CHECK POINT + VENAFI

PROTECT MACHINE IDENTITIES

PROTECT THE KEYS TO YOUR SECURE KINGDOM

Solution Benefits

- Detect threats hiding in encrypted traffic
- Maximize inspection with full machine identity discovery
- Safely enable allowed internet traffic while blocking malicious use of SSL/TLS encrypted channels
- Get started fast with existing machine identity inventory
- Maintain maximum inspection levels with fully automated machine identity lifecycle and distribution to firewalls

Solution Features

- Inspect TLS traffic using keys and certificates from applications
- Secure allowed encrypted channels
- Block malicious encrypted channels or internet use not allowed by policy
- Automate discovery and setup of existing machine identities
- Increase performance of inspection with automated distribution of machine identities
- Automated distribution of new machine identities when they are generated and/or renewed

INSIGHTS

There are two actors on a network—people and machines. People rely on usernames and passwords to identify themselves to machines so they can get access to 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 many more machine types, including applications, cloud workloads, virtual machines, containers and IoT—these machine identities become more critical.

Unfortunately, cybercriminals understand the power of keys and certificates and will often utilize machine identities in their attacks. Cybercriminals are using encryption against enterprises to conceal malware delivery, eavesdrop on communications and exfiltrate data undetected—undermining layered security defenses.

Industry experts believe over 70% of web malware will be carried by encrypted traffic in 2020. That's a huge blind spot for enterprise security systems, which may not have threat detection or protection against these attacks. With the widespread adoption of SSL/TLS encryption, the ability to ensure every key and certificate is available for decryption and then decrypt and inspect SSL/TLS traffic in real time, is more important than ever.

JOINT SOLUTION

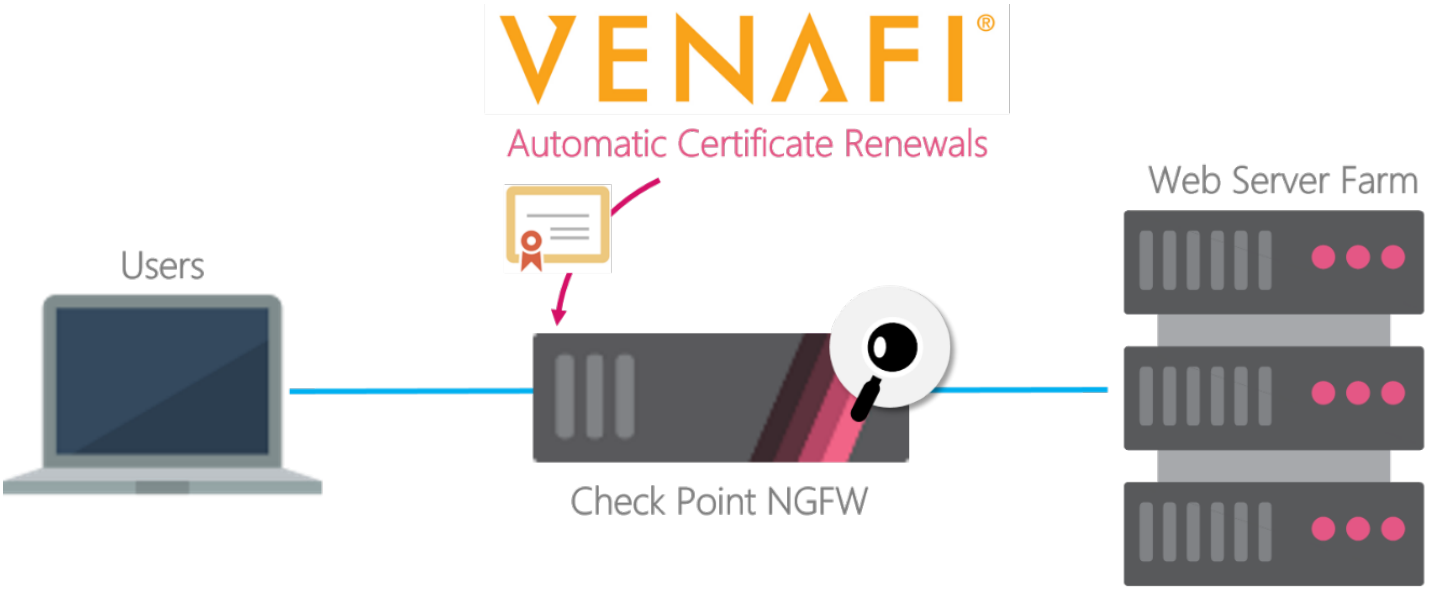
Together, Check Point and Venafi enable your organization to detect threats hiding in encrypted traffic. The Venafi Platform allows enterprises to protect and secure large numbers of highly complex machine identities. It provides the visibility needed to discover and automate the full lifecycle of SSL/TLS keys and certificates so that Check Point Next Generation Firewalls always have current machine identities to inspect traffic for threats.

Check Point Next Generation Firewalls (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 should be trusted, and which are being used as part of an attack. With Venafi in place, Check Point NGFWs have secure and unhindered access to machine identities, allowing them to detect and prevent attacks that hide in encrypted channels.

HOW IT WORKS

The Venafi Adaptable Application Driver for Check Point automates SSL/TLS machine identities used in Check Point inbound HTTPS inspection policies. Certificates are defined as Venafi-synced objects within Check Point and automatically kept in sync with the Venafi Trust Protection Platform.

- Bulk-provisioning jobs in Venafi allow new machine identities, matching specified policy, to be provided to Check Point gateways automatically on a schedule or on-demand.
- Expiring certificates are automatically renewed at the certificate authority (CA), provisioned by Venafi to Check Point NGFWs and applied in the Check Point NGFW HTTPS inspection policy.
- Inspection policies are always up-to-date with the most recent version of machine identities, ensuring there are no gaps in SSL/TLS visibility, and encrypted threats are never missed.



CONCLUSION

While SSL/TLS provides security and authentication, it also can create blind spots for enterprise security. Cybercriminals can use encryption to hide malicious activity from an organization's security controls, including NGFW, intrusion prevention systems (IPS) and controls in order to evade detection and hide attacks. Together, Check Point and Venafi help to solve that problem by fully automating the delivery and configuration of critical machine identities in use by organizations protected with Check Point NGFWs.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT VENAFI

Venafi is the cybersecurity market leader in machine identity protection, 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.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | www.checkpoint.com