

RUNTIME RODEO:
Where Open Source Image Behavior is Tamed

RAD SECURITY

AGENDA:

- Introduction to Software Security Supply Chain
- Current Focus in Cloud Native Security
- Understanding Runtime Behavioral Fingerprints
- Case Study: Solarwinds Attack
- Proposed Standard for Behavioral Fingerprints
- Application to Open Source Images
- Advantages of Behavioral Fingerprints
- Q&A Session
- Call to Action

RAD SECURITY

Introduction to Software Security Supply Chain

SBOMs (Software Bill of Materials)

Catalogs all components and dependencies in a software application, ensuring transparency and traceability.

SCA (Software Composition Analysis)

Identifies known vulnerabilities in open-source and third-party components, helping to mitigate risks early in development.

CVEs (Common Vulnerabilities and Exposures)

Standardized identifiers for publicly known cybersecurity vulnerabilities, enabling easier sharing of data across tools.

Image Signing

Cryptographically verifies the integrity and origin of container images, ensuring they haven't been tampered with.

RAD SECURITY

Current Focus in Cloud Native Security

Pre-Deployment Measures

- Software Bill of Materials (SBOMs) provide transparency of components used.
- Source Code Analysis (SCA) helps in identifying vulnerabilities early.
- Common Vulnerabilities and Exposures (CVEs) are tracked and mitigated.
- Image signing ensures the integrity of container images before deployment.

Introduction to Runtime Attestations

- Monitors the behavior of containers during execution.
- Captures deviations from expected behavior to detect tampering.
- Adds an additional layer of security beyond pre-deployment measures.
- Can prevent sophisticated attacks like Solar Winds by verifying runtime behavior.

RAD SECURITY

Integrating supply chain checks in the SDLC ensures software security and reliability.

The Software Development Life Cycle (SDLC) is a structured approach that controls the development of software applications from inception to deployment. By incorporating supply chain checks at various stages, organizations can identify vulnerabilities and prevent the introduction of malicious code. This proactive approach helps maintain the integrity and security of the software supply chain, leading to more reliable software products.

RAD SECURITY

Understanding Runtime Behavioral Fingerprints

- A runtime behavioral fingerprint is a cryptographically verified profile of an image's behavior during execution.
- It captures various runtime activities, such as system calls, network connections, and file access patterns.
- By monitoring and verifying these behaviors, anomalies that indicate tampering or malicious activities can be detected.
- This approach complements traditional pre-deployment security measures like SBOMs and image signing, offering a more comprehensive security solution.



RAD SECURITY

Case Study: Solarwinds Attack



The Solar Winds attack involved tampering with Orion software during the CI/CD process, inserting malicious code into updates.



Traditional measures like SBOMs, SCA, and CVEs were ineffective because the malicious code was added post-verification.



A runtime behavioral fingerprint could have detected abnormal activities, preventing the spread of tampered software.

RAD SECURITY

Proposed Standard for Behavioral Fingerprints



Key Criteria for Fingerprints

Behavioral fingerprints should include process activity, network connections, and file system changes. Each activity must be cryptographically hashed for integrity.



Decision Points

Determining what constitutes normal vs. anomalous behavior is crucial. Criteria must be clearly defined, and thresholds must be set for acceptable deviations.



Example Implementation

Using nginx, monitor and record typical request patterns, response sizes, and error rates. Any deviation from these patterns would trigger an alert.

RAD SECURITY

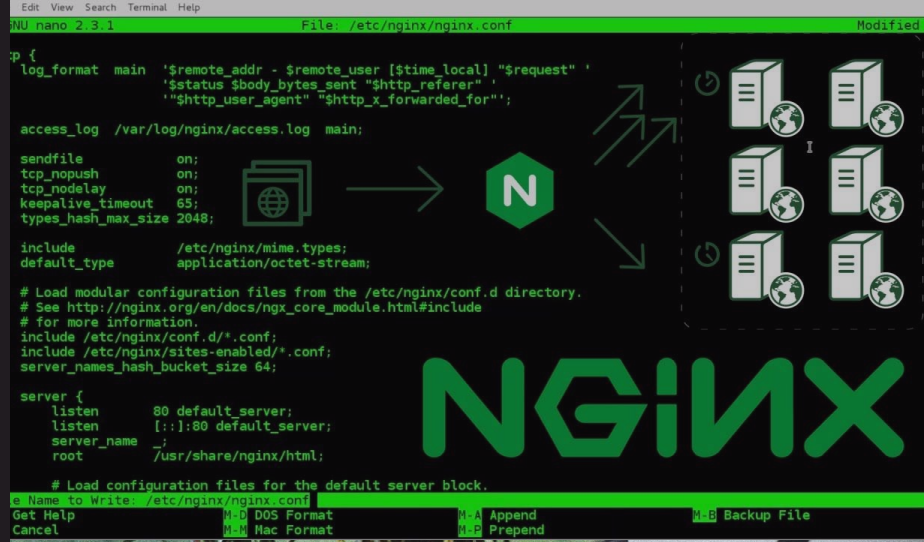
Application to Open Source Images

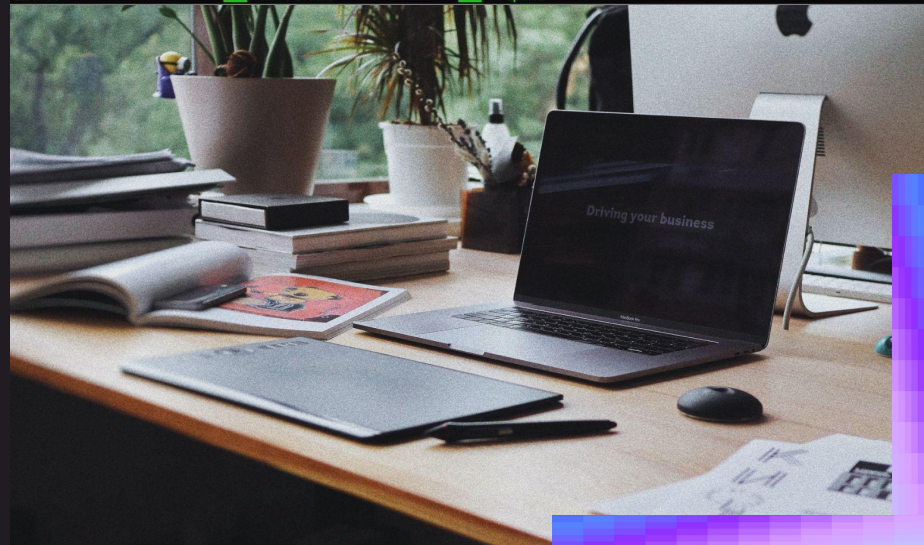
Nginx Behavioral Fingerprint

For Nginx, the fingerprint includes HTTP request patterns, module usage, and typical file paths accessed. Exclude static assets.

Apache Behavioral Fingerprint

For Apache, include log activity patterns, module interactions, and configuration file changes. Exclude non-runtime configurations.





RAD SECURITY

Advantages of Behavioral Fingerprints



Real-time Detection: Identify anomalous behavior instantly, enabling faster response to potential threats.

Enhanced Security: Significantly improve the security of the software supply chain by verifying runtime behaviors, not just static attributes.

Tamper Proof: Create cryptographically verified fingerprints that are resistant to tampering and unauthorized changes.

Comprehensive Coverage: Provide an additional layer of security that complements existing measures like SBOMs and image signing.

RAD SECURITY

The RAD Catalog revolutionizes runtime supply chain security.

The RAD (Runtime Analysis and Detection) Catalog is a collection of behavioral fingerprints & CI plugins designed to fortify runtime supply chain efforts. Leveraging advanced machine learning, it identifies & mitigates threats in real-time, ensuring a secure & resilient supply chain. This tool enhances security & streamlines monitoring of runtime environments, making it indispensable for modern enterprises.

RAD SECURITY

Take the leap to enhance your security with runtime behavioral fingerprints.

By adopting runtime behavioral fingerprints, you not only strengthen your software supply chain security but also proactively guard against sophisticated attacks like Solar Winds. This new standard can be seamlessly integrated into your existing security practices, providing a cryptographically verified layer of trust. Join the movement towards more resilient cloud native security today.

RAD SECURITY

Q&A SESSION

- What are the key differences between traditional pre-deployment security measures and runtime behavioral fingerprints?
- How would the implementation of runtime behavioral fingerprints have potentially prevented the Solar Winds attack?
- What are the challenges you foresee in adopting this new standard across different organizations?
- Can you provide more examples of open source images where behavioral fingerprints could be beneficial?
- How do you envision the future of software supply chain security evolving with the inclusion of runtime attestations?