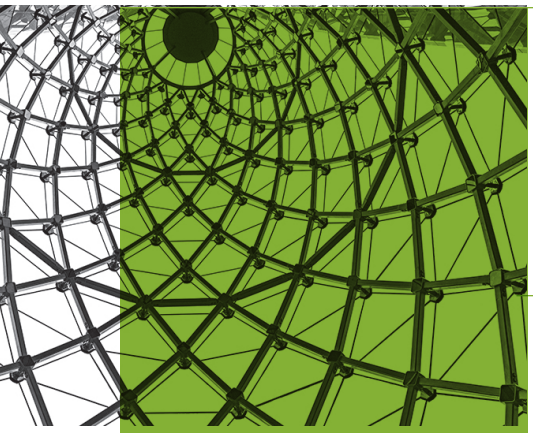

JUNIPER CLOUD WORKLOAD PROTECTION

Product Overview

Juniper Networks® Cloud Workload Protection automatically defends application workloads in any cloud or on-premises environment against attempts to exploit application vulnerabilities as they happen, including the OWASP Top 10 and memory-based attacks. It controls application execution and monitors the application's behavior and context, comparing what it's supposed to do against what's happening in real time. It protects the targeted vulnerability from being exploited automatically with run-time protection, without an administrator needing to intervene. Juniper Cloud Workload Protection ensures that production applications always have a safety net against vulnerability exploits, keeping business-critical services connected and protected.

Product Description

Application security is a core tenet of the Juniper Experience-First Networking philosophy. Nearly everything we do on the network involves applications, from Web browsing and chat to mobile games and business services that allow us to get work done. Applications store, process, and exchange data, enabling us to connect to each other and make our digital lives easier. When we use them, we need them to be accessible right away, and we trust that our application experience will be secure.

Sometimes when application code is written, it can contain errors that present opportunities for attackers. These errors can cause the underlying resources and processes (or workloads) that power the application, such as databases and registries, to be vulnerable. In spite of secure coding practices, organizations may not even be aware specific application vulnerabilities exist until it's too late. Organizations need a safety net that protects application workloads against exploits, including zero-day attacks.

Juniper Cloud Workload Protection is highly effective at detecting the increasingly sophisticated attacks that target applications but often go undetected by network and endpoint security solutions. Juniper's easy-to-deploy, non-invasive agent installs in minutes. Using a deterministic technique of optimized control flow integrity (OCFI), Juniper Cloud Workload Protection automatically creates a DNA map of each application at runtime. This map is used to determine whether the application is executing correctly, resulting in extremely accurate attack detection that eliminates almost all false positives.

Juniper Cloud Workload Protection can be deployed in public cloud, on-premises, or in hybrid environments, and it protects web applications, container workloads, and Kubernetes. Whether applications are in production or pre-production, Juniper Cloud Workload Protection provides an effective defense that gives developers an opportunity to remediate vulnerabilities before they become liabilities, and it helps keep organizations in compliance.

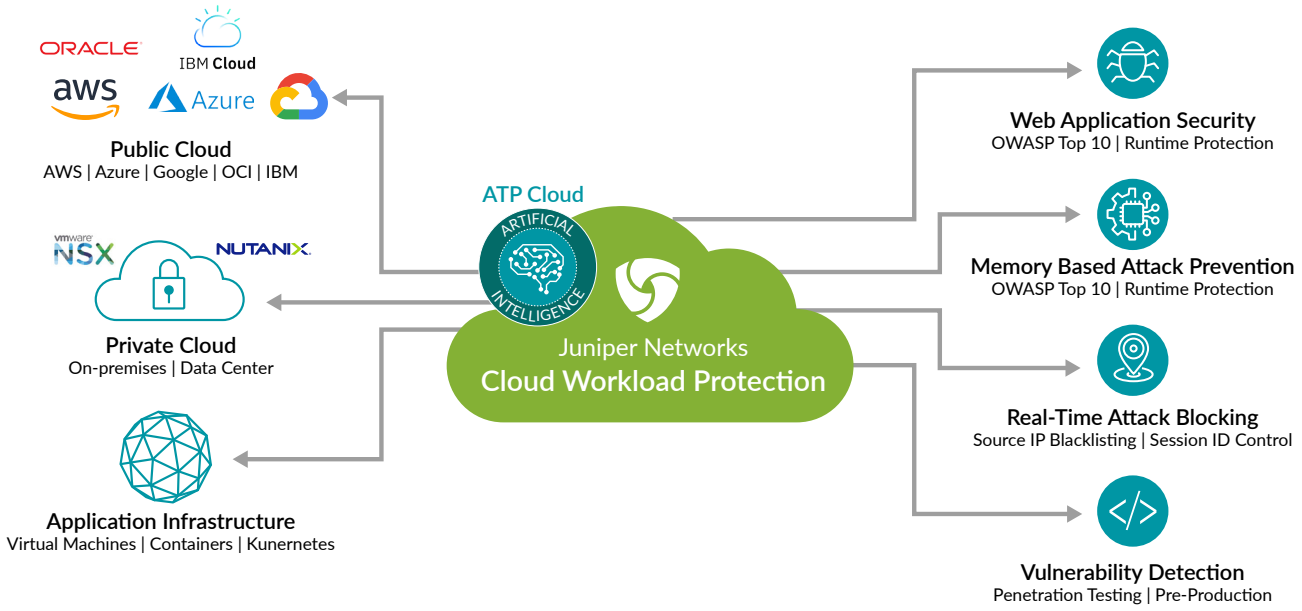

Figure 1: Juniper Cloud Workload Protection architecture.

Architecture and Key Components

Juniper Cloud Workload Protection is a lightweight agent that can be deployed within applications or workloads deployed on Docker, Kubernetes, and AWS Fargate. Application languages supported include Java, Node.JS, PHP, and Ruby. Juniper Cloud Workload Protection helps organizations with:

- Zero-day attacks: Applies deterministic method for detecting zero-day attacks on unknown or unpatched vulnerabilities.
- Vulnerability management: Continuously assesses vulnerabilities in applications and containers.
- Container monitoring: Provides monitoring and reporting of container activity, along with vulnerability scanning.
- Minimal false alerts: Drastically reduces false alerts with a unique DNA map that validates application execution without relying on behavior or signatures.
- Secure mesh/Segmentation: Enhances workload security and prevents lateral propagation of attacks with security service mesh and segmentation.
- Comprehensive telemetry: Provides rich application-level security event generation and reporting, including application connectivity and topology.

Features and Benefits

Juniper Cloud Workload Protection is a lightweight software agent that controls application execution and monitors its behavior and context—tracking what the application is supposed to do against what's happening in real-time. Vulnerability remediation is done automatically without administrator intervention. Juniper Cloud Workload Protection ensures that production applications always have a safety net against vulnerability exploits, keeping business-critical services connected and protected. This new Juniper product provides the following critical capabilities:

Run-Time Application Protection

Signatureless and serverless run-time application self-protection provides real-time protection against attacks. It protects the application from malicious actions, such as exploitation and data theft, without any manual intervention, catching sophisticated attacks that endpoint detection and Web application firewall solutions cannot.

OWASP Top 10 and Memory-Based Attack Prevention

Juniper Cloud Workload Protection provides real-time protection against critical security risks, such as OWASP Top 10 and memory-based attacks, including fileless, return-oriented programming, and buffer overflow attacks.

Comprehensive Telemetry

DevSecOps teams gain insight to threat activity from rich application-level security event generation and reporting, including application connectivity, topology, and detailed information about the attempted attack.

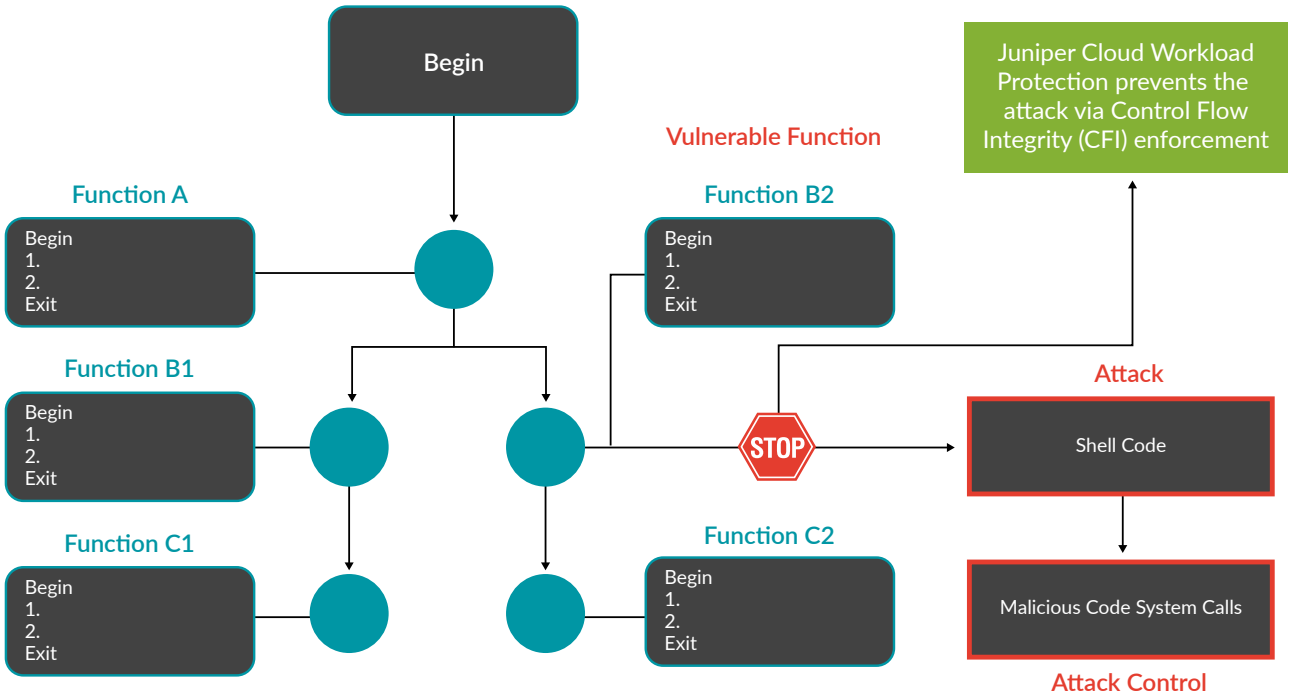

Figure 2: Control Flow Integrity enforcement prevents threats and attacks.

Minimal False Alerts

Optimized Control Flow Integrity technology helps reduce false alerts by validating the execution of applications and detecting attacks without using behavior or signatures.

Web Application Security

Sophisticated attacks on web applications evade detection from signature and pattern-matching solutions like end-point detection and response products and Web application firewalls. Juniper Cloud Workload Protection continuously validates the execution of applications to detect attacks in real-time, with minimal false alerts. When an unknown vulnerability arises or a threat that cannot be immediately patched, Juniper Cloud Workload Protection can protect business services and applications from exploitation. Juniper Cloud Workload Protection helps organizations:

- Significantly improve application security.
- Maintain a high-performance architecture without impacting web applications.
- Support popular development languages and cloud services.

Vulnerability Detection

Security teams have a short window to find vulnerabilities in applications, containers, and custom code. The continuous deployment model shortens the testing window and too often vulnerable components make it to production. Juniper Cloud Workload Protection is deployed alongside penetration testing and scanning tools or in the QA environment, and it provides a unified solution for vulnerability detection. Juniper Cloud Workload Protection provides:

- A single solution to detect vulnerabilities in applications, containers, and user code.
- The exact location of the vulnerability within the code and proof of exploitability for better understanding and quick remediation.
- An agent that integrates into continuous integration processes and continuous development workflows and security testing methodology without interfering, and improving automation.

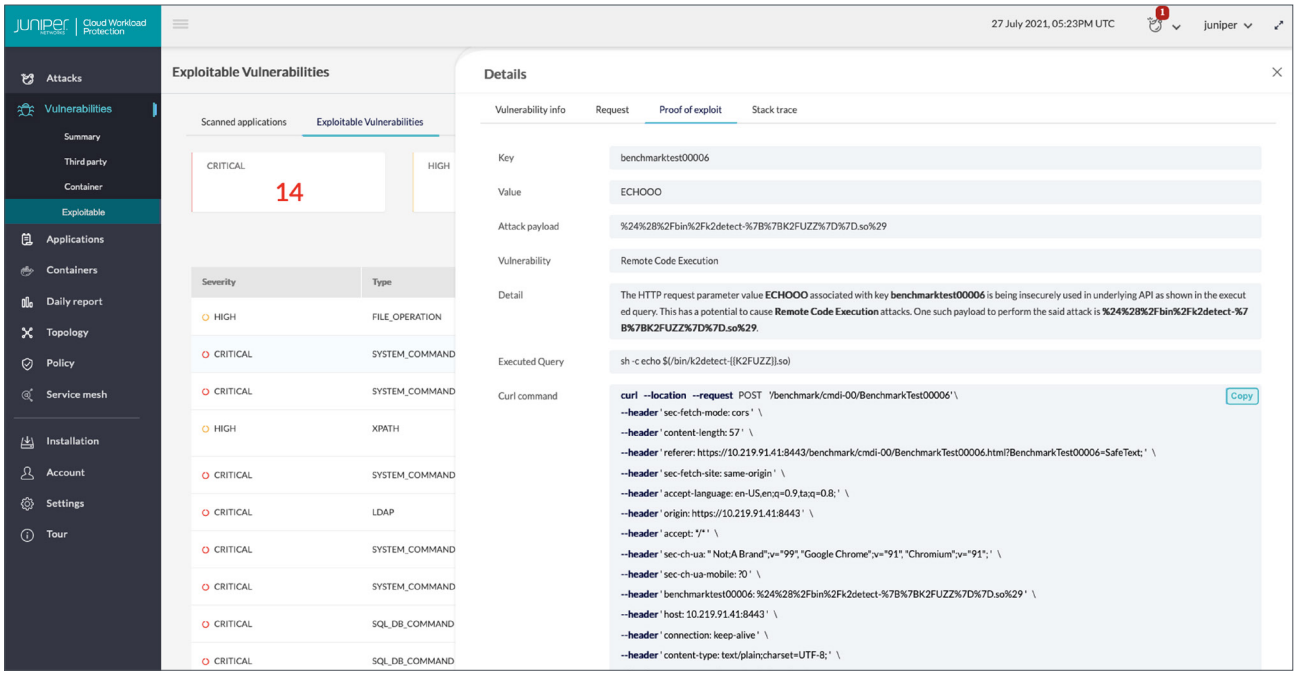

Figure 3: Exploitable Vulnerabilities dashboard.

Container and Workload Security

Cloud native applications running containers can be compromised if the containers have vulnerabilities or backdoors. In addition to protecting applications, Juniper Cloud Workload Protection monitors the behavior of containers and scans them for vulnerabilities to improve security. Segmentation and secure mesh further improves security and reduces the blast radius of attacks. Juniper Cloud Workload Protection delivers:

- Vulnerability scanning for containers and application workloads.
- Behavior monitoring of all containers and API usage, and detects backdoors.
- Protection of cloud-native applications deployed in containers and Kubernetes.

Zero Trust Microsegmentation

Juniper Cloud Workload Protection shields application resources from lateral threat propagation through microsegmentation and integration with the Juniper Networks® vSRX Virtualized Firewall to restrict access based on risk, even as workloads and virtual environments change. Automated threat response with built-in, real-time telemetry helps security teams detect once and block across the entire network.

Juniper Cloud Workload Protection is the newest part of Juniper's Zero Trust data center architecture, a key component in building a threat-aware network. Our world-class data center networking solutions and Connected Security strategy connect and orchestrate application infrastructure across multiple data center environments and secure every point of connection along the way, from the data center gateway to the interconnect, between servers, and within application workloads.

Ordering Information

Juniper Cloud Workload Protection offers flexible licensing options and can be purchased per application or per workload, where all licenses can be transferred to other applications or workloads mid-term at no additional cost.

To order a Juniper Cloud Workload Protection license or to access software licensing information, please visit the How to Buy page at www.juniper.net/us/en/how-to-buy/.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 2401119 PZ
Schiphol-RijkAmsterdam, The
Netherlands Phone:
+31.207.125.700

Agile Networks
3200 Lake Drive,
Citywest Business Campus,
Dublin 24, Ireland
Phone: +353-1-8853160
www.agilenetworks.ie