Red Hat
Enterprise Linux

Top Red Hat Enterprise Linux features for implementing zero trust architectures

Contents

1 Protect your organization with zero trust

2 What is zero trust?

3 Operating systems: The foundation for zero trust

4 Identity management: Access control for IT resources

5 Get started with zero trust

Protect your organization with zero trust

As organizations expand their use of public clouds, mobile devices, and remote work practices, traditional network perimeters fragment, bringing new security challenges to IT environments.

Organizations increasingly encounter bad actors who attempt to exploit vulnerabilities that exist due to outdated security paradigms like single-factor authentication, implicit trust, perimeter-based architectures, and inadequate user and event behavior tracking. As security threats and the impact of breaches continue to grow, organizations recognize the need for a more robust and proactive security strategy. In fact, more than 50% of cybersecurity professionals view improved identity and access management and secure application access as current security priorities.[1]

Zero trust proposes a fundamental shift in how we perceive and establish trust within a network, rejecting the assumption that everything inside is safe and everything outside is not. It challenges the traditional model by assuming that no user or asset can be inherently trusted within or outside of a network perimeter. Instead, users and assets must be continuously authenticated and authorized regardless of their location or network access.

This e-book discusses considerations for establishing zero trust architectures in Linux® environments and how Red Hat® Enterprise Linux can help you protect your IT environment and organization.

The high cost of a changing threat landscape

US$4.45 million
Average cost of a data breach across industries and regions in 2023[2]

US$180,358
Average reduction in breach costs when effective identity and access management is deployed[2]

82%
Share of breaches that involved data stored in cloud environments or across multiple environments[2]

51%
Percentage of organizations planning to increase security investments as a result of a breach[2]

1 *Cybersecurity Insiders sponsored by Fortra. "2023 Zero Trust Security Report," 2023.*

2 *IBM Security. "Cost of a Data Breach Report 2023," July 2023.*

What is zero trust?

Zero trust is an architectural pattern that applies security to each asset, rather than exclusively managing security at a network perimeter or through a centralized security management solution. The foundational tenet of the zero trust model is that no actor, system, network, or service operating inside or outside the security perimeter is implicitly trusted. For one resource to connect to another resource, the session must be both authenticated and authorized to establish explicit trust.

How does zero trust work?

Identity and access management is at the core of zero trust architectures. Zero trust architectures should deny access to assets by default. Every subject that wants to interact with an asset must request explicit access for that specific interaction and the risk of that interaction should be evaluated before allowing access. As such, an understanding of the subject's identity and attributes is critical. You need to determine who is requesting access, which assets they need to access, the purpose of the transaction, and how access should be constrained according to time, method, and function.

Once access decisions are made, you must store, manage, curate, and update identities and identity attributes in a protected and consistent manner. Most organizations use 1 or more identity management, directory server, or credential management systems to administer this information. You should also continually reassess these access decisions to ensure that they remain valid over time.

A zero trust architecture based on these key principles can help you better protect your IT environment and organization:

1. Never trust actors implicitly.
2. Employ a least privilege access strategy.
3. Assume networks and network traffic are compromised by default.

These are the key principles that Red Hat employs to guide zero trust capabilities throughout the entire Red Hat portfolio, including Red Hat Enterprise Linux, Red Hat Insights, and Red Hat Identity Management.

What is a trust boundary?

A trust boundary is any logical separation between components where the subjects participating in an interaction change their trust status, typically between the two states of *trusted* and *untrusted*. Generally, the transition from *untrusted* to *trusted* requires both authentication of the subject's identity and authorization of the subject's right and need to access a specific asset.

Operating systems: The foundation for zero trust

Your operating system is the foundation for your IT environment and zero trust architecture. It provides essential security features, controls user and application access, encrypts sensitive information, and protects secrets to establish and maintain a security-focused computing environment.

This chapter discusses key operating system capabilities for adopting zero trust.

Trusted operating system supply chain

Zero trust models require your operating system to be as secure as possible. To reduce the risk of security vulnerabilities in the operating system, Red Hat Enterprise Linux is delivered using a trusted software supply chain. Static code analysis of the entire operating system identifies errors in programming style, memory reference methods, and input stream validation and ensures compliance with standard coding practices. Extensive quality engineering (QE) testing minimizes security flaws before shipping. Vulnerability patching processes regularly deliver remediation against known issues. Published software bills of materials (SBOMs) help you audit and evaluate the curated, tested components—including source code, open source software and libraries, middleware, and development frameworks—that are part of Red Hat Enterprise Linux.

Mandatory access control

To implement a zero trust architecture, your operating system must be able to isolate and control access to resources on an individual basis. Red Hat Enterprise Linux includes built-in mandatory access controls (MAC) with Security-Enhanced Linux (SELinux), a technology that manages access using centralized security policies. Granular, customizable control over files, processes, users, and applications minimizes the risk of inappropriate privilege escalations, while process isolation and container separation mitigate privilege escalation attacks. And the ability to deny all access by default aligns with zero trust and least privilege principles.

Try generating customized SELinux security profiles for containerized applications.

Access the **interactive lab**.

Application allowlisting

Application allowlisting establishes an index of approved applications and executable files that are permitted to run on a system by a specific user. This practice complements mandatory access controls, which can control application behavior but do not know which applications are trusted. Red Hat Enterprise Linux provides built-in application allowlisting capabilities using File Access Policy Daemon (fapolicyd) to detect and prevent unauthorized applications from running on systems or networks. And, with predefined and customizable allowlist policies, system administrators have more control over the applications running on their servers and networks.

Learn how to approve applications with fapolicyd.

Access the **interactive lab**.

Modern, scalable, policy-based encryption

Data and network traffic encryption increases protection for your IT environment and organization. Several industry standards—including National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140—require system-wide encryption settings. Customizable, policy-based cryptography controls in Red Hat Enterprise Linux let you apply consistent configurations across your systems to help meet your requirements. Default profiles for common security standards simplify compliance. And automated policy application and enforcement streamline management, reduce errors, and control decryption of files and software volumes.

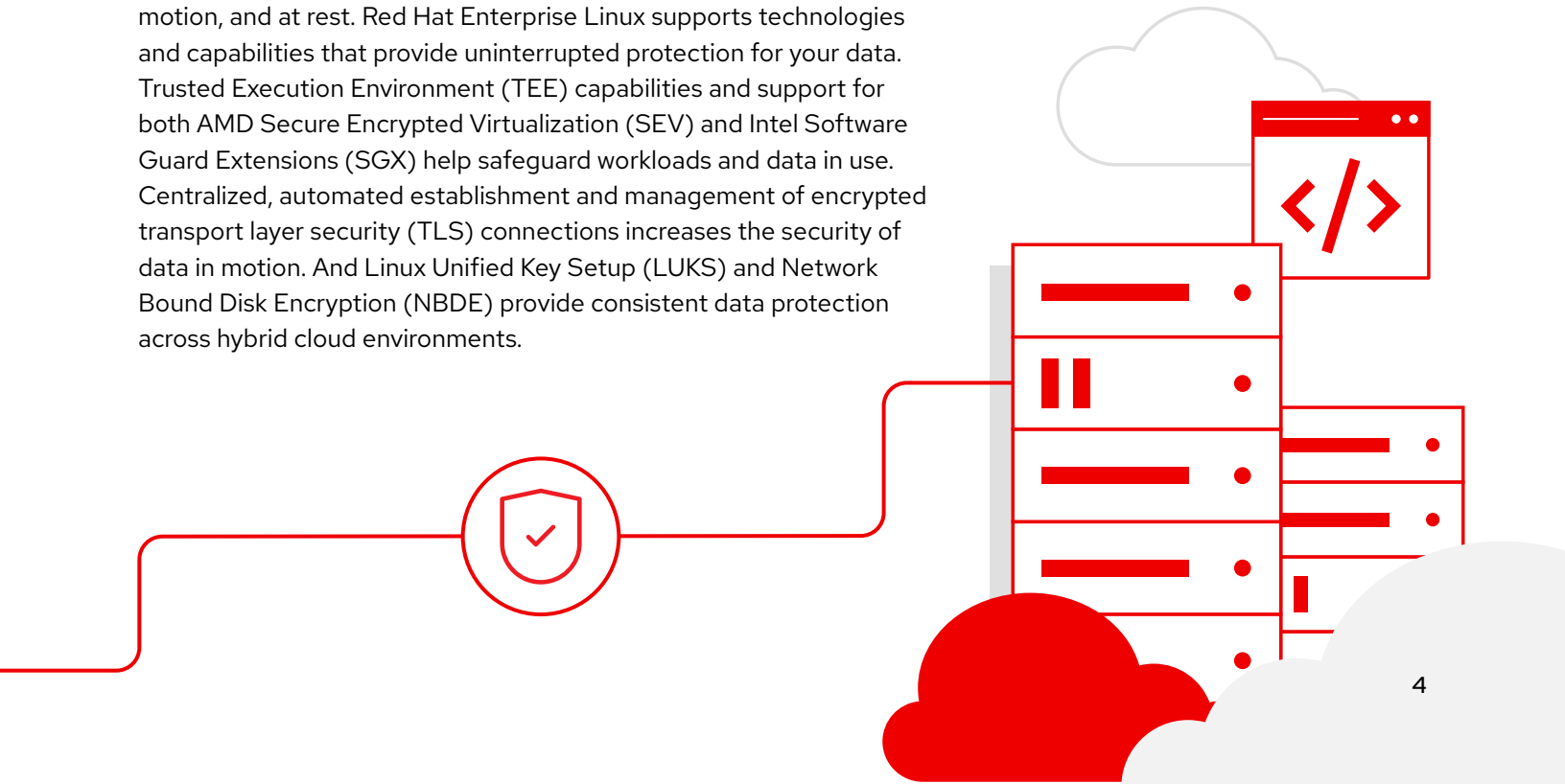
Learn how to use system-wide cryptographic policies.

Access the **interactive lab for configuration**.

Access the **interactive lab for customization**.

Data protection in all stages

Zero trust models require data to be secured at all times—in use, in motion, and at rest. Red Hat Enterprise Linux supports technologies and capabilities that provide uninterrupted protection for your data. Trusted Execution Environment (TEE) capabilities and support for both AMD Secure Encrypted Virtualization (SEV) and Intel Software Guard Extensions (SGX) help safeguard workloads and data in use. Centralized, automated establishment and management of encrypted transport layer security (TLS) connections increases the security of data in motion. And Linux Unified Key Setup (LUKS) and Network Bound Disk Encryption (NBDE) provide consistent data protection across hybrid cloud environments.



Hardware-based root of trust

Hardware-based root of trust, remote attestation, and measured boot technologies help you verify system integrity and ensure that your systems have not been modified or tampered with. Red Hat Enterprise Linux provides key capabilities that support these technologies.

- Move your cryptographic secrets out of software and onto tamper-proof hardware devices like smart cards, hardware security modules (HSMs), and Trusted Platform Modules (TPMs).
- Use TPMs and measured boot capabilities to cryptographically compute and store hashed measurements of secure boot processes and runtime binaries.
- Verify boot measurements with remote attestation agents to determine if systems are compromised before initiating the appropriate remediation actions.

Compliance scanning

Noncompliance with corporate and industry standards and regulations can be both risky and costly for your organization. Red Hat Enterprise Linux includes built-in compliance and vulnerability scanning tools like Open Security Content Automation Protocol (OpenSCAP) to help you automate and simplify audits, find and remediate improperly configured systems, and maintain compliance with less effort. Key features include:

- Predefined and customizable compliance profiles.
- Reporting and baseline-generation capabilities.
- Integration with Red Hat Satellite and Red Hat Insights for management at scale.
- Built-in security baselines for Payment Card Industry Data Security Standard (PCI-DSS), Enhanced Operating System Protection Profile (OSPP), Australian Cyber Security Centre (ACSC) Essential Eight, Center for Internet Security (CIS) Benchmark, Health Insurance Portability and Accountability Act (HIPAA), and Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG).

Try security compliance and vulnerability scanning using OpenSCAP.

Access the **interactive lab**.

Learn how to remediate vulnerabilities with Red Hat Insights.

Access the **interactive lab**.

Automated configuration management

Automation is critical to maintaining consistent security configurations and meeting governance and compliance requirements at scale. Red Hat Enterprise Linux system roles let you automate security configuration and management across hybrid cloud environments and reduce the expertise required to implement a zero trust architecture. This predefined automation content based on Red Hat Ansible® Automation Platform simplifies the configuration of security-focused features like SELinux, NBDE, Secure Shell (SSH), cryptographic policies, and identity and certificate management.

Try Red Hat Enterprise Linux system roles

Access the **interactive lab**.

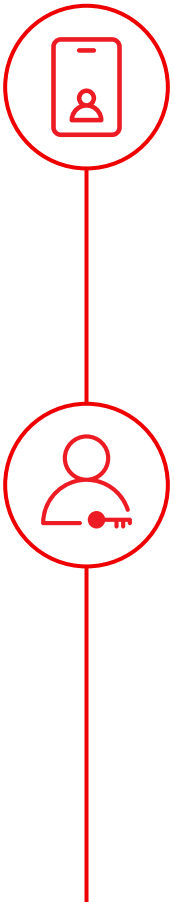
Identity management: Access control for IT resources

Identity management (IdM) solutions ensure that authorized users—and only authorized users—can access the resources they need. By encompassing organization-wide policies and technologies, these solutions properly identify, authenticate, and authorize access to assets through identities, attributes, credentials, and certificates.

This chapter discusses key identity management capabilities for adopting zero trust.

Identity store

A domain controller allows you to manage identities, access, and policies for users, services, and hosts. Included with Red Hat Enterprise Linux, Red Hat Identity Management is a centralized identity store and domain controller that helps reduce administrative overhead, simplify security management, and ensure consistency across your environment. With it, you can store all identities in one place, consolidate operations, and apply policies uniformly across resources and environments. Simplified domain registration lets you create a trusted security boundary, while streamlined authentication improves the overall end user experience.



Single sign-on

In zero trust architectures, each service, device, and server requires separate access authentication. Single sign-on (SSO) systems simplify access by using a central identity service to allow servers to check for verified users. Red Hat Enterprise Linux supports OAuth 2.0 and Red Hat Identity Management to allow users to authenticate once and access multiple services, providing a streamlined experience. Integration with various services—including Red Hat's single sign-on technology, Microsoft AzureAD, and GitHub—lets you continue to use your existing identity services while providing flexibility for the future.

Integration with other identity management systems

Most organizations already use one or more identity management systems for their Linux and Windows environments. Integrating these systems into a single overall solution can help you centralize operations, ensure consistency across your organization, and improve administrative efficiency. Red Hat Identity Management natively integrates with Microsoft Active Directory so you can manage identities across mixed environments while applying tailored access control policies directly to your Red Hat Enterprise Linux domain.

Policy management

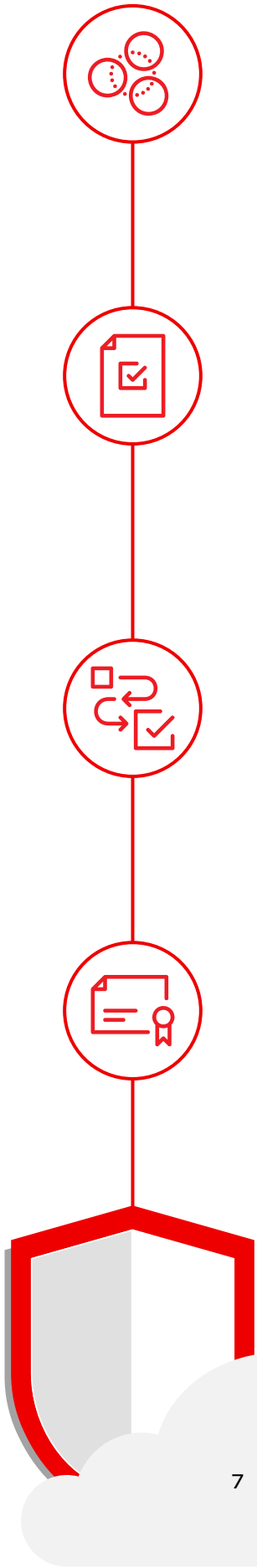
A policy-based approach to identity management can help you improve consistency, efficiency, and security. Red Hat Identity Management lets you set and apply policy-based controls from a centralized interface to ensure that identities, access, and resources are configured properly. Customizable identity and access policies help limit privilege escalations across your environment. And role-based access controls (RBAC) let you delegate identity management server administrative capabilities—including authentication and authorization management and session recording, auditing, and logging—across your team.

Multifactor authentication

Multifactor authentication (MFA) adds an extra layer of security by requiring multiple checks to verify an identity before granting access. Red Hat Identity Management supports MFA via cryptographic devices like hardware tokens and smart cards. You can also select and configure multiple authentication types—including passwords, certificates, Remote Authentication Dial-In User Service (RADIUS), one-time passwords (OTP), and Public Key Cryptography for initial authentication (PKINIT)—and set default authentication methods for all users.

Certificate management

Digital certificates contain information needed to authenticate the identity of users, applications, websites, and other subjects. They should be created, monitored, renewed, and retired according to least privileges principles. Red Hat Identity Management supports complete life cycle management for user, host, and service certificates. You can also deploy Red Hat Certificate System, a certificate authority that supports advanced management activity like smart card provisioning, customized certificate types, and protected secret storage. Support for common protocols and standards—including X.509, Automatic Certificate Management Environment (ACME), Simple Certificate Enrollment Protocol (SCEP) and Secure Sockets Layer (SSL), and TLS – lets you create certificates that work with your IT ecosystem. Automatic tracking of certificate expiration dates ensures timely renewals. And public key infrastructure (PKI) authentication verifies that identities can be trusted.



Get started with zero trust

Adopting a zero trust architecture can help you protect your IT and business assets in a fast-changing world.

Red Hat provides a reliable, integrated, and security-focused foundation for zero trust architectures. In fact, you may already use many of the components needed to implement a zero trust model. Red Hat Enterprise Linux offers security technologies, controls, certifications, and support for designing, building, and managing zero trust architectures. And with Red Hat Identity Management, you can centralize identity management, enforce security controls, and comply with security standards across your entire environment.

Try it out today with our **no-cost, web-based interactive labs**.

568051_0124_KVM

Red Hat