CONTEXT-AWARE ACCESS CONTROL WITH JUNIPER AND WOOTCLOUD

Identify every device on your network, profile risks, and take action

Challenge

The proliferation of IoT and unmanaged devices with limited or no local security software exposes corporate networks to cyber attacks. Lack of visibility leads to security exposures, downtime, lower productivity, and spiraling operational costs.

Solution

The Juniper and WootCloud solution offers complete visibility and context-aware control over wired and wireless devices from the moment they join the network, identifying threats and ensuring devices comply with security policies.

Benefits

- *Identify known and unknown threats across wired and wireless networks*
- *Exploit ML and AI to calculate risk from unmanaged and transient devices*
- *Automate risk mitigation through visibility, context, microsegmentation, and access control*
- *Observe and manage devices at IoT scale, enforcing at the switch, access point, and firewall*

With the increasing number of devices attaching to the enterprise wired and wireless network, organizations are looking for tools to help them identify and control who and what is connected. The required technology must gather device-level analytics to determine a specific device's risk profile and share this information across network management, enforcement, and monitoring solutions. The goal is to ensure that only authorized devices are allowed to stay connected to the network, and any potential threats are quickly mitigated to prevent lateral spread by leveraging enforcement across wired and wireless networks.

The Challenge

The increasing number and types of devices connected to the network—especially those that are unmanaged or lack the ability to run local security software—require the business to find other ways to identify and remediate threats quickly. Compounding this challenge is a proliferation of connected devices that occupy multiple communication spectrums like Wi-Fi, Bluetooth, BLE, and ZigBee.

Smart device manufacturers have little experience dealing with security, and there are no industry-defined standards to drive trusted software development. Many smart devices store and send sensitive data, including credentials, in plain text, effectively making default device configurations and passwords public.

These devices end up connecting to the enterprise over the LAN, WAN, and Personal Area Network (PAN), where a single attack can affect an entire series of connected devices. The complex layers of smart device systems make it difficult to identify problems by obfuscating their origins. As a result, while identifying all devices via device fingerprinting has become critically important, traditional device fingerprinting doesn't provide enough information to act upon confidently.

Knowing who and what devices are on the network through the use of artificial intelligence (AI) and machine learning (ML) is key to using the entire network as a threat detection and enforcement tool. Juniper® Mist™ cloud services AIOps and WootCloud work together to understand who and what is on the network and enforce corporate security policies in an automated fashion while reducing risk to the enterprise.

The Juniper Networks-WootCloud Solution

Working together, Juniper Networks and WootCloud have developed a Context-Aware Access Control solution that gives network and security admins the tools they need to increase device visibility and provide enforcement at every network connection point. Context-Aware Access Control includes device-level risk and threat assessment that delivers an industry-leading integrated solution, providing actionable insights by combining device context, network data, and threat intelligence.

The joint Juniper-WootCloud solution allows organizations to quickly understand the risk profile for all devices, including unmanaged, transient, and IoT, using this information to enforce a unified policy across the wired and wireless network infrastructure.

With Juniper Connected Security, all network devices—not just perimeter firewalls—work together as a unified threat detection and security enforcement domain. The solution begins with Juniper Networks® SRX Series Services Gateways, which gather threat intelligence across the network and provide enforcement and filtering at the perimeter.

Juniper Advanced Threat Prevention Cloud gathers threat intelligence, leveraging device-level information provided by WootCloud HyperContext. This includes threat and risk assessment for the devices connected to the wired and wireless network, providing real-time visibility and ensuring risks are known for all connected devices.

Knowing the threat and risk score for all connected devices allows Juniper Mist cloud services to automate enforcement across the Juniper Series of High-Performance Access Points and Juniper Networks EX Series Ethernet Switches. Devices found to have a higher risk can be automatically quarantined or removed from the network until they can be investigated and remediated to reduce the risk level, at which point they are allowed to reconnect.

Through WootCloud, policy enforcement can also be extended to an SRX Series firewall to automatically prevent devices with a higher risk level from connecting to the network until those devices are remediated. This ensures policies can be applied to block or quarantine devices regardless of where they are on the network.

Working together, Juniper and WootCloud ensure complete network visibility across wired and wireless networks. The joint Context-Aware Access Control solution defines device risk and suggests mitigation policies across the network, greatly enhancing security while reducing the time for detection and policy enforcement.

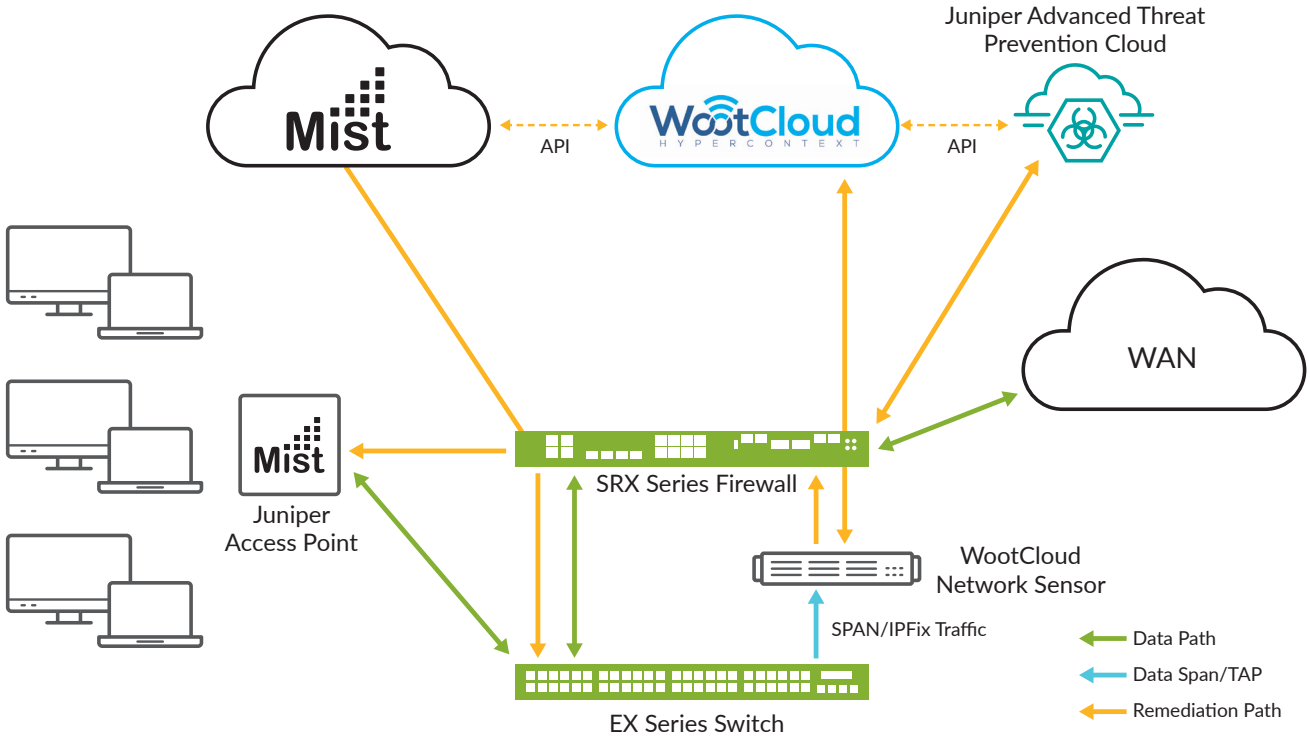

Figure 1: Context-Aware Access Control from Juniper and WootCloud

Features and Benefits

The integration of context-aware access control from Juniper Networks and the contextual device security from WootCloud delivers:

- Greater visibility and enforcement for all devices, including unmanaged, transient, and headless
- A more comprehensive connectivity and risk score for every device in the environment
- Microsegmentation via software-driven dynamic access control beyond 802.1X
- Zero-day threat detection, lateral threat prevention, and remediation

Solution Components

SRX Series Services Gateways

SRX Series Services Gateways are intelligent next-generation firewalls (NGFWs) that deliver outstanding protection, market-leading performance, six nines reliability and availability, scalability, and services integration. Available in both physical and virtual form factors, SRX Series firewalls are ideally suited for service provider, large enterprise, and public-sector networks, delivering the highest level of protection all the way to the application layer. SRX Series NGFWs also offer advanced services such as application security, advanced security services, intrusion prevention system (IPS), integrated threat intelligence services, and Juniper Advanced Threat Prevention.

Juniper Advanced Threat Prevention Cloud

Juniper Advanced Threat Prevention is a cloud-based service that integrates with SRX Series firewalls, extending security to deliver a dynamic anti-malware solution that adapts to an ever-changing threat landscape. The solution also includes Security Intelligence (SecIntel) for a comprehensive view of known threats, encrypted traffic insights to uncover hidden threats using SSL encryption, and adaptive threat profiling.

EX Series Ethernet Switches

EX Series Ethernet Switches are designed to meet the demands of today's high-performance businesses, letting companies grow their networks at their own pace while minimizing large up-front investments. Based on open standards, EX Series switches provide the carrier-class reliability, security risk management, virtualization, application control, and TCO that today's businesses demand.

Juniper Access Points

Juniper offers a variety of Wi-Fi access points and cloud-based services such as asset tracking, location capabilities using virtual Bluetooth Low Energy (vBLE), Juniper Mist Wired Assurance, Juniper Mist Wi-Fi Assurance, and the Marvis Virtual Network Assistant. For Juniper SD-WAN deployments, the Contrail® Service Orchestration Web portal provides visibility into Juniper Access Points by enterprise site and context-aware pass-through to the Juniper Mist portal.

Juniper Mist Cloud Services

The Juniper Mist cloud services platform can be fully operated and managed through a programmable cloud that includes microservices and an inline AI engine to deliver superior scalability, agility, resiliency, and insights. Juniper Mist cloud services provide onboarding, configuration, and operation control over all wireless deployments and all EX Series access switching deployments. They also provide operational and management functions that deliver Wi-Fi, virtual Bluetooth LE services, Juniper Mist Wi-Fi Assurance and Juniper Mist Wired Assurance, including user service levels, anomaly detection, automated event correlation for troubleshooting, dynamic packet capture, policy configuration, guest WLAN access, and more.

WootCloud HyperContext Platform

The WootCloud HyperContext Platform performs the following functions.

- **Device Discovery**: Delivers an agentless, passive, and nonintrusive solution that discovers managed and unmanaged devices on both the network and RF spectrums, tying these spectrums to a single device.
- **Granular Device Context**: Collects device information from physical, logical, operational, and locational touch points and performs deep packet inspection to provide a fine-grained analysis of every device in the organization.
- **True Identity**: Accurately identifies and fingerprints all new devices in the organization automatically, recognizing anomalous behavior at the device level and offering insights and analytics about device-level risks, threats, and best practices around mitigating threat profiles.
- **Risk Assessment**: Provides a unique risk profile for each device, calculated by a proprietary algorithm to identify SecOps, Network Ops, and IT Ops gaps to improve device risk posture.
- **Microsegmentation**: Implemented in a software layer, decoupled from the network hardware and network access control (NAC) tools, and, when coupled with deep device context, delivers segmentation that is easy to deploy and operate automatically at IoT scale.
- **Large-scale automation via policy enforcement**: Includes a powerful policy engine that automates and enforces control points for large numbers of devices, maintaining organizational hygiene.

Summary—Make Your Network More Intelligent with Context-Aware Access Control from Juniper and WootCloud

The joint Juniper-WootCloud Context-Aware Access Control solution gives enterprises a complete picture of all devices connected to the network, ensures these devices adhere to the risk and threat profiles set forth by the organization, and offers automated policy enforcement and remediation. This joint solution delivers consistent security across the wired and wireless network to effectively identify and mitigate threats, all while making the network more intelligent.

Next Steps

To learn more about the Juniper-WootCloud solution, please contact your Juniper or WootCloud representative, or visit https://juniper.net and https://wootcloud.com/.

About WootCloud

WootCloud HyperContext® is an agentless, device focused, network segmentation, access control, and threat response platform that automates enterprise security at IoT scale. A privately held company, WootCloud is headquartered in San Jose, California, with offices in India and Argentina.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701