Red Hat
Enterprise Linux

Build a foundation for zero trust in Linux environments

A zero trust architecture can help you better protect your IT environment and organization.

Red Hat uses several key principles to guide zero trust architecture implementation:

- Never trust actors implicitly, always verify.
- Employ a least privilege access strategy.
- Assume networks and network traffic are compromised by default.

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

Modern IT environments demand new approaches to security

Traditional perimeter-based security approaches cannot effectively protect new, widely distributed, cloud-based environments. And security threats and the impact of breaches continue to grow. Bad actors exploit vulnerabilities that often exist due to outdated security paradigms like single-factor authentication, implicit trust, perimeter-based architectures, and inadequate user and event behavior tracking.

Implementing a zero trust architecture can help you protect your IT environment and organization. This overview discusses considerations for establishing zero trust architectures in Linux® environments.

What is zero trust and how does it work?

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. In order for one resource to connect to another resource, the session must be both authenticated and authorized to establish explicit trust.

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. An understanding of the subject's identity and attributes are critical for this evaluation. 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 one or more identity management, directory server, and credential management systems to administer this information. You should also continually reassess these access decisions to ensure that they remain valid over time.

Considerations for implementing a zero trust architecture

While adopting a zero trust security approach typically involves changes to your security and IT mindsets and processes, there are a number of technological capabilities that are needed as well. The following sections discuss key operating system and identity management solution capabilities and features to look for when adopting a zero trust architecture.

Operating system capabilities and features

Your operating system serves as the foundation for your IT environment and zero trust architecture.

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 two things:

- **Authentication**, verification, and validation of the identity of the subject.
- **Authorization**, verification, and validation of the right to and need to access an asset.

Trusted operating system supply chain

Zero trust models require that your operating system be as secure as possible and able to deny all access by default. Choose a security-focused operating system that is delivered through a trusted software supply chain to reduce your risk. Consider operating system vendors that offer:

- Static code analysis of the entire operating system to identify errors in programming style, memory reference methods, and input stream validation and ensure compliance with coding best practices.
- Compiler flags to run applications and assign memory segments in a non-predictive way to prevent stack smashing, mitigate memory corruption, and provide control flow integrity hardware support.
- Extensive quality engineering (QE) testing to minimize security flaws before shipping.
- Vulnerability patching processes that regularly deliver remediation against known vulnerabilities.

Mandatory access control

Your operating system must also be able to isolate and control access to resources on an individual basis. Mandatory access control (MAC) technologies like Security-Enhanced Linux (SELinux) do just this according to centrally managed security policies. Look for these operating system capabilities:

- Built-in MAC with granular, customizable control over files, processes, users, and applications to minimize the risk of inappropriate privilege escalations
- Ability to deny all access by default to align with zero trust principles

Modern, scalable, policy-based encryption

Data and network traffic encryption increases protection for your IT environment and organization. Several industry standards—including Federal Information Processing Standard (FIPS) 140—require system-wide encryption settings. Policy-based encryption lets you apply consistent configurations across your systems to help meet compliance requirements. Choose an operating system that includes:

- Policy-based cryptography controls that let you apply settings consistently across your systems.
- Default profiles for common security standards like FIPS 140.
- Automated policy application and enforcement to streamline management, reduce errors, and only decrypt files and software volumes if specifically allowed by policy.
- Customizable policies and settings to meet your organization's needs.

Application allowlisting

Application allowlisting is the practice of specifying an index of approved applications or executable files that are permitted to run on a system by a specific user. This practice is complementary to mandatory access controls, which can control application behavior but do not know which applications are trusted.

Select an operating system that provides built-in application allowlisting capabilities like File Access Policy Daemon (fapolicyd) to detect and prevent unauthorized applications from running on systems or networks, as well as predefined and customizable allowlist policies.

Hardware-based root of trust

Hardware-based root of trust capabilities help you verify system integrity and ensure that your systems have not been modified or tampered with. Opt for an operating system that lets you 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).

Compliance scanning

Noncompliance with corporate and industry standards and regulations can be costly and risky for your organization. System scanning tools like Open Security Content Automation Protocol (OpenSCAP) can ease audits and help you remediate noncompliant systems. Look for an operating system that provides:

- Built-in scanning tools with predefined and customizable compliance profiles.
- Reporting and baseline-generation capabilities to ease auditing and show drift.
- Automated remediation of noncompliant systems.
- Automation and integration with other tools for management at scale.

Transaction monitoring and logging

Monitoring and logging let you audit user actions to determine if a malicious action has occurred. Session recording and log aggregation tools can help you gain insight into actions across your environment. Choose an operating system that offers:

- Logging of input, output, system state, and environment variables to provide contextual insight.
- Off-system log storage to prevent tampering.
- Customizable recording settings for simpler auditing.

Key security standards

- FIPS 140
- Common Criteria (CC)
- Secure Technical Implementation Guidelines (STIG)

Independent attestation and security certification

Third-party verification of your operating system's compliance with security standards lets you operate with more confidence. Select an operating system that offers compliance with common standards.

Identity management solution capabilities and features

Your identity management solution encompasses identities, their attributes, credentials, certificates, and other items needed to authorize and authenticate access to assets.

Identity store

A domain controller allows you to manage identities, access, and policies for users, services, and hosts. Using a centralized identity store and domain controller can help reduce administrative overhead, simplify security management, and ensure consistency across your environment. Consider a solution that provides centralized identity management capabilities to streamline operations and promote consistency. Your solution should also support the infrastructure footprints and platforms you use now and intend to use in the future.

Key authentication types

- Normal, one-time, and hardened passwords
- Remote Authentication Dial-In User Service (RADIUS)
- Public Key Cryptography for Initial Authentication (PKINIT)

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 and ensure consistency across your organization. Opt for an identity management solution that works with popular tools like Microsoft Active Directory to manage identities across mixed environments.

Policy management

A policy-based approach to identity management can help you improve consistency, efficiency, and security. Identity management solutions that allow you to set and apply policy-based controls from a centralized interface can help ensure that identities, access, and resources are configured properly. Look for these features and capabilities:

- Role-based access control (RBAC) and policy-based access control capabilities
- Customizable identity and access policies
- Authentication and authorization management capabilities
- Session recording, auditing, and logging capabilities

Multifactor authentication

Multifactor authentication (MFA) adds an extra layer of security by requiring multiple checks to verify an identity prior to granting access. Choose identity management solutions that offer configurable authentication types and support for MFA via hardware tokens and smartcards.

Common certificate protocols and standards

- X.509
- Automated Certificate Management Environment (ACME)
- Simple Certificate Enrollment Protocol (SCEP)
- Secure sockets layer (SSL)
- Transport layer security (TLS)

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. Select an identity management solution that provides:

- Complete life cycle management for user, host, and service certificates.
- Support for common protocols and standards.
- Automatic tracking of certificate expiration dates to ensure timely renewals.
- Support for public key infrastructure (PKI) authentication.

Single sign-on

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. Users can authenticate once and access multiple services. Select an identity management solution that supports web authentication as well as the services you use now and plan to use in the future.

Build a foundation for zero trust with Red Hat Enterprise Linux

Red Hat provides foundational technology that you can use to design, build, and manage zero trust architectures. Red Hat® Enterprise Linux provides the security technologies, controls, certifications, and support needed to adopt zero trust models. It meets all of the operating system requirements discussed in this overview with delivery via a trusted supply chain, SELinux access controls, system-wide encryption policies, application allowlisting, hardware-based root of trust, session recording capabilities, and system roles. It also includes a built-in OpenSCAP scanner and the Red Hat Insights predictive analytics and remediation service. Finally, Red Hat Enterprise Linux is certified to many government security standards like CC, FIPS 140, STIG, and Section 508.

Included with Red Hat Enterprise Linux, Red Hat Identity Management can help you centralize identity management, enforce security controls, and comply with security standards across your entire environment. It delivers the capabilities needed to implement zero trust best practices while simplifying your identity management infrastructure. It integrates with Microsoft Active Directory, lightweight directory access protocol (LDAP), and other third-party solutions through standard interfaces. Red Hat Identity Management also supports certificate-based authentication and authorization techniques.

Red Hat Enterprise Linux and Red Hat Identity Management integrate with the rest of the Red Hat portfolio to provide a unified foundation for zero trust architectures.

- Red Hat Single Sign-On provides web single sign-on capabilities based on popular standards.
- Red Hat Satellite is an infrastructure management product that helps you keep your Red Hat Enterprise Linux environments running efficiently, with security, and in compliance.
- Red Hat Ansible® Automation Platform provides an enterprise framework for building, operating, and managing IT automation at scale.
- Red Hat Certificate System is a certificate authority that supports advanced management activity like smart card provisioning, customized certificate types, and protected secret storage.
- Red Hat Directory Server is an operating system-independent, network-based, scalable registry that lets you centrally store identity and application information for distributed directory topologies.

Next steps

- Learn more about Red Hat Enterprise Linux security.
- Read about Red Hat's approach to hybrid cloud security.

Deploy faster with expert services

Red Hat offers services to help you adopt a zero trust architecture based on Red Hat platforms and products.

- Red Hat Open Innovation Labs is an immersive residency that pairs engineers with open source experts to help you achieve real business outcomes.
- Red Hat Services: Zero Trust Adoption Journey is a consulting engagement that helps you assess your current situation and create a plan for building a zero trust architecture.

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 develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com

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

redhat.com