I.T. SECURITY IN A DIGITAL WORLD

DATASHEET

STAYING COMPETITIVE AND SECURE IN A VULNERABLE LANDSCAPE

As customers demand digital access and more software is delivered as a service, organizations need new technologies to compete, but adopting them makes security and regulatory compliance more difficult. In addition, securing devices and infrastructure that are outside of your environment is a key challenge.

IT teams must manage and secure a continuously evolving landscape. New vulnerabilities emerge regularly, from external attacks and internal issues caused by human error or malice. However, business often views security teams as blockers to rapid productivity, rather than supporters.

IT security must evolve to better support business while ensuring confidentiality, integrity, and availability by:

- Balancing risk and security to optimize for resilience and agility, knowing that complete security is not possible.
- Ensuring proactive and reactive security with automation.
- Involving security professionals with the line of business throughout the IT and application life cycle.
- Using data and analytics to anticipate, detect, and respond to security issues and support IT and business collaboration to evaluate and manage risk.

With these capabilities, IT teams can achieve continuous security throughout IT environments at all stages of development and deployment.

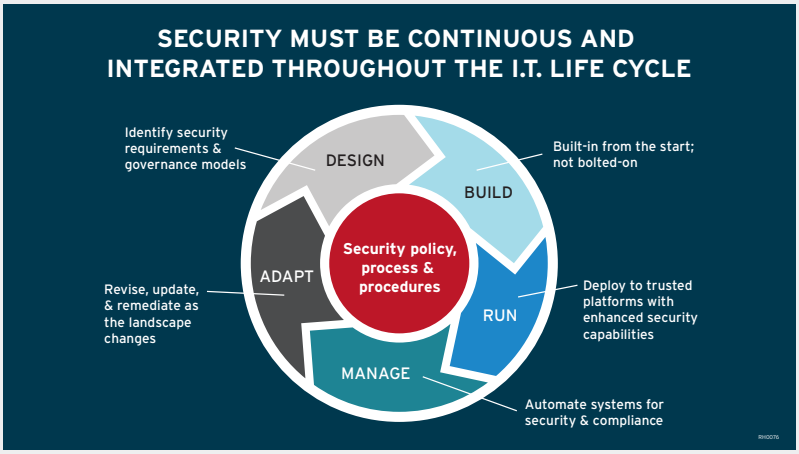

Figure 1. A continuous IT security process offers protection at every stage.

LEARN MORE ABOUT I.T. SECURITY

- Guide to open source IT security: redhat.com/en/technologies/guide/it-security
- Security topic page: redhat.com/en/insights/security

In a global, connected IT landscape, robust security at the source—the application stack—is critical.

SECURITY AT EVERY STEP

Red Hat offers a tested, supported portfolio of stable open source infrastructure and application development solutions for enterprise adoption of emerging technology. With Red Hat® products and services, organizations can take advantage of security built into each phase of the application life cycle.

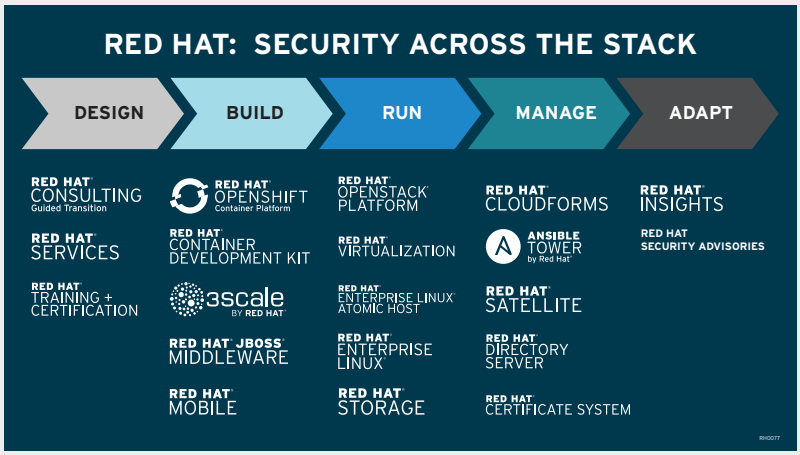

Figure 2. Red Hat's enterprise-ready open source portfolio offers security at all stages of application development and deployment.

PHYSICAL AND CLOUD INFRASTRUCTURE

Red Hat Enterprise Linux® is FIPS 140-2 and Common Criteria certified, simplifying compliance with a variety of government standards.[1] Security-Enhanced Linux (SELinux) is integrated into Red Hat Enterprise Linux. Originally developed by the National Security Agency (NSA), SELinux enables secure multitenancy to help administrators enforce mandatory access controls (MAC) for every user, application, process, and file. Red Hat Enterprise Linux also provides a dynamically managed firewall and verifiable end-to-end encryption, including SHA-512-based password hashes, file-system encryption, and NSA Suite B cryptography enhancements and certifications.

Red Hat Virtualization delivers secure virtualization using the labeling capabilities of SELinux to restrict a virtual machine's (VM's) access to resources outside of its boundaries, such as host machine data or other VMs.

Red Hat OpenStack® Platform combines the benefits of Red Hat Enterprise Linux with the fastest-growing cloud infrastructure platform. OpenStack is dependent on its underlying Linux operating system for everything from service operation and access to hardware resources to system performance, stability, and security.

1 *redhat.com/en/technologies/industries/government/standards*

CONTAINER PLATFORMS

Red Hat Enterprise Linux 7 provides container isolation using four key features: SELinux, Linux namespaces, Linux cgroups, and Secure Computing Mode (seccomp).

Red Hat Enterprise Linux Atomic Host provides a minimum operating system for running containers, reducing the attack surface for additional protection.

Red Hat OpenShift Container Platform uses multitenancy and security models within Red Hat Enterprise Linux to provide container isolation as well as extensive control over the compute and storage resources available to each OpenShift application.

IDENTITY AND ACCESS MANAGEMENT

Identity Management in Red Hat Enterprise Linux is an extension of a generic Lightweight Directory Access Protocol (LDAP) provider and offers all of the configuration options for an LDAP provider.

Red Hat Directory Server is an LDAP-compliant server that centralizes user identity and application information. It provides an operating system-independent, network-based registry for storing application settings, user profiles, group data, policies, and access control information.

Red Hat Certificate System offers a public key infrastructure (PKI) that serves as a scalable, secure framework to establish and maintain trusted identities, keep communications private, and manage certificate life cycles—including issue, renew, suspend, revoke, archive, and recover capabilities. Red Hat Certificate System manages single- and dual-key X.509v3 certificates needed to handle robust authentication, single sign-on (SSO), and secure communications.

OpenStack Identity (Keystone) acts as a common authentication system across cloud operating systems and can integrate with existing back-end directory services, such as LDAP. It supports multiple forms of authentication, including standard username and password credentials, token-based systems, and Amazon Web Services (AWS)-type credentials.

STORAGE

Red Hat offers both file and block storage with superior data protection delivered through features such as SELinux, access control lists, and embedded encryption capabilities. With Red Hat, organizations can deploy the same storage on premise, in Linux containers, or in private, public, and hybrid clouds.

MIDDLEWARE AND APPLICATION SERVICES

Directly supporting applications, middleware plays a key role in application security, especially for applications that rely on Java™.

Red Hat JBoss® Middleware offers a role-based Java Platform, Enterprise Edition (Java EE) security model based on Java Authentication and Authorization Service (JAAS). JAAS delivers a framework for providing authentication and authorization for all Java applications, ensuring that the client has the necessary permissions to access a secured resource.

- **Red Hat JBoss Core Services Collection** provides entitlements to many popular capabilities frequently deployed with Red Hat JBoss Middleware products. A web SSO server provides a SAML 2.0- or OpenID Connect-based identity provider. In addition, Red Hat JBoss Core Services Collection includes OpenJDK to offer cryptographic algorithms and interfaces for Red Hat JBoss Middleware.
- **Red Hat JBoss Fuse A-MQ** is used as a critical component to securely and reliably collect and appropriately route all continuous monitoring data.

Red Hat Mobile Application Platform provides central control over security and policy management, Mobile Backend-as-a-Service (MBaaS) integration with enterprise systems, and several cloud deployment options.

3scale API Management by Red Hat protects back-end application programming interface (API) servers with strict traffic control. 3scale's architecture provides multiple options for traffic control—including open source gateways, a hosted cloud service, plug-ins, and a content delivery network (CDN). With this offering, organizations can protect individual methods, distribute calls to multiple back ends, and monitor all traffic. The result is a centralized overview that offers powerful traffic control within the data flow.

MANAGEMENT

Red Hat Satellite and **Red Hat CloudForms** can check security configuration settings and examine systems for signs of compromise using OpenSCAP standards and specification-based rules. OpenSCAP can also be used to automate and monitor system configurations to meet additional security and regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) or Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs).

Ansible Tower by Red Hat can configure systems, deploy software, and orchestrate more advanced IT tasks such as continuous deployment (CD) or zero downtime rolling updates across the enterprise. Ansible can inspect Windows and Linux endpoints for vulnerabilities and security compliance.

Red Hat Insights is an analytics offering that helps organizations proactively manage their IT infrastructures. Comparisons against Red Hat's constantly expanding knowledgebase are used to provide real-time assessment of performance, availability, stability, and security risks. After thorough analysis, any critical issues requiring attention are prioritized by severity and clearly displayed in an easy-to-use interface.

Red Hat security advisories deliver proactive notification about security flaws that affect Red Hat products and services. Red Hat provides patches to supported versions of Red Hat products—frequently on the same day the vulnerability is first published. As a result, Red Hat minimizes disruption by helping enterprises continue to work with current versions safely, then upgrade to newer versions when ready.

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.

NORTH AMERICA
1 888 REDHAT1

EUROPE, MIDDLE EAST, AND AFRICA
00800 7334 2835
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
apac@redhat.com

LATIN AMERICA
+54 11 4329 7300
info-latam@redhat.com

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

redhat.com
INC0476725_v3_1216