PALO ALTO NETWORKS AND INDENI

Device Health Automation

Key Benefits of the Integration

Find issues accurately:

Indeni uses XML APIs and SSH to apply device-specific health checks created by Palo Alto Networks administrators.

Analyze devices continuously:

Monitor device state, configuration skew, and deviation from local standards as well as best practices.

Solve complicated problems quickly:

Each issue includes context, history, impact, suggested remediation steps, and relevant Palo Alto Networks Support Portal links.

The Challenge

Next-generation firewalls (NGFWs) bring enhanced security with rich APIs to provide high internal visibility. Still, many organizations use generic monitoring frameworks for system health analysis. The resulting lack of context can lead to misdiagnosis, increasing error rates as well as the time and effort required for what should be routine maintenance.

Palo Alto Networks and Indeni

The Indeni Knowledge Platform delivers precise, actionable insight for Palo Alto Networks NGFWs. Using Indeni, enterprises can continuously ensure each NGFW is set up according to best practices, runs at top performance, and meets industry standards.

Indeni Knowledge Platform

Indeni gives IT teams the information they need to find, analyze, and resolve network issues. Through a combination of curated learning, continuous analysis, and precise remediation steps, Indeni helps IT proactively address issues and efficiently use talented resources.

Palo Alto Networks

The Palo Alto Networks Security Operating Platform prevents successful cyberattacks through intelligent automation. It combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks, and mobile devices, natively providing the right capabilities at the right place across all stages of the attack lifecycle.

Use Case No. 1: Automated Health and High Availability Readiness Validation

Challenge

Palo Alto Networks NGFWs are feature rich, but relying on CPU and memory usage doesn't provide enough insight into how well those features are working. Likewise, high availability keeps traffic flowing—but only with proper synchronization of state and configuration within the cluster.

Answer

Using native queries via XML API and CLI over SSH, Indeni applies knowledge specific to Palo Alto Networks NGFWs and Panorama™ management for continuous detection of potential problems. This includes, among other things, best practice violations, high availability unreadiness—such as cross cluster routing table next-hop mismatches—and outages due to expiration of licenses or support.

Use Case No. 2: Reduce Administrative Overhead and Operational Impact

Challenge

Customers trust Palo Alto Networks NGFWs in sensitive roles with tight risk tolerances, but they often defer PAN-OS® updates out of uncertainty about new builds. Each new maintenance release means customers must accept risk, either from known issues or from a new build.

Answer

Indeni Knowledge modules are updated frequently by expert administrators based on recent events, support announcements, and new PAN-OS releases. Each detected issue includes a description, impact, and remediation steps, providing actionable information to maintain trust in the NGFW.
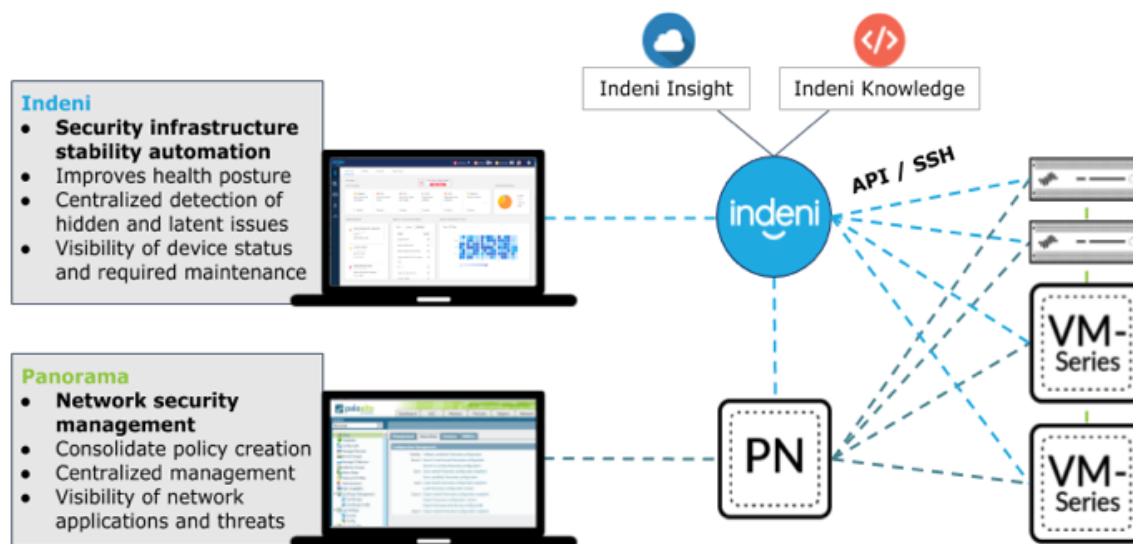

Figure 1: Palo Alto Networks and Indeni integration

About Indeni

Indeni is the automation platform for network and security infrastructure stability. With content built by Indeni Crowd, organizations gain access to a living repository of device-specific modules for maintenance, high availability, network visibility, security, compliance, and vendor best practices. Learn more at https://indeni.com.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices. Find out more at www.paloaltonetworks.com.