Red Hat
OpenShift

Zero Trust Networking

Multi-Team OpenShift-Focused Deliverable

Marc Curry
Consulting Product Manager, OpenShift
Cloud Platform BU

2023-09-06

Zero Trust Networking

Zero Trust

Assume that everything is independently and always exposed to all potential threats.

OpenShift Zero Trust Networking Deliverable

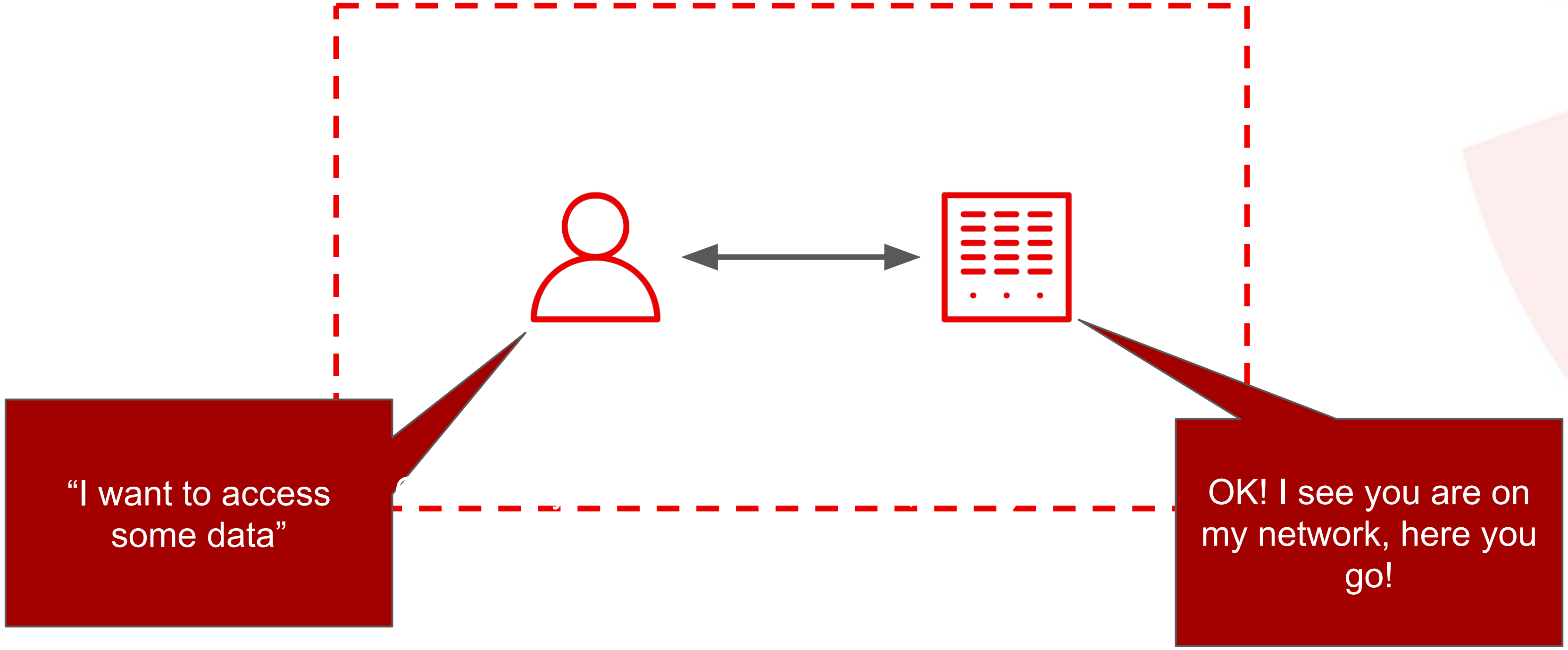
In line with White House Executive Order 14028:

“Improving the Nation's Cybersecurity”,

OpenShift will be focusing and improving its already-existing Zero Trust architecture to make Zero Trust Networking easier to understand and deploy, starting in Q4CY2023.

Implicit Trust Today

Users and applications are trusted because they are all inside the same boundary

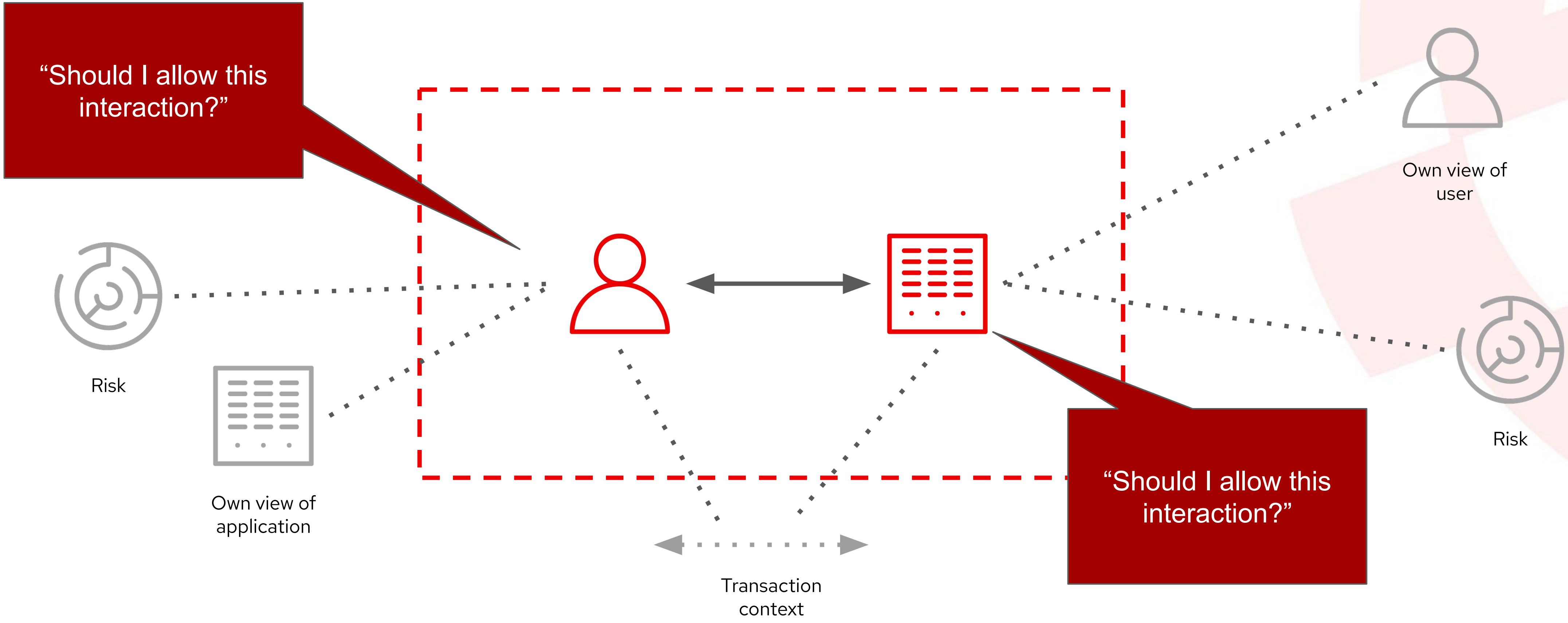


“I want to access some data”

OK! I see you are on my network, here you go!

Explicit Trust Is the Goal

Trust is no longer implicit -- but derived from the specifics of each transaction



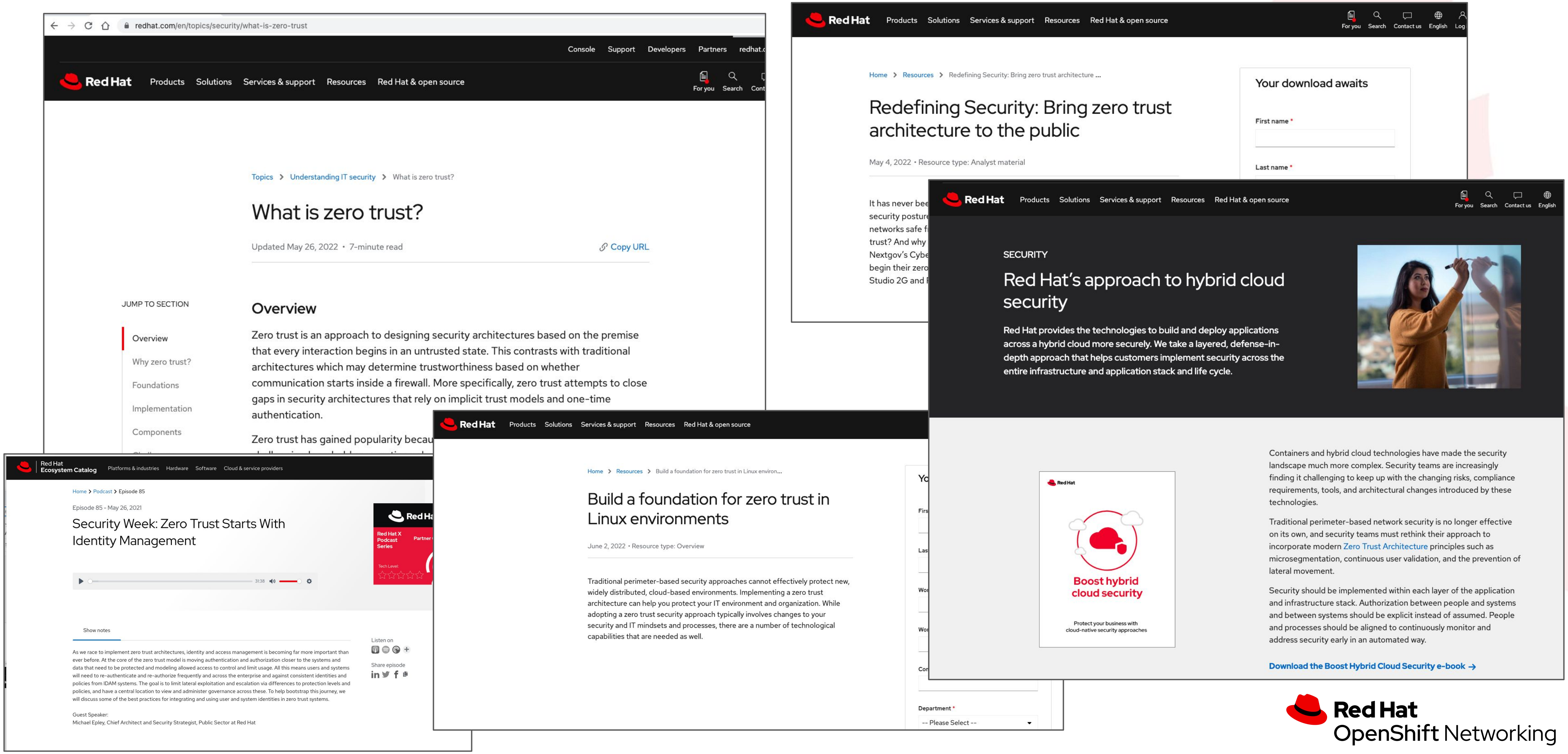
“Should I allow this interaction?”

“Should I allow this interaction?”

Zero Trust at Red Hat

Zero Trust Momentum at Red Hat

Zero Trust SIG



redhat.com/en/topics/security/what-is-zero-trust

Topics > Understanding IT security > What is zero trust?

What is zero trust?

Updated May 26, 2022 • 7-minute read

Copy URL

JUMP TO SECTION

- Overview
- Why zero trust?
- Foundations
- Implementation
- Components

Overview

Zero trust is an approach to designing security architectures based on the premise that every interaction begins in an untrusted state. This contrasts with traditional architectures which may determine trustworthiness based on whether communication starts inside a firewall. More specifically, zero trust attempts to close gaps in security architectures that rely on implicit trust models and one-time authentication.

Zero trust has gained popularity becau

Home > Resources > Redefining Security: Bring zero trust architecture ...

Redefining Security: Bring zero trust architecture to the public

May 4, 2022 • Resource type: Analyst material

It has never bee
security posture
networks safe f
trust? And why
Nextgov's Cybe
begin their zero
Studio 2G and

Your download awaits

First name *

Last name *

SECURITY

Red Hat's approach to hybrid cloud security

Red Hat provides the technologies to build and deploy applications across a hybrid cloud more securely. We take a layered, defense-in-depth approach that helps customers implement security across the entire infrastructure and application stack and life cycle.

Red Hat
Boost hybrid cloud security
Protect your business with cloud-native security approaches

Containers and hybrid cloud technologies have made the security landscape much more complex. Security teams are increasingly finding it challenging to keep up with the changing risks, compliance requirements, tools, and architectural changes introduced by these technologies.

Traditional perimeter-based network security is no longer effective on its own, and security teams must rethink their approach to incorporate modern Zero Trust Architecture principles such as microsegmentation, continuous user validation, and the prevention of lateral movement.

Security should be implemented within each layer of the application and infrastructure stack. Authorization between people and systems and between systems should be explicit instead of assumed. People and processes should be aligned to continuously monitor and address security early in an automated way.

Download the Boost Hybrid Cloud Security e-book →

Home > Podcast > Episode 85

Episode 85 - May 26, 2021

Security Week: Zero Trust Starts With Identity Management

Show notes

As we race to implement zero trust architectures, identity and access management is becoming far more important than ever before. At the core of the zero trust model is moving authentication and authorization closer to the systems and data that need to be protected and modeling allowed access to control and limit usage. All this means users and systems will need to re-authenticate and re-authorize frequently and across the enterprise and against consistent identities and policies from IDAM systems. The goal is to limit lateral exploitation and escalation via differences to protection levels and policies, and have a central location to view and administer governance across these. To help bootstrap this journey, we will discuss some of the best practices for integrating and using user and system identities in zero trust systems.

Guest Speaker:
Michael Epley, Chief Architect and Security Strategist, Public Sector at Red Hat

Home > Resources > Build a foundation for zero trust in Linux environ...

Build a foundation for zero trust in Linux environments

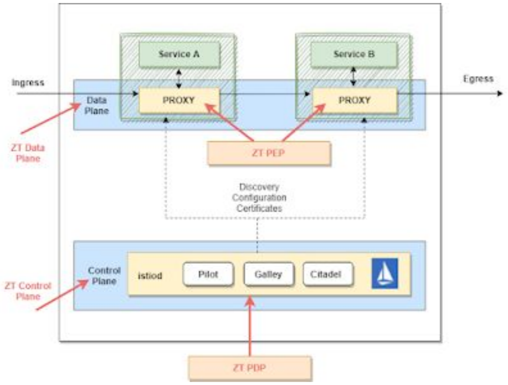
June 2, 2022 • Resource type: Overview

Traditional perimeter-based security approaches cannot effectively protect new, widely distributed, cloud-based environments. Implementing a zero trust architecture can help you protect your IT environment and organization. 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.

Department *

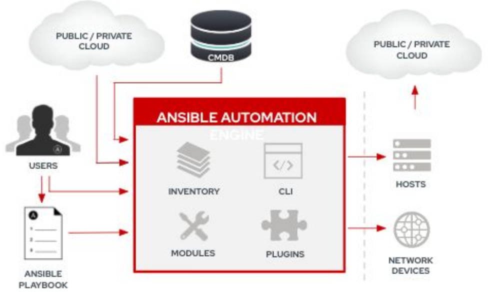
-- Please Select --

ZT is Already Supported by Red Hat’s Portfolio



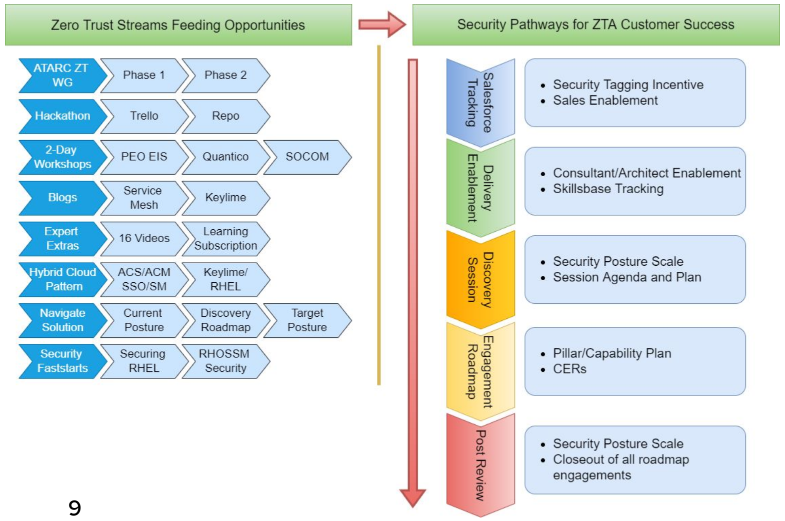
OpenShift

Ansible



Zero Trust

ZT maturity via **services engagements**



Zero Trust Streams Feeding Opportunities

- ATARC ZT WG → Phase 1 → Phase 2
- Hackathon → Trello → Repo
- 2-Day Workshops → PEO EIS → Quantico → SOCOM
- Blogs → Service Mesh → Keylime
- Expert Extras → 16 Videos → Learning Subscription
- Hybrid Cloud Pattern → ACS/ACM SSO/SM → Keylime/ RHEL
- Navigate Solution → Current Posture → Discovery Roadmap → Target Posture
- Security Faststarts → Securing RHEL → RHOSSM Security

Security Pathways for ZTA Customer Success

Salesforce Tracking
- Security Tagging Incentive
- Sales Enablement

Delivery Enablement
- Consultant/Architect Enablement
- Skillsbase Tracking

Discovery Session
- Security Posture Scale
- Session Agenda and Plan

Engagement Roadmap
- Pillar/Capability Plan
- CERs

Post Review
- Security Posture Scale
- Closeout of all roadmap engagements

Security Ecosystem

cilium paloalto NETWORKS f5

TIGERA dynatrace Infoblox NEXT LEVEL NETWORKING zscaler

anchore CYBERARK splunk> illumio

THALES Zettaset SYNOPSYS VIRSEC

NETFOUNDRY sysdig aqua AKEYLESS

solo.io snyk sonatype

Identity Platforms

(IDM, DS/CS, SSO)

ADFS Ping Identity SailPoint

Azure Active Directory okta

Red Hat Directory Server

Red Hat Single Sign On

Red Hat Certificate System

Source: Red Hat’s Zero Trust Adoption Journey

Zero Trust Networking Development Focus

What is the status of ZTN for OpenShift Today?

- Today, Zero Trust Networking is largely IPsec and Network Policy
- No single product technology solves the ZTN space, though some have greater existing contributions than others (e.g. Service Mesh)
- ACS and ACM will have major contributions to ZTN

High-Level Initial Engineering Focus

- Short-term: use what we've got already (target EOY2023)
- We can't *require* every solution option or existing product solution, but we should optionally provide them
- For existing solutions today, it may be a matter of documentation
- Identify our gaps and provide solutions
- Gap solutions may include partnering with 3rd-party providers

Targeted Capabilities

- **Observability for Constant, and Retrospective, Evaluation**
  - The ability to observe and verify all of the things that make up ZTN. This important for intrusion detection, forensics, and is helpful for operational load management.
- **Risk Assessment**
  - The ability to examine policies to make it easier for people to understand and develop.
- **Identification and Authentication**
  - Establishing a trust relationship by verification of the identity of the other end of a connection. Management of certificate lifecycles to limit use if compromised.
- **Inter-Service Authorization**
  - The ability to control access to services based on request identity.
- **Traffic Authentication and Encryption (e.g. mTLS)**
  - The ability to ensure that traffic on-the-wire is encrypted and that the source is identifiable.
- **Endpoint Security**
  - Enabling trust of remote endpoint connections to, for example, ensure certified images are run on trusted hardware and policies controlling an endpoint can be established based on endpoint characteristics.
- **Session validation / Session validity expiration (current session only)**
  - The ability to issue short-lived tokens (perhaps even single-use) so that tokens from a compromised pod are useless elsewhere.
- **Transaction-Level Verification**
  - The ability to identify and authenticate individual transactions. This can include rate-limiting by source, observability, and semantic validation that a transaction is well-formed.
- **Sitewide Policy Enforcement and Distribution**
  - The ability to apply and govern site-wide policies. This should allow for delegation of some permissions to users and cluster administrators within defined bounds.

Array of Existing Cross-Product Capability Providers

- Network Observability Operator
- Kubernetes Network Policy
- Admin Network Policy
- Istio/Envoy (pod-to-pod)
- OpenShift Service Mesh / Kiali
- IPsec (N-S, E-W)
- cert-manager
- Red Hat Service Interconnect
- Advanced Cluster Security
- Advanced Cluster Manager
- Submariner

- Kuadrant
- Gateway API
- 3Scale (API Gateway)
- namespace/SELinux/cgroups
- OpenShift Distributed Tracing Platform
- Red Hat SSO
- KubeVirt / Kata Containers
- SPIFFE / Spire
- OpenShfit Service Certs
- Supply Chain / Trusted Computing
- Insights
- …

Zero Trust Networking Resources

Resources / Collateral

- Zero Trust SIG GDrive Repository
- Red Hat Zero Trust Strategy Executive Briefing
- What is Zero Trust and why it is the future of cybersecurity
- ATARC Zero Trust Demonstration
- Zero Trust Networking Working Group - WIP Technical Alignment Document
- ZTN Architecture Working Group Charter
- Project Compass Notes
- Red Hat OpenShift Networking - Strategy and Roadmap
- The Big Bang! Zero trust and supply chain security

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

in linkedin.com/company/red-hat

▶ youtube.com/user/RedHatVideos

f facebook.com/redhatinc

twitter.com/RedHat