RAPID7

SOLUTION BRIEF

ADOPTING THE ZERO TRUST SECURITY MODEL FOR CLOUD DEVELOPMENT

Enhancing Cloud Security with Rapid7's Continuous Verification and Monitoring Tools

Introduction to Zero Trust Architecture

As organizations increasingly migrate to the cloud, the limitations of traditional perimeter-based security models become more apparent. The Department of Defense's (DoD) Zero Trust Architecture (ZTA) offers a modern security approach that challenges the assumption that any user, device, or network is inherently trustworthy. Emphasizing the principle of "never trust, always verify," ZTA ensures that every access request—whether originating from inside or outside the network—is rigorously authenticated, authorized, and continuously monitored.

This approach is particularly vital in cloud environments, where the distributed and dynamic nature of infrastructures renders perimeter-based security ineffective. Rapid7's platform plays a key role in enabling organizations to embrace and implement the Zero Trust framework, providing solutions for identity and device management, network segmentation, and real-time threat detection.

Note: For the latest DOD guidance on ZTA, including new overlays and principles, refer to the updated document detailing these changes. See the DOD's "Zero Trust Architecture Overlays" available at https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf.

UNDERSTANDING ZTA IN CLOUD DEVELOPMENT

Zero Trust shifts the focus from a perimeter-based defense to continuous validation of access at every layer of your system. Here's a quick rundown of the core principles:

- **Identity:** Every user, service, and device needs to be authenticated before accessing resources.
- **Devices:** Only trusted devices should be allowed access to sensitive data or systems.
- **Networks:** Network access must be tightly controlled to limit lateral movement and reduce exposure.
- **Applications:** Applications need to be secure by design and monitored continuously during runtime.
- **Workloads:** Cloud workloads—like containers and microservices—must be protected with strict security policies.
- **Data:** Sensitive data must be encrypted and only accessible to authorized entities, throughout its lifecycle.

The goal of ZTA is to minimize the attack surface and prevent unauthorized access or lateral movement. For cloud environments, where traditional security models fall short, Zero Trust is essential to secure data and applications effectively.

Rapid7's platforms are built to help organizations implement Zero Trust across their cloud environments, ensuring that every access request is verified and that your resources are continuously monitored and protected.

HOW RAPID7 HELPS YOU ALIGN WITH ZTA

Identity & Access Management (IAM) with Continuous Authentication

Zero Trust mandates strict identity verification, and Rapid7 enables this with robust IAM features. Every access request—whether from a user, service, or device—undergoes continuous verification.

- **Continuous Authentication:** Rapid7 supports multi-factor authentication (MFA) and behavioral analytics to verify users. By analyzing access patterns, the platform flags suspicious activity indicating compromised credentials or malicious intent.

- **Least-Privilege Access:** Role-based access control (RBAC) ensures minimal permissions for users, services, and devices, reducing the attack surface.

With continuous identity verification and least-privilege access, Rapid7 enforces strict access controls in alignment with Zero Trust principles.

Device & Network Security with Continuous Monitoring & Segmentation

Zero Trust requires ongoing monitoring of devices and networks. Rapid7 provides real-time device monitoring and dynamic network segmentation to secure cloud resources.

- **Device Security:** Devices are monitored for compliance, ensuring they meet security standards before accessing cloud resources.

- **Network Segmentation:** Dynamic segmentation limits access based on factors like user role and device health, preventing lateral movement if a breach occurs.

By enforcing device compliance and network segmentation, Rapid7 ensures only trusted devices and users access cloud resources, reducing attack exposure.

Application & Workload Protection with Real-Time Monitoring

Applications and workloads are prime targets in cloud environments, requiring continuous monitoring for Zero Trust security. Rapid7 offers real-time protection for applications, containers, microservices, and cloud workloads.

- **Application Security:** Automated vulnerability scans and runtime protection monitor applications for vulnerabilities and abnormal behavior, with threat intelligence detecting emerging risks.

- **Workload Protection:** Continuous monitoring of containers and serverless functions blocks unauthorized access and prevents lateral movement.

By monitoring applications and workloads for abnormal behavior, Rapid7 ensures quick detection and resolution, upholding Zero Trust's continuous verification principles.

Rapid7 Mapping to DoD ZTA

Rapid7 Product	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
Nexpose & Insight VM Enterprise Vulnerability Management (On-Prem & Cloud)	✓	✓	✓				
InsightCloudSec Cloud Native Application Protection Platform for Hybrid Cloud & Private Cloud (On-Prem & Cloud)	✓	✓	✓	✓	✓	✓	✓
AppSpider & InsightAppSec Dynamic Application Protection Platform (On-Prem & Cloud)			✓			✓	
InsightIDR Extended Detection & Response Platform (Cloud)	✓	✓		✓			✓
InsightConnect Security Orchestration & Automation (On-Prem & Cloud)				✓		✓	
Threat Command External Threat Intelligence Platform, Digital Risk Protection (Cloud)							✓
Metasploit Pro #1 Penetration Tool in the World (On-Prem & Cloud)	✓						
Surface Command Attack Surface Management	✓			✓			✓

EXPECTED OUTCOMES OF IMPLEMENTING ZTA WITH RAPID7

- **Reduced Risk of Unauthorized Access**: Continuous identity verification, device monitoring, and strict access controls significantly reduce the risk of unauthorized access to cloud resources. Zero Trust's emphasis on least-privilege access ensures that only the right entities can access sensitive data and systems.
- **Enhanced Threat Detection and Response:** With real-time monitoring of devices, applications, and workloads, Rapid7 can detect threats as they arise. Detailed visibility into network traffic, user behavior, and application performance allows security teams to quickly identify and respond to anomalous activities, minimizing the impact of any potential breach.
- **Improved Compliance and Security Posture:** By enforcing Zero Trust principles like RBAC, device health, and data encryption, Rapid7 helps organizations meet security best practices and regulatory compliance requirements, all while maintaining a robust security posture.
- **Limited Lateral Movement and Reduced Exposure:** Dynamic network segmentation and workload protection ensure that even if an attacker gains a foothold in one part of your system, they can't easily move laterally. This containment strategy dramatically reduces your attack surface and the potential impact of security incidents.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

THE BOTTOM LINE

Adopting a Zero Trust approach is crucial for securing cloud environments, and Rapid7's platforms make it easier to implement. By continuously verifying identities, monitoring devices, securing applications, and protecting workloads, we help organizations follow the Zero Trust framework's core principles throughout their cloud infrastructure.

With Rapid7, organizations can minimize unauthorized access, enhance their threat detection and response capabilities, and improve their overall security posture—ensuring that cloud resources are tightly controlled, threats are quickly identified, and any security incidents are contained to mitigate damage.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight