Versa Advanced Threat Protection

As cyber threats evolve, intensifying in both frequency and sophistication, traditional security paradigms are falling short. Businesses must proactively enhance their security programs with more advanced, agile, and intelligent systems to defend against sophisticated threats, including zero-day exploits, advanced persistent threats (APTs), ransomware, and phishing attacks.

Why Versa Advanced Threat Protection?

Part of Versa's Unified SASE offering, Versa Advanced Threat Protection (ATP) is an intelligent blend of AI-driven file analysis and sandboxing. This combination creates a formidable security shield capable of thwarting cyber threats from phishing and exploit delivery to more elusive zero-day malware attacks. By isolating and examining suspicious files in a safe, controlled environment, sandboxing reveals clandestine threats and generates invaluable threat intelligence. This intelligence offers real-time insights into emerging threats and their attack modes, enabling proactive defenses.

Since the Versa Unified SASE platform cohesively integrates networking and security at the operating system level through a unique single-pass scanning architecture, Versa ATP achieves an unrivaled depth of visibility and context regarding network traffic, user behavior, and security events. Versa ATP ensures organizations are faster and targeted in their response, allowing them to make better informed, proactive decisions to bolster their defenses.

As shown in Figure 1, Versa ATP collaborates with other components of Versa's Security Service Edge (SSE) suite to deliver a comprehensive security solution that safeguards organizations at every level. These components include: Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), Data Loss Prevention (DLP), Remote Browser Isolation (RBI), Intrusion Protection System (IPS), malware protection, IP reputation, URL filtering, application control, Denial-of-Service protection, and Next Generation Firewall (NGFW), among others.

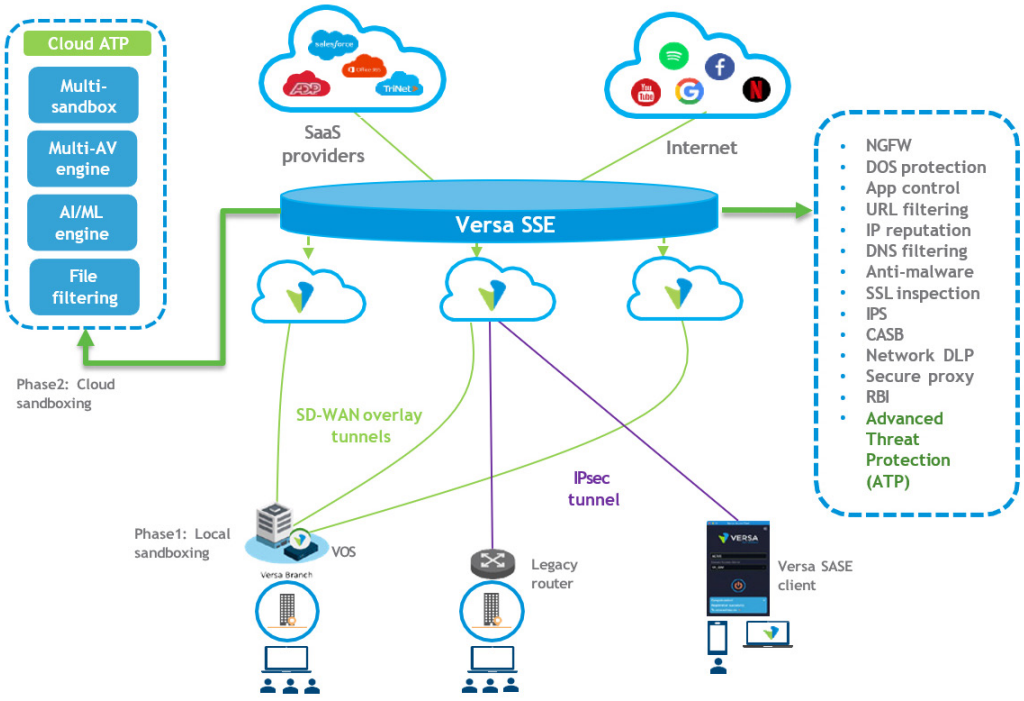

Fig. 1: Versa unified platform with Advanced Threat Protection capability

How It Works

Versa ATP works in two phases. The first phase is local file analysis by an on-premises Versa Operating System (VOS) device or Versa SASE Gateway (also referred to as Versa Cloud Gateways), which performs preliminary analysis and evaluation of files. In the second phase, cloud multi-sandboxing is performed for zero-day protection. Both phases are detailed below.

Local File Analysis by on-premises VOS devices and Versa SASE Gateways

Versa's local file-analysis components inspect all files and perform file reputation lookup on the on-premises Versa Operating System (VOS) device, as shown in Figure 2 below. The local analysis capabilities described below enable the identification of potential risks and threats early in the process, thereby benefiting organizations with faster threat detection and response times.

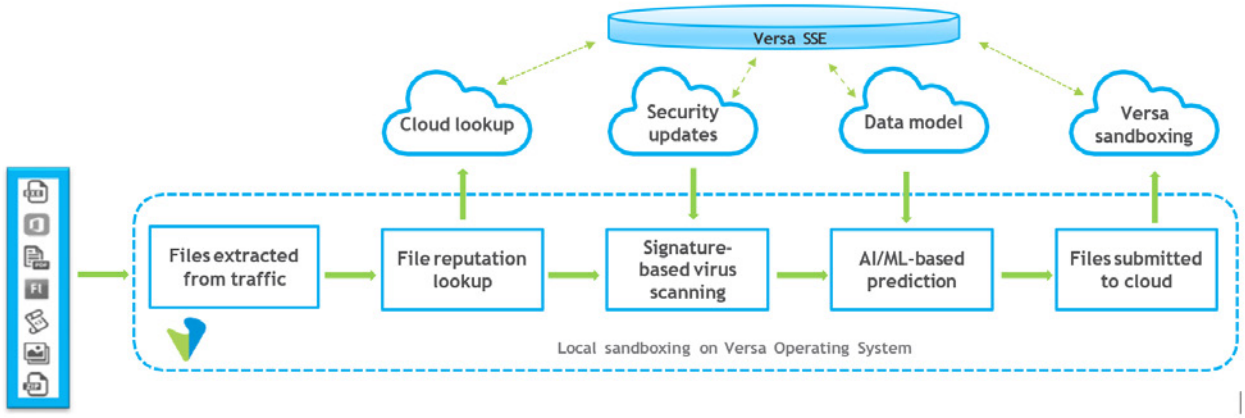

Fig. 2: Steps in the Versa file analysis process that are performed locally on the Versa Operating System

File reputation and signature analysis

Based on the file type, files are extracted from the traffic and reconstructed to compute a SHA-based checksum. A cloud lookup cross-references the file's checksum reputation in the Versa sandbox cloud. If not found, recursive API lookups are performed in third-party databases and cached in the Versa Cloud. Finally, the onboard AV engine analyzes the file, which performs signature and heuristic-based detection. This multi-layered approach ensures that known and unknown threats are effectively detected and blocked as early as possible.

Static and AI/ML analysis

Versa ATP continually harnesses the power of AI and ML technologies to enhance its threat detection and response capabilities. A lightweight AI/ML service runs locally on VOS, receiving data-model updates from the Versa sandbox cloud as needed. Then, it analyzes the file against the trained data model. This helps reduce the number of files submitted to the cloud for further sandboxing, enhancing the end-user experience. Additionally, a static analysis, including YARA rule processing, is conducted to identify any indicators of compromise promptly.

Multi-Sandboxing in the Versa Cloud

If there is no definitive verdict about a file from local analysis, the file is further scrutinized by Versa's Advanced Threat Protection platform. Versa's ATP performs multi-layer and multi-method analysis, which involves static analysis, identification using multiple AV engines, malware detection based on AI/ML, and dynamic analysis by isolating and examining suspicious files in a safe, controlled sandbox environment consisting of virtual machines on bare metal. Suspicious files are sent to the Versa Cloud, where they undergo comprehensive analysis using multiple detection modules designed to identify hidden malicious behavior. Versa ATP utilizes multiple unique detection methods and techniques to augment its sandboxing capabilities. This increases the chances of detecting advanced threats that can evade a single specific type of sandbox environment, providing a more robust defense against sophisticated attacks. Further components are detailed below.

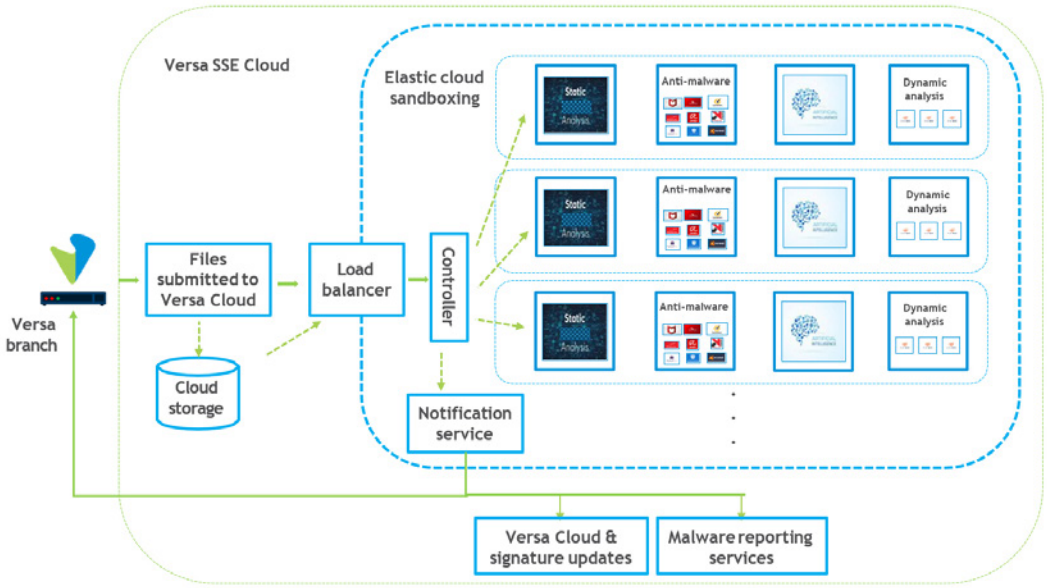

Fig. 3: Multi-sandboxing integrated into the Versa Cloud.

Multiple AV engines

Versa ATP employs multiple cloud-based antivirus engines to bolster its malware detection capabilities. By leveraging the collective intelligence of these engines, the platform can detect and block a broader range of threats, including previously unknown malware variants and zero-day exploits.

Static and dynamic analysis

Versa ATP incorporates static and dynamic analysis methods to improve its threat detection capabilities. Static analysis examines files without executing them, processes them through the YARA rule engine based on the latest YARA rules, and analyzes their code structure and content for signs of malicious behavior and IOCs. In contrast, dynamic analysis runs files in a controlled environment to observe their behavior and identify hidden threats. Using both methods, Versa ATP ensures a comprehensive and accurate analysis of potential threats, resulting in a more effective defense against advanced attacks.

AI/ML-based malware detection

Versa ATP's AI and ML-driven threat detection and response capabilities are trained against a sample of eight billion files, making it very accurate and efficient in detecting threats. Additionally, the data model continually evolves as it analyzes new samples, enabling fast and precise detection of zero-day and APT attacks.

Deception countermeasures

Versa ATP is designed to counter the deception techniques employed by cyber adversaries. By incorporating advanced heuristics, behavioral analysis, and contextual awareness, the system can identify and respond to deception tactics, such as obfuscated code, polymorphic malware, and other evasive techniques that attackers use to bypass security measures.

Reporting and Visibility

Versa ATP has robust reporting and visibility features, empowering organizations to maintain a proactive and adaptive security approach through in-depth insights into network traffic, user behavior, and security events. The detailed reports, real-time insights, and comprehensive analytics available include:

Sandbox analysis reports

Versa ATP sandboxing generates detailed reports on the analysis performed by each detection module. These reports provide insights into the behavior of potential threats, highlighting any malicious activities or patterns detected during the analysis. The analysis places individual threats and behaviors within the context of the broader attack or campaign, equipping organizations with additional information aligned with the MITRE ATT&CK framework, such as the threat actor and targeted industries. As a result, organizations can fine-tune their security policies and strategies to counter specific attacks and campaigns more effectively.

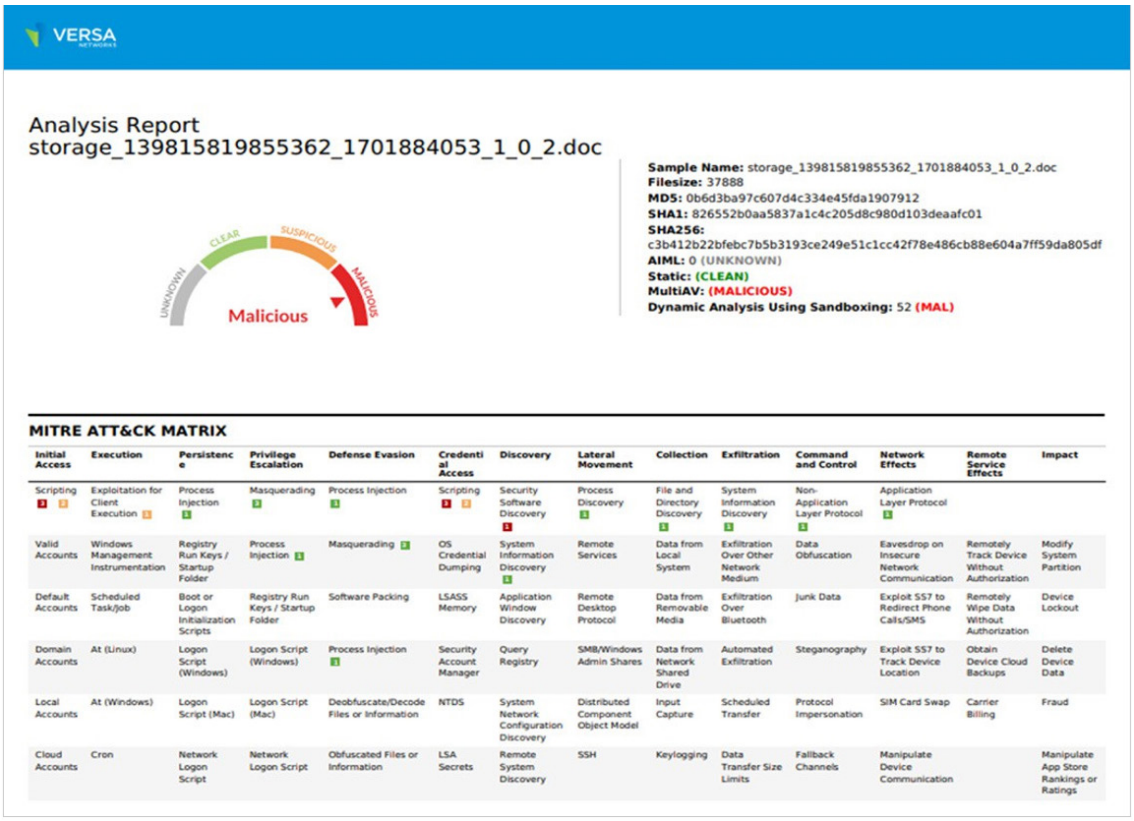

Fig. 4: Sandbox analysis report with MITRE Attack matrix for a file found to be malicious during dynamic analysis.

Real-time dashboard

Versa ATP provides a real-time dashboard that offers an at-a-glance view of the organization's security status, network traffic, and user activity, including intelligence gathered from the sandboxing system. This customizable dashboard enables security teams to focus on the most relevant information for their organization. Additionally, through real-time insights, the dashboard enables organizations to quickly identify and respond to potential security incidents before they escalate.

Traffic logs and reporting

Versa ATP includes a comprehensive traffic logging and reporting system that captures detailed information about network activity. These logs can be filtered and analyzed to identify patterns, trends, and anomalies indicating potential security threats. By closely monitoring network traffic, organizations can more effectively detect and respond to emerging threats.

Customizable reports

The Versa Unified SASE platform allows organizations to generate customized reports tailored to their needs, including reports on ATP findings. This flexibility enables security teams to focus on the most relevant data and insights, making it easier to identify trends, track progress, and measure the effectiveness of Versa ATP performance.

Role-based access control

To ensure that the right individuals have access to the appropriate level of information, Versa ATP supports role-based access control. This feature enables organizations to define user roles and assign appropriate access levels to various reports, dashboards, and analytics, ensuring that sensitive data is accessible only to authorized personnel.

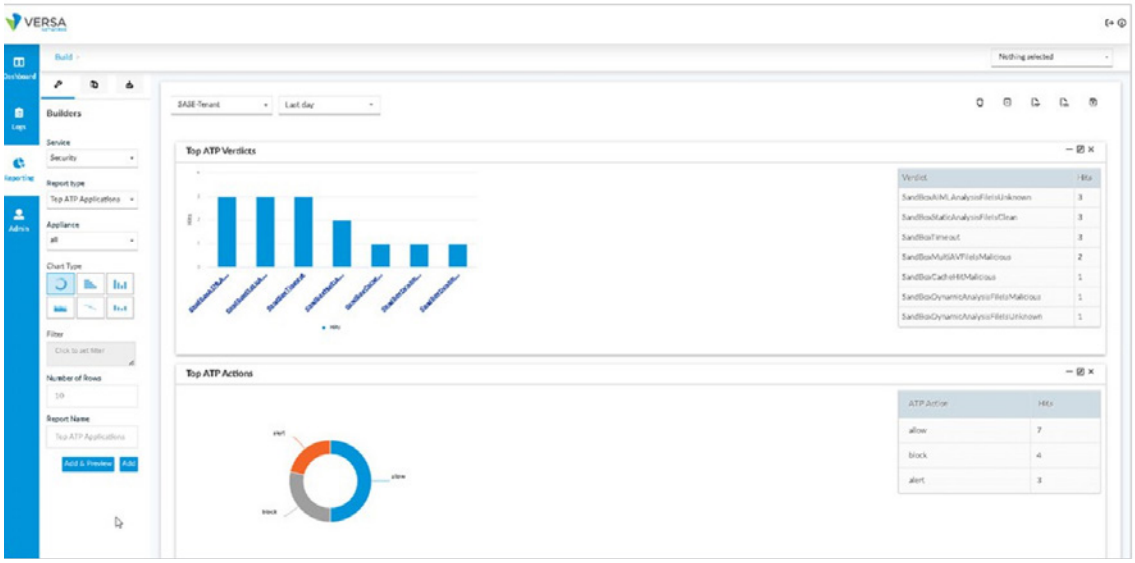

Fig. 5: Customizable report showing top ATP verdicts and actions taken (alerts, blocks, allows) for the chosen period.

Conclusion

Versa ATP delivers a robust, multi-layered set of advanced security features integrated into Versa's SSE and SASE platforms. Using AI/ML-powered detection, Versa ATP protects organizations against unknown attack vectors, emerging threats, and sophisticated deception techniques.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
Tel: +1 408.385.7660 | Email: info@versa-networks.com | Website: www.versa-networks.com