Build a foundation of security with Zero Trust and automation

How to operate in a Zero Trust reality

Table of contents

Introduction

Your organization doesn't shut down after 5 p.m. Neither do the cyber criminals and other bad actors searching for opportunities to steal data or wreak other havoc that can jeopardize your company, partners, and customers.

Today, organizations face a perfect storm of cybersecurity threats that keep IT, security, and operations teams on high alert. These threats affect organizations of all sizes and can cost billions. According to an IBM report, the average cost for a data breach from a cyberattack was US$4.24 million in 2021, up from US$3.86 million in 2020.[1]

These threats aren't restricted to external attackers either. The 2021 Data Breach Investigations Report from Verizon stated that 30% of breaches involved employees accessing systems outside their defined roles and permissions.[2]

The increase in the number and severity of attacks is driven by multiple factors, including rapid changes in network infrastructure, migrations from on-premise to cloud-based solutions, and the rise of remote work and work-from-home models since 2020.

The change to where employees work remotely has expanded attack surfaces, with both company-owned and employee-owned devices accessing sensitive systems over personal and public internet connections. There has also been an increase in the number and sophistication of phishing and spear-phishing attacks as employees work with colleagues they have never met.

The move to cloud-based solutions introduces numerous benefits for organizations—from cost savings to a significant reduction in physical document storage. But those benefits come with the ubiquitous cost of managing user, application, and infrastructure security for hundreds to thousands of users across legacy on-premise and cloud-based systems.

The combination of remote work and the move to the cloud have rendered the traditional VPN walled garden approach to security obsolete. In addition to employees connecting from more devices to more systems, the introduction of IoT and edge computing have exposed new potential attack vectors to cyber attackers.

Beyond the ways employees access systems, organizations have also scaled teams to manage disparate network and security systems. InfoSec, SysOps, NetOps, and other teams often work concurrently—and often independently from each other—to enforce security policies and respond to threats. Still, these teams often work separately, use different systems, and do not share common processes that affect their ability to coordinate a response. When it comes to security threats, every second counts in the response.

[1] "Cost of a data breach report 2021", IBM, accessed 16 June 2022.
[2] "2022 Data Breach Investigations Report", Verizon, accessed 16 June 2022.

Want to find out more about Zero Trust? Keep reading.

Already know about Zero Trust, but want to learn more about how to automate it? Skip ahead to Scaling Zero Trust with automation.

Another challenge driving cyberattack risks is that there is a lack of integration between the solutions powering and protecting organizational infrastructure. This creates additional roadblocks to efficient response to security incidents if the teams managing these solutions aren't able to communicate efficiently.

These cyberattack risks have attracted attention beyond security leaders. Organizations and vendors have adapted to support regulations including the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR). In 2021, the United States government recognized these threat increases with the introduction of the Executive Order on Improving the Nation's Cybersecurity.

Addressing these threats requires organizations to have a security-first mindset across their policies, networks, and applications. Many organizations are looking to Zero Trust architecture as a way forward, including the U.S. federal government with its mandate to advance towards implementing Zero Trust architecture across their networks.

But implementing Zero Trust is only the beginning—especially in large organizations with multiple sites and a mix of on-premise, cloud, and edge systems. Scaling Zero Trust architecture requires enterprise-level automation. In this e-book you'll learn how Red Hat® Ansible® Automation Platform is the right solution for your organization.

Zero Trust to the rescue?

Traditional security models were built around systems that employees would access from inside a physical location. As remote access options evolved from dial-up to always-on high-speed connections, external access was regulated with virtual private networks (VPNs). While VPNs provide secure authentication to a network, they also expose more resources and systems to users than they would need to access—creating potential security risks.

But today, VPNs and standard user-based permissions can no longer provide the level of security needed for the complicated on-premise, hybrid, and cloud-based solution architecture that organizations depend on to do business. A new model was needed, one that makes a foundational change to how we approach security. This shift in how security is approached is Zero Trust architecture.

Recognized as a security pattern in 2010, Zero Trust starts by assuming that there are attackers inside and outside of the network. Working off this assumption, Zero Trust defaults to starting every interaction in an untrusted state.

Instead of relying solely on location and role or user-based permissions, the Zero Trust framework requires that the user, device, and application are verified to create a trusted state for the interaction. Implementing Zero Trust encourages an entirely new security mindset by instructing system architects to authenticate a user or devices with each transaction, and only authorize access to data and systems based on the concept of least privilege.

Authenticating every transaction

The foundation of Zero Trust architecture is treating every interaction as a potential threat—inside and outside of the network. Before the interaction can proceed, its components need to be authenticated. Each Zero Trust architecture implementation will have its own unique required components, with the core set being:

- **User.** Authenticate that the user trying to access a network, application, or cloud-based system has the correct permissions.
- **Application.** Verify that the user has the correct permissions for the data or application they are trying to access.
- **Device.** Confirm the user is connecting to the resource using a device authorized to access the network and application.
- **Posture.** Check the device used to confirm it has the necessary updates, patches, and encryption to access the network and application securely.

The shift to Zero Trust is also happening in the public sector—most notably within the U.S. Federal Government. The 2021 Executive Order on Improving the Nation's Cybersecurity includes multiple mandates, from moving to secure cloud-based solutions to advancing towards Zero Trust architecture for all government infrastructure.

Organizations that sell to or support federal agencies must ensure they meet Zero Trust standards as those agencies upgrade their security and infrastructure.

Challenges with implementing Zero Trust

With growing threats and attack vectors, implementing Zero Trust across your organization is an imperative. But even with its numerous advantages over traditional security, there are challenges with implementing Zero Trust in existing infrastructure.

First, existing infrastructure can consist of multiple solutions from different vendors. While most vendors have made strides to adopt Zero Trust architecture principles, not every system offers interoperability with systems from other vendors. Internal teams—from SysOps to NetOps—could experience issues where solutions aren't operating in concert with each other. Or worse, disconnected teams and systems can cause breaks in threat detection when there are interoperability issues.

Second, Zero Trust requires a significant shift in how leaders think about and treat security. Moving from a castle and moat to a deny-by-default mindset means leaders have to commit their organization to upholding Zero Trust principles and practices, even when they appear to be getting in the way. Without this commitment, teams can often revert to legacy practices or even create separate "shadow IT" offerings that circumvent Zero Trust architecture, policies, and processes.

How to build a strong security foundation with Zero Trust architecture

Traditional security approaches like VPNs with physical or digital tokens were created to provide a secure remote path to an on-premise network. Often referred to as the castle-and-moat network security model, the focus was solely on one entry point which opened the door to all resources on the other side.

In physical security, the analogy would be keycard access to buildings or secure areas within buildings. An organization may feel like they have physical security using role-based security for employees to enter the building or move around to various areas. But that physical security can fail if a bad actor employs a social engineering hack such as pretending to be a delivery person and being waved through by building security personnel.

Zero Trust is the core, not an add-on

Zero Trust principals start with making security a foundational component of all projects, whether developing new products or implementing new infrastructure. Instead of building security around network access, Zero Trust architecture is applied to every interaction as a practice across the organization.

Where to start with Zero Trust

Implementing Zero Trust doesn't start with selecting vendors or migrating security platforms. Instead, organizations need to ask a simple question that has significant implications for their Zero Trust strategies—what data, applications, or systems are they trying to protect?

- **Build an inventory.** Understanding what is being protected gives organizations a baseline for creating the network, user, application, and workload rules and policies of their Zero Trust implementation. This baseline also provides SysOps, NetOps, and InfoSec teams with what analytics and analysis tools are needed to discover, identify, and react to security incidents.
- **Develop your processes and policies.** Once an organization has a clear view of what they are protecting, internal teams can work together to create Zero Trust processes and policies that enable employees to securely get their work.
- **Test. Modify. Deploy.** Ideas on paper can often work out differently when implemented. Seeing processes and policies in the real-world provides operations, networking, and security teams with the necessary feedback to make Zero Trust work for the entire organization.

Starting by understanding what is being protected is the foundation for scaling Zero Trust through automation.

Scaling Zero Trust with automation

Learn more about Ansible security automation, and uncover where you are in your security automation journey in this webinar.

Zero Trust architecture demands that assets including devices, data, and applications are protected the same way wherever they exist. For example, if a workload is moved from an on-premise datacenter to a private or public cloud, Zero Trust architecture requires the same security management rules to be applied. With Zero Trust architecture, the decisions are abstracted from the workload itself so the actual code doesn't change.

Across large organizations or rapidly growing businesses, leveraging automation can help scale their policies, rules, and processes as new tools or infrastructure are introduced. Before we look at how Red Hat® Ansible® Automation Platform delivers automation for the Zero Trust architecture, here are five advantages of automating Zero Trust:

Automation advantages

- **Know what you're protecting.** Understanding what is being protected is the key to scaling Zero Trust across an organization's devices, network, and applications. Automation helps organizations to track and log these assets across multiple locations and in the cloud.
- **Always-on compliance.** The use of bots and other automation tools by cyber criminals creates a need for a security system that is always looking out for threats. Automating Zero Trust ensures that policies are enforced 24 hours a day, 365 days a year.
- **Reduced risk.** InfoSec teams can adopt policies and rules as security incidents occur. These processes can then be codified as workflows and executed using automation, reducing the risk of an admin making a human error when implementing a change.
- **Improved responsiveness.** The longer a security risk is not responded to, the more potential for a breach or cyberattack. Automating Zero Trust empowers organizations to respond quickly, whether there are 1,000 users or 100,000 users, by creating automated actions that can be executed on-demand or by event-driven automation.
- **Fast prototyping.** Automation allows organizations to prototype, test, and implement changes to the security framework, regardless of how complex the framework is.

Zero Trust Automation goes beyond security

Extending Zero Trust beyond networking and security allows organizations to truly make security the foundation of every project and system. Automating these processes pushes the value of Zero Trust even further by ensuring policies and processes are applied and inspected to reduce the risk of cyberattacks or other breaches.

Consistent security and compliance

Automation can help enforce security and compliance rules by managing configurations, applications deployment, and compliance checks that feed into development processes. Organizations can automate provisioning, configuration, application deployment, and other areas.

Automation does more than secure applications and components. It can also be used to maintain those components and provide regular compliance checks and verification. It's end-to-end continuous enforcement of security posture for an organization's continuous integration and continuous development (CI/CD) life cycle.

Holistic software security

Zero Trust principles can also be applied to software and systems inside an organization. Teams and departments often require different applications, hardware, and solutions that don't have out-of-the-box interoperability. Automation can help integrate multiple systems from different vendors by enabling the creation of automation workflows to orchestrate efficient and secure interoperability.

Even more critical, internally and externally developed solutions may include open source components, that if not monitored for vulnerabilities, could create a new attack vector for cybercriminals. The same automations created to manage interoperability can be employed to keep applications in the correct secure state.

Compliance automation

Automation can be used to reduce human error in compliance-related tasks. One example is an organization that processes credit card transactions. Multiple processes and hardware and software reviews need to occur to audit Payment Card Industry Data Security Standard (PCI DSS) compliance. These audits also require timely and accurate data from these multiple systems. Automation can be employed instead of having an employee or team monitoring these processes to reduce human error and free up employee time for other more strategic projects.

Automating Zero Trust and more with Red Hat Ansible Automation Platform

Learn more about how automation can help you in Red Hat Ansible Automation Platform: A beginner's guide

Zero Trust works when organizations have clear visibility wherever a transaction occurs. Red Hat Ansible Automation Platform brings Zero Trust and other automation capabilities to your organization. The platform provides a quick return on investment (ROI) by lowering barriers to automation across security, networking, application, cloud, and edge computing.

Zero Trust	**Automating Zero Trust with Red Hat Ansible Automation Platform**
Zero Trust uses a deny-by-default approach.	Red Hat Ansible Automation Platform allows administrators to enforce access controls to assign permissions, privileges, and roles to users. It also automates encryption—including Mutual Transport Layer Security (mTLS), audit trails, and inventory controls.
Zero Trust uses authorization policies to restrict access to applications or resources.	Red Hat Insights for Ansible Automation Platform can help organizations monitor and identify failures or potential risks where SysOps or NetOps team intervention could be required.
Zero Trust ensures resources are patched before being accessed.	Red Hat Ansible Automation Platform ensures that security patches and updates are applied to application resources across an organization's infrastructure.

Red Hat Ansible Automation Platform is the connective tissue that brings together disparate technologies that otherwise don't communicate well with one another. There are over 100 Red Hat Certified Content Collections—supported by Red Hat and our partners—available to provide consistent automation across all infrastructure components, whether they're hybrid, cloud, or on-premise.

Ready to start your Zero Trust automation journey?

Red Hat Consulting can help you on your automation journey to adopt Zero Trust. Take a short self assessment, or reach out to the Red Hat Consulting team today.

Learn more about IT automation and start a trial today.

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.

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

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