Red Hat
Enterprise Linux 8

Brief

Build a security-focused datacenter

Red Hat Enterprise Linux 8 delivers security features to help protect your IT and business

Security is the top funding priority in 2019 according to IT decision makers at surveyed organizations.[1]

Red Hat Enterprise Linux 8 includes advanced security features to help protect your IT and your business:

- Secure default compiler flags and static code analysis
- Consistent cryptographic policies
- Transport Layer Security (TLS) 1.3 support
- Session recording

Datacenter security starts with your operating system

Security threats continue to grow. In fact, 33% of CIOs report that their organization has been subjected to a major cyber attack in the last two years.[2] As a result, security is the top funding priority in 2019 for surveyed organizations.[1]

A more secure datacenter begins with your operating system. Red Hat® Enterprise Linux® provides security technologies, controls, certifications, and the ongoing support of the Red Hat Product Security team to help safeguard your organization. Built-in security features help you proactively protect your datacenter environment. Mandatory access controls and application isolation in secure containers help you combat intrusions and meet regulatory compliance. Your Red Hat Enterprise Linux subscription also gives you continuous vulnerability monitoring with rapid security updates when critical issues arise.

Red Hat Enterprise Linux 8 adds even more security features—such as new compiler flags, improved cryptographic policies, advanced auditing, and updated protocols—to defend your IT and business.

Secure default compiler flags and static code analysis

Through static code analysis and new compiler flags, Red Hat Enterprise Linux delivers more security by default. Prior to release, Red Hat performs static code analysis across the entire Red Hat Enterprise Linux code base, including the core operating system and all supplied utilities. The static code analysis tool identifies errors in programming style, memory reference methods, and input stream validation to ensure compliance with coding best practices. This prevents many security flaws from shipping in Red Hat Enterprise Linux. Red Hat also contributes these fixes and improvements back to the upstream community to strengthen those distributions.

To avoid many common security vulnerabilities, Red Hat applies special compiler flags when compiling the Red Hat Enterprise Linux source code. These flags use Position Independent Execution (PIE) and Relocate Read-Only Object (RELRO) functionality to run applications and assign memory segments in a nonpredictive manner. This helps to prevent stack smashing, mitigate memory corruption, and provide control flow integrity hardware support. It also randomizes the full address space layout across Red Hat Enterprise Linux 8 and all running applications. As a result, it is more difficult for unauthorized parties to predict and access the locations of applications and data.

Red Hat Enterprise Linux 8 also contains Annobin and Annocheck functions to incorporate compiler and build information into the binary, allowing you to self-inspect and validate the product.

Consistent cryptographic policies

Red Hat Enterprise Linux 8 provides a simple way to ensure system-wide, consistent cryptography settings to address compliance requirements. New cryptographic profiles—legacy, default, future, and FIPS140 (Federal Information Processing Standard Publication 140-2)—make it easier to manage and automate cryptographic settings across your environment, reducing the risk of errors. Rather than configuring libraries manually, you can use a single command to change cryptographic

1 *Qualtrics and Red Hat, Global IT Trends & Priorities Research, November 2018.*

2 *Harvey Nash and KPMG, "CIO Survey 2018: The transformational CIO," 2018.* home.kpmg/xx/en/home/insights/2018/06/harvey-nash-kpmg-cio-survey-2018.html.

settings – including allowed cryptographic key lengths, hashes, parameters, protocols, and algorithms – without modifying your applications. Of course, you can still override these settings on a case-by-case basis as needed.

Transport Layer Security 1.3 support

Transport Layer Security (TLS) is the most widely used transport protocol on the web. The latest version of the protocol, TLS 1.3, includes many improvements, but also requires significant changes to the underlying operating system. Red Hat Enterprise Linux 8 was completely redesigned to implement TLS 1.3 throughout. All applications were also recompiled to use the new protocol.

Red Hat Enterprise Linux 8 supports TLS 1.3 in the OpenSSL 1.1.1, GNUTLS (GNU Transport Layer Security), and NSS (Network Security Services) cryptographic libraries. Accordingly, any applications that consume these libraries will use TLS 1.3. Additionally, Red Hat updated several subsystems – including Apache, GNOME, Perl, Python, Ruby, and Java/OpenJDK – to use TLS 1.3.

With TLS 1.3 enabled, Red Hat Enterprise Linux 8 provides faster, more secure transport and prevents man-in-the-middle and replay attacks, even when the observer has the encryption key.

Session recording

Session recording permits greater security compliance and auditing. Red Hat Enterprise Linux 8 provides terminal session recording integrated with auditing. This feature records both the input (optional) and output of users' shell sessions – including text window resizing and timing – and correlates them with the environment and state of the system. Sessions are recorded as JSON (JavaScript Object Notation) formatted audit records via file, system journal, or syslog. You can quickly export records off the system for increased security and tamper-proofing.

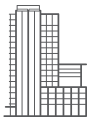
Integration with System Security Services Daemon (SSSD) and Red Hat Identity Management allows you to record sessions on a per-user or per-group basis. Sessions can be played back via a terminal window or the new web console. You can also manage session recording settings using the web console. This provides full auditability of changes and easier, more complete compliance, security monitoring, and debugging.

Learn more

Security continues to be a top concern for all organizations. With a security-focused design, Red Hat Enterprise Linux can help you better protect your datacenter and your business.

Find out more at redhat.com/en/technologies/linux-platforms/enterprise-linux.

Already a customer? Visit access.rehat.com/products/red-hat-enterprise-linux/.



About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

North America
1 888 REDHAT1
www.redhat.com

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
@redhat
linkedin.com/company/red-hat

redhat.com
F17208_v1_0519_KVM