DEFENDING NETWORK ACCESS WITH RISK PROFILING DRIVEN BY MIST AI

See what's connected to your network using AI and mitigate threats with a single click

Challenge

IT teams need to find a way to protect their networks, including those devices they don't directly control but must allow to connect.

Solution

Juniper's Risk Profiling driven by Mist AI empowers IT teams to defend their infrastructure by providing deep network visibility and enabling policy enforcement at every point of connection throughout the network.

Benefits

- *Quickly identify and react to compromised devices*
- *Lower operational costs*
- *Optimize the user experience*
- *Physically locate compromised wireless devices*

One of the most common vulnerabilities found in networks that have experienced security breaches is inadequate network visibility. You cannot mitigate or adequately respond to a breach if you don't know what's happening on your network. But there is far too much occurring on today's networks for administrators to handle on their own. Enter Risk Profiling driven by Mist AI.

Risk Profiling driven by Mist AI brings Juniper® Connected Security to the AI-Driven Enterprise by combining real-time actionable threat detection and intelligence with AIOps driven by Mist AI™. With AI-Driven Risk Profiling, your Juniper wireless infrastructure will be secured by Juniper® Advanced Threat Prevention.

The Challenge

The life cycle of networked devices is no longer controlled by IT. Employee-owned devices share networks with other corporate-owned equipment when working remotely. IoT devices, which are virtually impossible to secure, are regularly added to networks without IT's knowledge.

The network perimeter is now everywhere. Preventing compromise is nearly impossible. IT professionals need a solution that allows them to see when compromise events occur, automate responses to those events, and move quickly to protect the rest of the network from further compromise.

Juniper Networks Risk Profiling Driven by Mist AI

Juniper Networks® Risk Profiling driven by Mist AI brings network security to the distributed access network edge. Campus and branch networks, along with managed work-from-home and pop-up network sites, are now active participants in their own defense as part of the threat-aware network. Integration with Mist AI speeds resolution of user experience and information security events alike, lowering operational costs.

Risk Profiling driven by Mist AI extends security beyond the Internet perimeter without requiring access network administrators to learn a new tool. This allows Wi-Fi administrators to quickly identify and react to compromised devices without having to engage other teams.

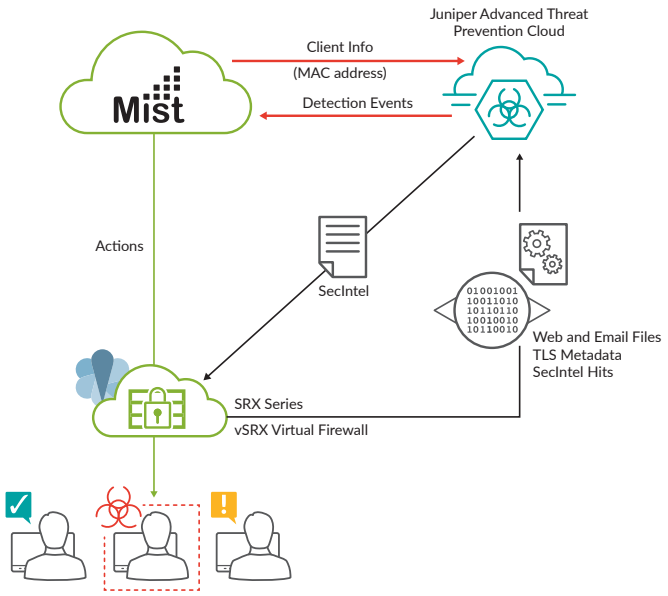

Figure 1: The major components of Risk Profiling driven by Mist AI

Any infected wireless client observable by Mist AI will have a threat score/indicator associated with it. This threat score is determined by Juniper Advanced Threat Prevention Cloud. Clients with no detections will not have a score. Mist Client Level Insights are based on threat detections made by Juniper Networks® SRX Series Services Gateways and Juniper Advanced Threat Prevention Cloud.

Features and Benefits

Risk Profiling driven by Mist AI delivers the following features.

- Powerful security intelligence powered by Juniper Advanced Threat Prevention Cloud:
  - Dynamic malware analysis
  - SecIntel threat feeds
  - Encrypted traffic insights
  - Infected host risk scoring
- Threat intelligence-based actions:
  - Take place within the Juniper Advanced Threat Prevention Cloud
  - Based on risk score
  - Offer one-touch mitigation
- Geospatial location of devices:
  - Locate on your map
  - Devices can be moving or stationary
  - Locate people or IoT devices

Solution Components

Requirements:

- Junos® operating system 19.4 (20.2 for ETI)
- Juniper Mist™ Wi-Fi Assurance
- Juniper Mist™ WAN Assurance
- Juniper Advanced Threat Prevention Cloud

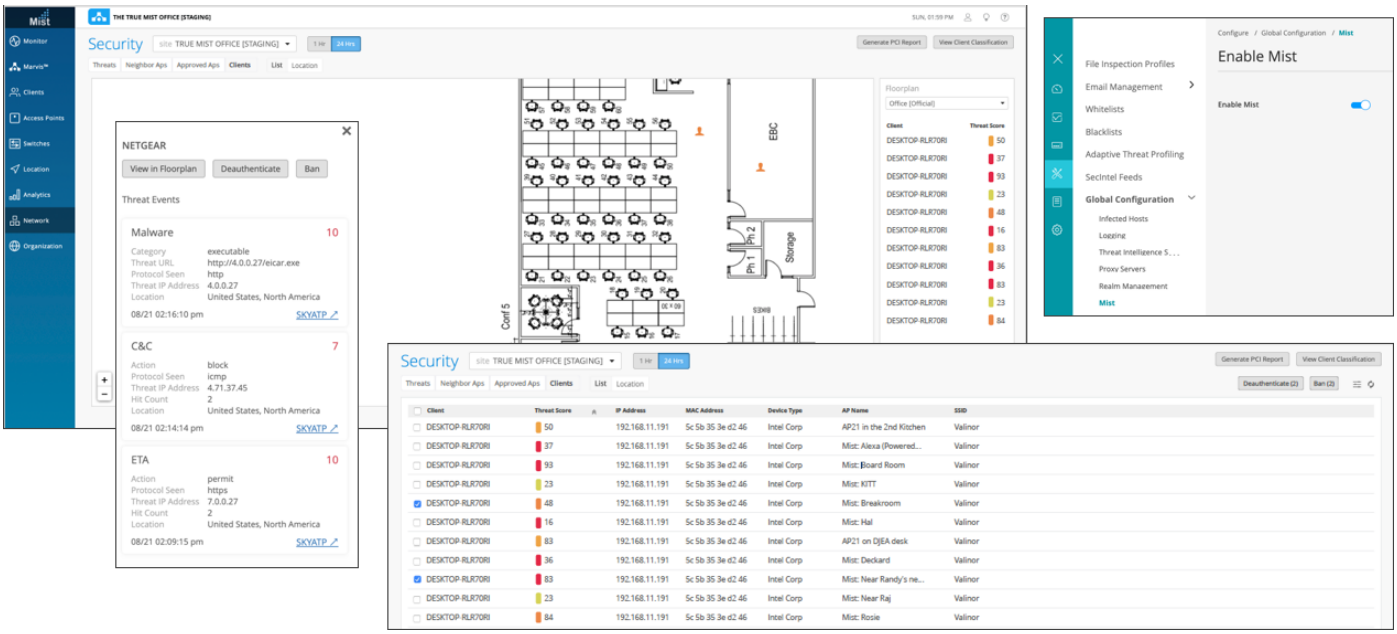

Figure 2: Risk Profiling driven by Mist AI features

Works with:

- Juniper® Series of High Performance Access Points
- Juniper Networks EX Series Ethernet Switches
- SRX Series Services Gateways (vSRX Virtual Firewall, 3xx, 15xx)

Threat alerts shared by Juniper Advanced Threat Prevention Cloud with Mist AI include:

- Malware downloads from websites
- Malware downloads from e-mail attachments
- SecIntel hits
  - Command and Control server (C&C), attacker IP, third party, etc.
- Encrypted traffic insights detections
- Host status changes:
  - Mitigation events taken by the customer (such as resolving an event as fixed, ignored, or false positive)
  - Done through Juniper Advanced Threat Prevention Cloud customer portal

See, Automate, and Protect

The end of strict control over endpoints is not the end of IT security. The best and arguably the only realistic option for most organizations to secure a network going forward is to build security into the network itself. Risk Profiling driven by Mist AI provides a critical layer of visibility and policy enforcement for the threat-aware networks of the next decade.

Next Steps

To find out more about Juniper Networks products and solutions, please visit www.juniper.net.

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