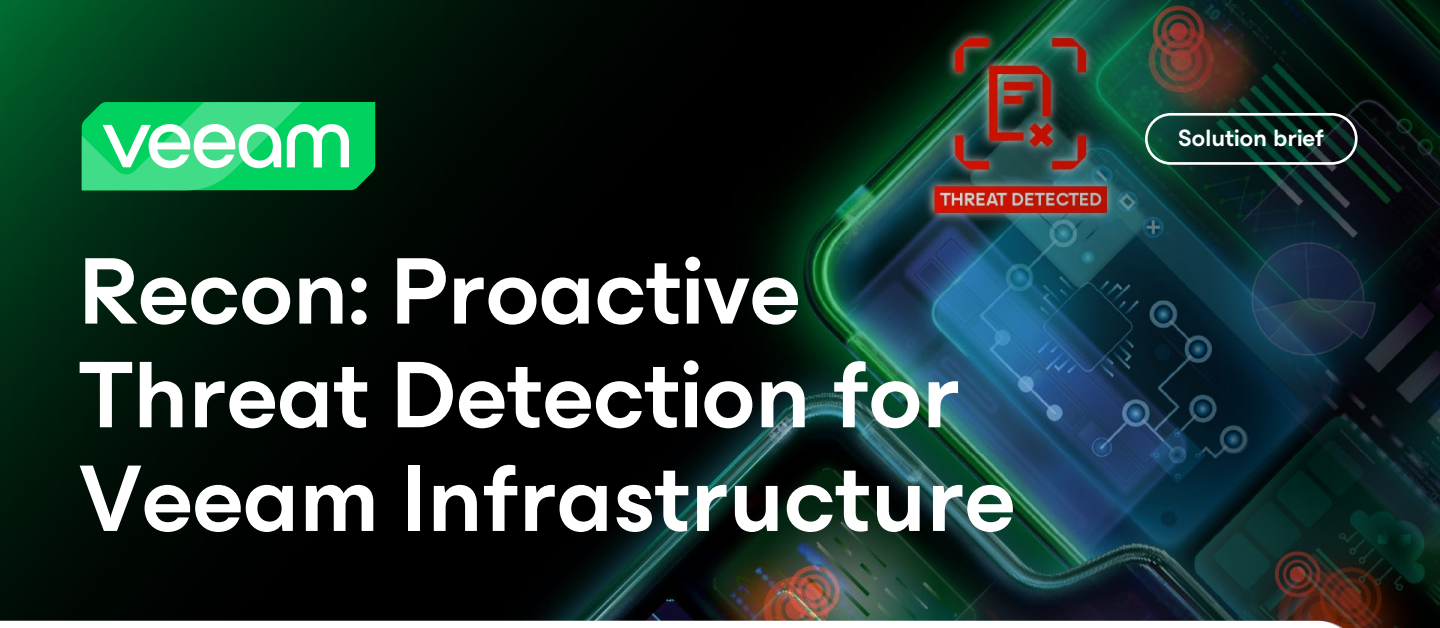

Solution brief

Recon: Proactive Threat Detection for Veeam Infrastructure

Overview

Recon is a patent-pending, lightweight software agent integrated into Veeam Data Platform Advanced and Premium Editions. Developed in collaboration with Coveware by Veeam, it is the only solution in the data protection market offering proactive behavior-based detection based on real-world ransomware incidents.

How It Works

Recon continuously monitors Veeam environments for:

- Unusual user behavior and brute force login attempts
- Unexpected network connections
- Suspicious file activity and installations
- Data exfiltration attempts

Each event is analyzed and mapped to known adversary tactics and techniques, enabling IT and security teams to take preventive action swiftly.

Key Benefits

- **Proactive Threat Detection:** Identifies suspicious activity before it escalates into a full-blown cyberattack.
- **MITRE ATT&CK Mapping:** Automatically correlates findings to adversary Tactics, Techniques, and Procedures (TTPs).
- **Rapid Deployment:** Easily installed on Veeam Backup & Replication servers, proxies, gateways, Active Directory servers and other servers within the Veeam environment (up to 10 servers).
- **Secure Data Handling:** Collected data is encrypted and securely uploaded to a cloud-based portal for analysis. Findings are also now available in the Veeam Data Platform Threat Center.
- **Findings available via API for third party integration:** The Veeam app for Microsoft Sentinel includes Recon findings.

Case Study

A municipality using Veeam Data Platform Premium Edition deployed Recon across its infrastructure.
It immediately detected brute force attacks from foreign IPs and alerted the IT team. Prompt action was taken to block login attempts, preventing compromise and a ransomware attack thus safeguarding sensitive financial and personal data.

Why It Matters

With ransomware threats evolving rapidly, organizations need more than reactive defenses. Recon empowers teams to detect and respond to threats before damage occurs by delivering unmatched data resilience and peace of mind.

Complementary Technologies

Recon is part of a broader Veeam Data Platform security feature set including:

- **Inline Scanning:** Provides inline entropy analysis, with AI-powered in-process detection of ransomware encryption and text artifacts including dark web links and ransom notes.
- **Guest Index Data Scan:** Detects threats during backup using advanced file system activity analysis to detect the appearance of suspicious files, large number of file deletion, renamed files, or file extension changes.
- **Veeam Threat Hunter:** Best-in-class machine learning and heuristic analysis signature-based backup scanner designed to detect millions of malware variants. It includes a frequently updated database of malware signatures to ensure up-to-date protection.
- **IoC (indicators of Compromise) Tools Scanner:** Identifies tools that are utilized by threat actors and notifies before impact.
- **Security and Compliance Analyzer:** Built-in security assessment tool to ensure that backup environments follow security best practices.

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data portability, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 82% of the Fortune 500, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam