Palo Alto Networks and Venafi

Eliminate Threats with Automated Decryption and Machine Identity Lifecycle Orchestration

Benefits of the Integration

Together, Palo Alto Networks and Venafi enable you to:

- Seamlessly, automatically manage and monitor all Palo Alto Networks machine identities, ensuring they adhere to issuance policies and compliance. Automatically notify and deploy on target systems.
- Automatically discover which machine identities are installed on your Palo Alto Networks devices and ensure that the right identities are enabled and optimally functioning.
- Mitigate risks by decrypting network traffic to detect and remediate threats that lie in encrypted communications.

The Challenge

There are two actors on a network: people and machines. People rely on usernames and passwords to identify themselves to machines so they can access networks and data. Cryptographic keys and digital certificates identify and authenticate machines. As the number of machines increases—driven by digital transformation and the emergence of more machine types, including cloud workloads, virtual machines, containers, and internet of things (IoT) devices—these keys and certificates become more critical.

Industry experts believe that encrypted traffic will carry more than 70% of web malware in 2020. That's a huge blind spot for enterprise security systems, which may not have threat detection or protection against these attacks. Cybercriminals can use encryption against enterprises to conceal malware delivery, eavesdrop on communications, and exfiltrate data undetected, undermining layered security defenses. With the widespread adoption of TLS/SSL encryption, the ability to ensure every key and certificate is available for decryption—and then to decrypt and inspect TLS/SSL traffic in real time—is more important than ever.

Venafi Trust Protection Platform

Venafi Trust Protection Platform manages machine identities by delivering an enterprise-grade platform designed for security, operational efficiency, and organizational compliance. The platform provides visibility of all machine identities across the extended enterprise. With full situational awareness of cryptographic security risk posture at all times, organizations are able to automate the identification of weak certificates while enabling quick response with automated remediation.

Palo Alto Networks

Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) inspect all traffic at Layer 7 and offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

ML-Powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The application, content, and user—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Palo Alto Networks and Venafi

Palo Alto Networks ML-Powered NGFWs and the Venafi platform work together to protect privacy, secure network transactions, and defend intellectual property. The integrated solution helps you identify which encrypted channels you can trust and which are being used in an attack. With the Venafi platform in place, Palo Alto Networks NGFWs have secure and unhindered access to machine identities, allowing them to detect and prevent attacks that hide in encrypted channels.

Use Case No. 1: Enable Traffic Decryption to Inspect all Ingress and Egress Traffic

Challenge

The inability to decrypt traffic at vital ingress and egress points poses great risk to an organization. Invalid or expired machine identities allow threats to go undetected.

Solution

You can leverage Venafi Trust Protection Platform to manage the lifecycle of machine identities across Palo Alto Networks devices, enabling detection of threats hiding in encrypted traffic. As an added benefit, you gain increased visibility by automating the delivery of certificates to Palo Alto Networks devices as soon as they are renewed. This eliminates gaps in the inspection process from expired certificates.

Use Case No. 2: Provision Trust Stores

Challenge

A trust store is a collection of root certificates that are trusted by default and maintained by the companies that make operating systems and web browsers. Maintaining allow and block lists of trusted root certificates is difficult because different devices on a network all have different file type requirements. This leads to manual processes wherein accidental misconfiguration may lead to unwanted trust, which can be devastating to security.

Solution

Venafi Trust Protection Platform allows your administrators to create trust "bundles" of easily updated and maintained allowed and/or blocked certificates, which can be automatically provisioned to Palo Alto Networks devices that need them. This can help alleviate resource bottlenecks by automating manual tasks around machine identities in your organization.

About Venafi

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. To learn more, visit www.venafi.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

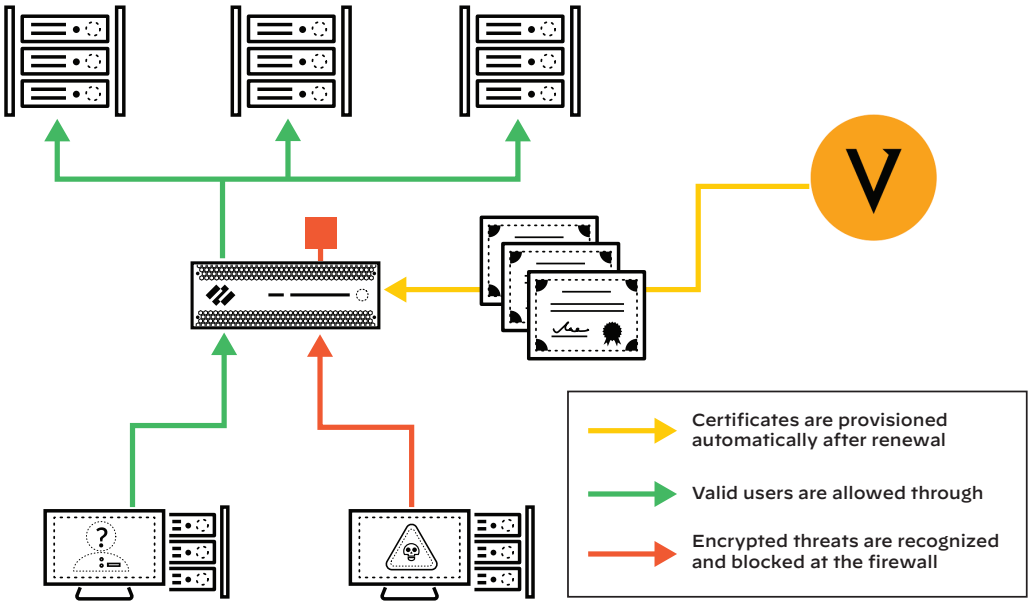

Figure 1: Automatic decryption with Venafi, enabling Palo Alto Networks NGFWs to detect threats in encrypted traffic

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

palo-alto-networks-and-venafi-tpsb-111320