloud infrastructure, security concerns persist—and can even increase. Together, Red Hat and Microsoft mitigate threats to cloud workloads. Dedicated security teams, extensive testing, and well-established processes and best practices identify and remediate vulnerabilities. Modern, advanced security features and tools deter threats and safeguard applications and data. To discover how you can improve cloud-based application security, contact your Red Hat or Microsoft sales representative.

Learn more at redhat.com/en/insights/security and azure.com/redhat.

CERTIFICATION AND COMPLIANCE DOCUMENTATION

- Red Hat Customer Portal: access.redhat.com/articles/2918071
- Microsoft Trust Center: microsoft.com/en-us/trustcenter/compliance/complianceofferings

ABOUT RED HAT

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

CONNECT WITH RED HAT

redhat.com
facebook.com/redhatinc
@redhat
linkedin.com/company/red-hat

ABOUT MICROSOFT

Microsoft is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more.

CONNECT WITH MICROSOFT

microsoft.com
facebook.com/Microsoft
@Microsoft
linkedin.com/company/Microsoft