SOLUTION BRIEF

Versa Advanced Threat Protection

As cyber threats evolve, intensifying in both frequency and sophistication, it's clear that traditional security paradigms are falling short. This reality underscores businesses' need to proactively bolster their security posture with more advanced, agile, and intelligent security systems than ever before to defend against advanced threats such as zero-day exploits, advanced persistent threats (APTs), ransomware, and phishing attacks.

Why Versa Advanced Threat Protection?

Versa ATP is an intelligent blend of AI-driven file analytics and sandboxing that is a platform capability of Versa's unified SASE and SSE offerings. This combination creates a formidable security shield capable of thwarting many cyber threats, from phishing and exploit delivery to the more elusive zero-day malware attacks in the attack kill chain. By isolating and examining suspicious files in a safe, controlled environment, sandboxing reveals clandestine threats and, in turn, 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 is able to achieve an unrivaled depth of visibility and context regarding network traffic, user behavior, and security events, ensuring organizations are faster and more targeted in their response and allowing them to better make informed, proactive decisions to bolster their defenses.

As seen in Figure 1, Versa ATP works together with other components of Versa's full SSE security suite to provide a holistic security solution that protects your organization at every level, including: CASB, DLP, Secure Proxy, Remote Browser Isolation, IPS, Malware protection, IP reputation, URL filtering, App control, Denial of Service protection, and NGFW.

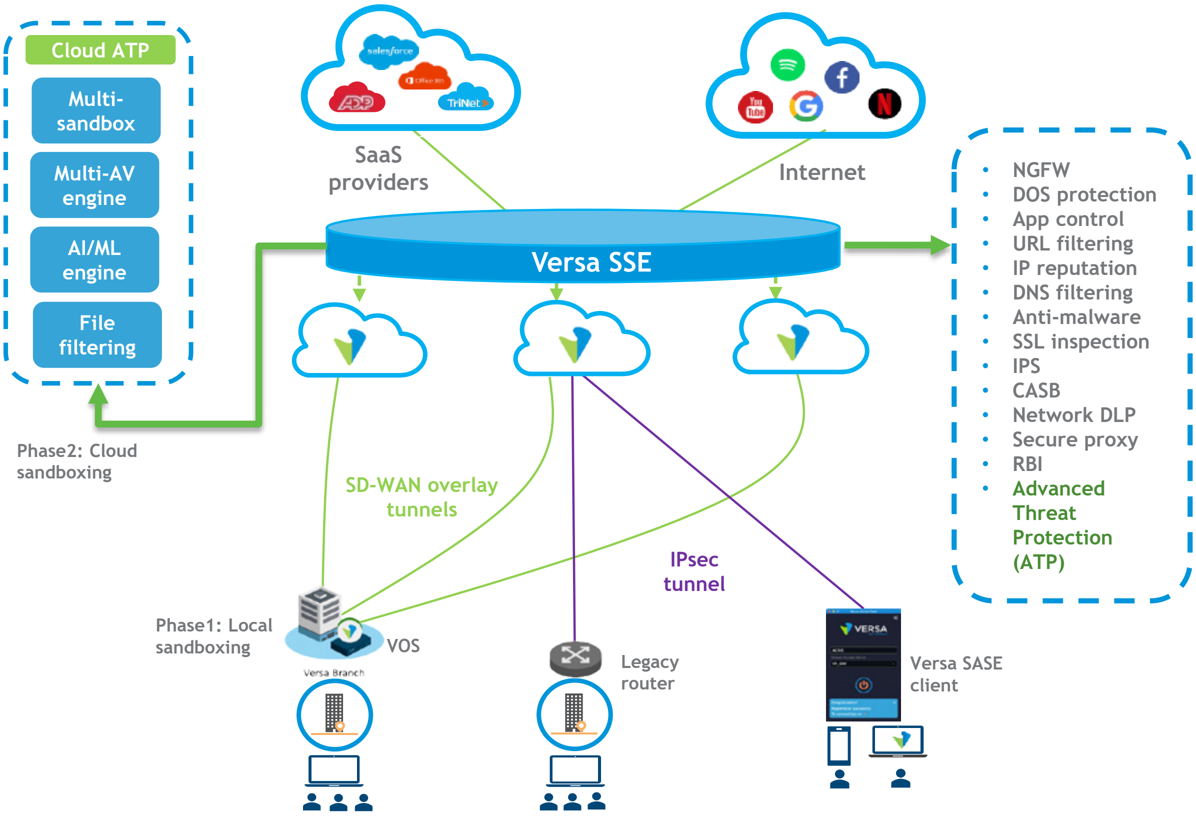


Fig. 1: Versa unified platform with Advanced Threat Protection capability

How It Works

Versa ATP works in two phases, with a local file analytics and sandboxing component, which performs preliminary analysis and evaluation of files, and cloud multi-sandboxing in a second phase for zero-day protection, both detailed below.

Local File Analytics and Sandboxing

Versa's local sandboxing inspects all files and performs file reputation lookup at the on-premises Versa Operating System (VOS) device, as shown in Figure 2 below. The local analysis capabilities described immediately below allow for potential risks and threats to be identified early in the process, benefiting organizations with faster threat detection and response times and include:

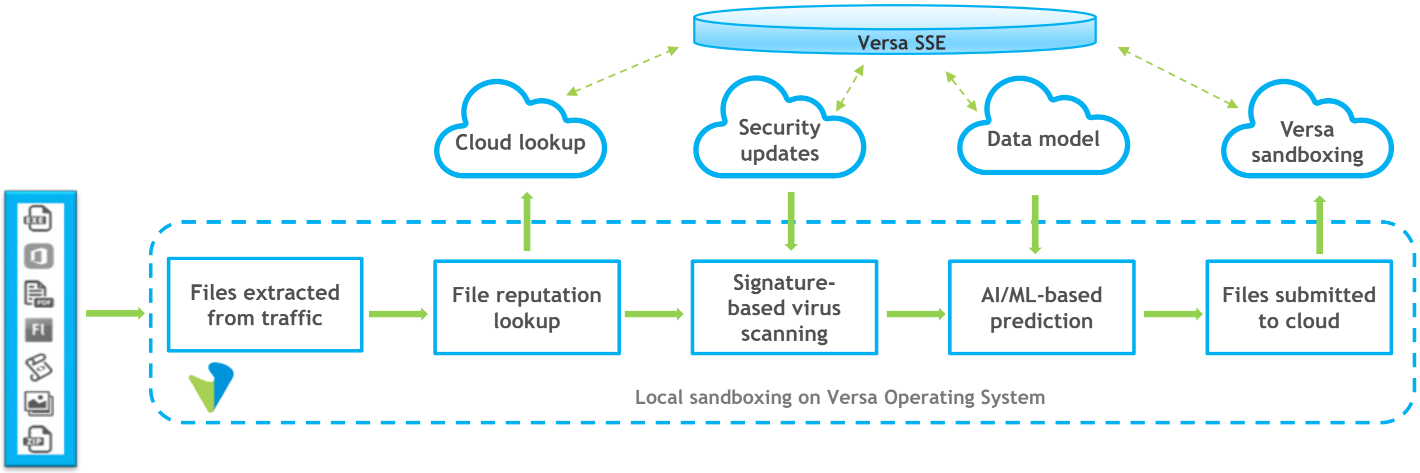


Fig. 2: Steps in the Versa file analysis process that are performed locally on the Versa Operating System

File reputation and signature analysis: Based on the file type, files are extracted from the traffic and reconstructed to compute an 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.

Static and AI/ML analysis: Versa ATP harnesses the power of AI and ML technologies to enhance its threat detection and response capabilities continuously. A lightweight AI/ML service runs locally on VOS that gets 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. In addition, a static analysis, including YARA rule processing, is also performed to immediately identify any Indicators of Compromise.

Multi-Sandboxing in the Versa Cloud

Following the local analysis steps, Versa's cloud sandboxing capability performs multi-layer analysis involving static and dynamic analysis and AI-based detection and identification using multiple AV engines. Suspicious files are sent to the Versa Cloud, where they are subjected to 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 capable of evading a single specific type of sandbox environment, providing a more robust defense against sophisticated attacks. Further component details include:

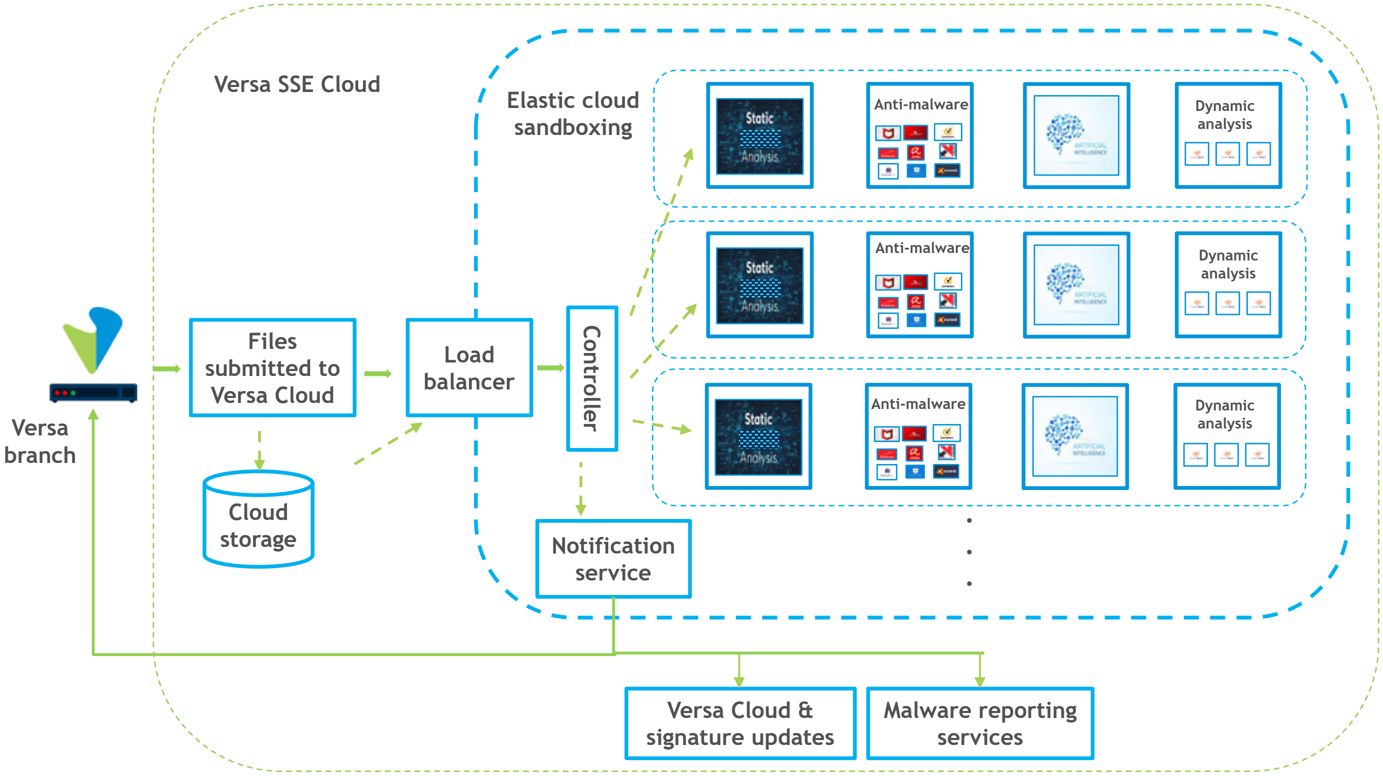


Fig. 3: Multi-sandboxing integrated into the Versa Cloud.

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.

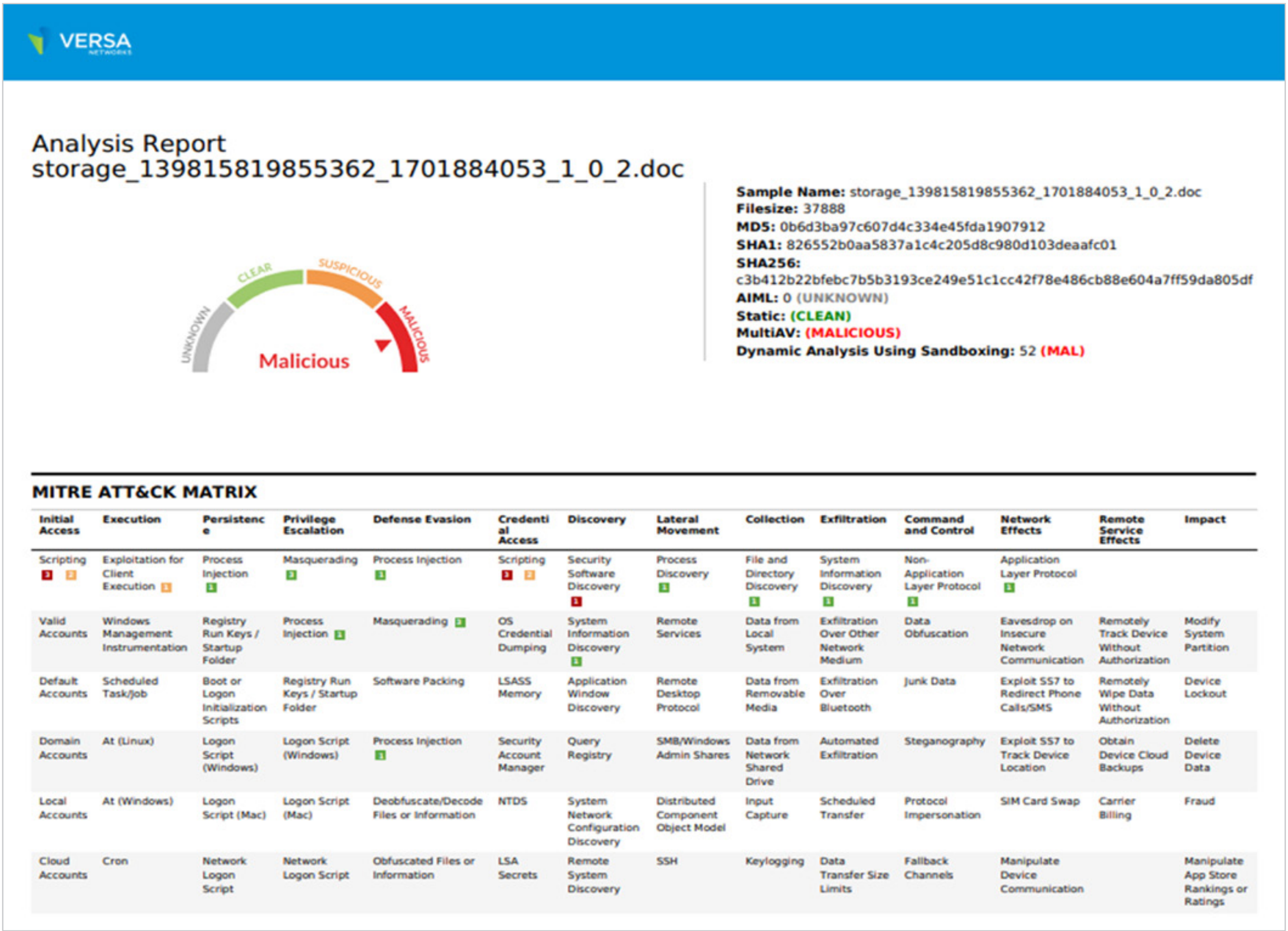
Static and AI/ML analysis: Versa ATP's AI and ML-driven threat detection and response capabilities are trained against a sample of eight billion files, making it very accurate and efficient in detecting threats. In addition, the data model constantly evolves as it analyzes new samples, providing fast 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, behavior analysis, and contextual awareness, the system can identify and respond to deception tactics, such as obfuscated code, polymorphic malware, and other evasive techniques 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. As a result, organizations can fine-tune their security policies and strategies to counter specific attack vectors more effectively by understanding the nature of the threats targeting their networks.



Analysis Report
storage_139815819855362_1701884053_1_0_2.doc

Sample Name: storage_139815819855362_1701884053_1_0_2.doc
Filesize: 37888
MD5: 0b6d3ba97c607d4c334e45fda1907912
SHA1: 826552b0aa5837a1c4c205d8c980d103deaafc01
SHA256:
c3b412b22bfebc7b5b3193ce249e51c1cc42f78e486cb88e604a7ff59da805df
AIML: 0 (UNKNOWN)
Static: (CLEAN)
MultiAV: (MALICIOUS)
Dynamic Analysis Using Sandboxing: 52 (MAL)

MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Scripting 3 2	Exploitation for Client Execution 1	Process Injection 1	Masquerading 3	Process Injection 1	Scripting 3 2	Security Software Discovery 1	Process Discovery 1	File and Directory Discovery 1	System Information Discovery 1	Non-Application Layer Protocol 1	Application Layer Protocol 1		
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Process Injection 1	Masquerading 1	OS Credential Dumping	System Information Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder	Software Packing	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Carrier Billing	Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

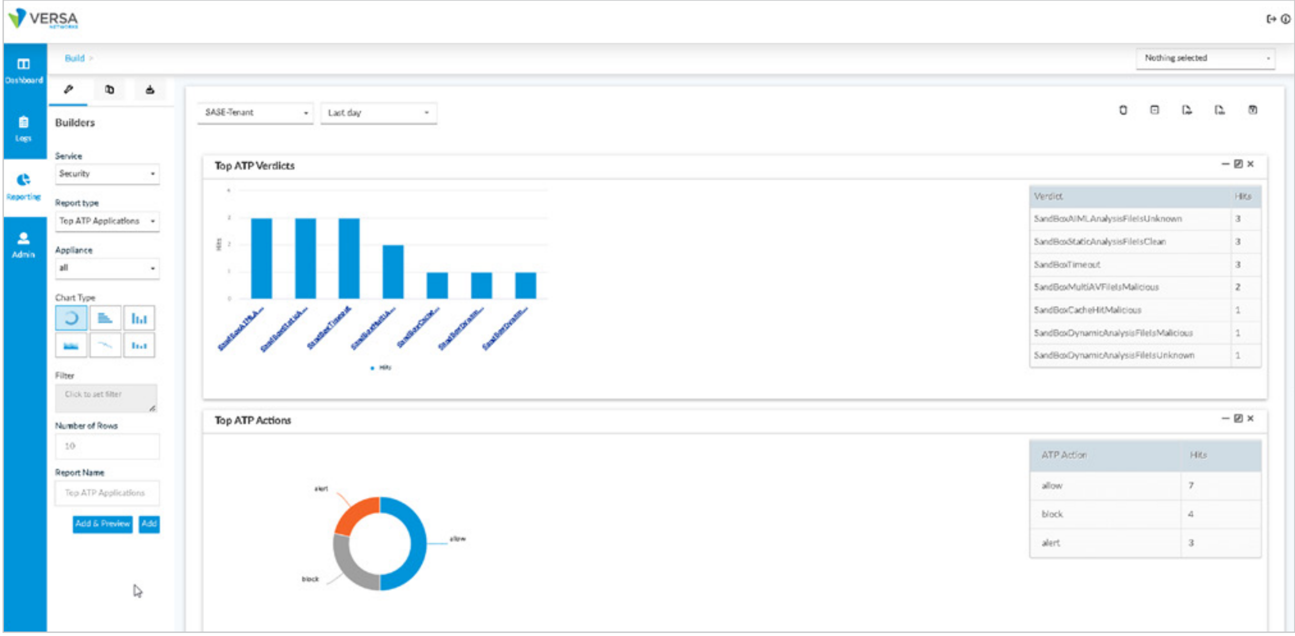
Fig. 4: Sandbox analysis report with Mitre Attack matrix for a file found to be malicious during dynamic analysis.

Real-time dashboard: Versa ATP offers a real-time dashboard that provides an at-a-glance view of the organization's security status, network traffic, and user activity, including intelligence gleaned from the sandboxing system. This customizable dashboard enables security teams to focus on the most relevant information for their organization. In addition, by providing real-time insights, the dashboard helps organizations 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 detect and respond to emerging threats more effectively.

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 different reports, dashboards, and analytics, ensuring that sensitive data is only accessible to authorized personnel.



Builders

Service: Security

Report type: Top ATP Applications

Appliance: all

Filter: Click to set filter

Number of Rows: 10

Report Name: Top ATP Applications

SASE-Tenant

Last day

Top ATP Verdicts

Verdict	Hits
SandBoxAIMLAnalysisFileIsUnknown	3
SandBoxStaticAnalysisFileIsClean	3
SandBoxTimeout	3
SandBoxMultiAVFileIsMalicious	2
SandBoxCacheHitMalicious	1
SandBoxDynamicAnalysisFileIsMalicious	1
SandBoxDynamicAnalysisFileIsUnknown	1

Top ATP Actions

ATP Action	Hits
allow	7
block	4
alert	3

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

Conclusion

Versa ATP provides organizations with a robust, multi-layered set of advanced features integrated into Versa's SSE and SASE platforms using AI/ML-powered detection to protect digital assets from unknown attack vectors, emerging advanced threats, and sophisticated deception techniques.

About Versa Networks

Versa Networks, the leader in single-vendor Unified SASE platforms, delivers AI/ML-powered SSE and SD-WAN solutions. The platform provides networking and security with true multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and Service Providers. Thousands of customers globally with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, BlackRock Inc., Liberty Global Ventures, Princeville Capital, RPS Ventures and Triangle Peak Partners. For more information, visit www.versa-networks.com or follow Versa Networks on X (Twitter) @versanetworks

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