

# Versa Advanced Threat Protection

## Introduction

Cyberattacks have become more advanced, employing complex techniques such as zero-day exploits, and ransomware. According to the Ponemon Institute, the global average cost of a breach continues to rise and nearly two thirds of business leaders felt their cybersecurity risks had increased. The number of cyberattacks is rising, posing significant risks to organizations' financial and reputational standing. With the rise of remote work and digital transformation, organizations are more exposed to these threats. Traditional security measures are no longer sufficient to protect against such sophisticated attacks. Therefore, adopting a comprehensive and adaptive security solution like Versa Advanced Threat Protection (ATP) is crucial. Versa ATP is designed to protect organizations from these advanced threats by integrating cutting-edge technologies and a multi-layered defense strategy, ensuring protection across on-premises, cloud, and hybrid environments.

## The Versa Approach

### Comprehensive Best-of-Breed Approach

Versa ATP leverages multiple antivirus, malware, and advanced threat detection engines, creating a formidable defense against cyber threats. Unlike approaches that limit users to proprietary solutions, Versa ATP's open approach allows for the integration of certified threat intelligence and ATP engines, giving organizations unparalleled flexibility and effectiveness in their security architecture.

### Diverse Approaches and Broad Threat Coverage

By utilizing a blend of static and dynamic analysis tools like VirusTotal, Yara rules, and AI/ML-based detection, Versa ATP provides extensive threat coverage. This multifaceted approach ensures that threats are scrutinized from every angle, leaving no stone unturned in the quest for cybersecurity.

### Superior Scalability

Versa ATP's hybrid architecture, backed by a cloud-native sandbox can scale with your business. This provides an alternative to solutions that have limits on detonations and load-balanced instances. Versa ATP scales effortlessly to handle much larger volumes and broader coverage, ensuring that as your organization grows, your security measures grow with it.

### Flexible and Hybrid Architecture

Versa ATP delivers security services across on-premises, cloud, hybrid, and private environments with ease. This flexibility ensures that organizations can maintain robust protection regardless of how their infrastructure evolves, supporting a hybrid workforce and dynamic business environments.

### AI/ML-Powered Detection

Versa ATP's AI/ML Engine leverages artificial intelligence and machine learning to analyze vast amounts of data, recognize threat patterns, and adapt to new threats. This capability allows Versa ATP to not only identify zero-day malware but also predict and mitigate emerging threats, staying one step ahead of cyber adversaries.

### Comprehensive Threat Protection for both Known and Unknown Threats

Versa ATP offers extensive threat protection, capable of detecting both known and unknown threats through a range of techniques, including IP/URL/DNS/File Filtering and Anti-Virus. This comprehensive approach ensures that your organization is protected from the full spectrum of cyber threats, safeguarding your most valuable assets.

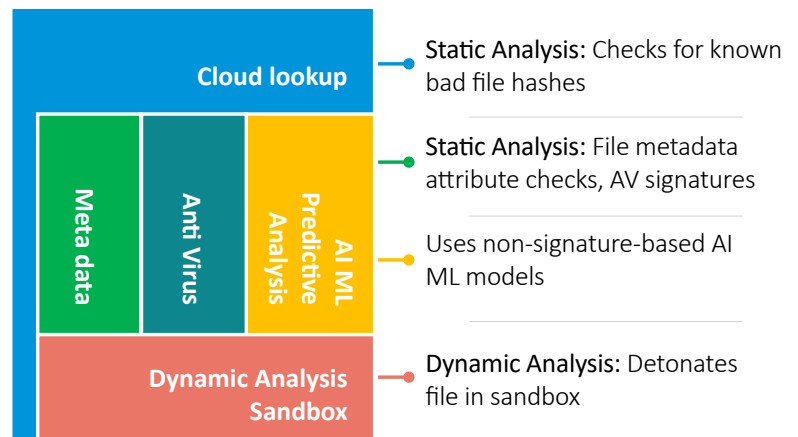
## What is Versa Advanced Threat Protection (ATP)?

Versa ATP is a comprehensive security solution aimed at defending organizations against sophisticated malware-based threats that conventional security measures often miss. It integrates a multi-layered approach to tackle both known and unknown threats, providing enhanced efficacy and enabling scalability across on-premises, cloud, and hybrid environments. Versa ATP's key components include:

### Key Modules of Versa ATP

#### Multi-AV Engine

Versa ATP leverages multiple antivirus engines to conduct thorough file scanning, ensuring comprehensive protection against a wide range of malware. This engine analyzes various file types such as executable files (EXE), Object Linking and Embedding (OLE) files, Word documents, PowerPoint presentations (PPTX), PDFs, and JavaScript. By leveraging multiple antivirus engines, Versa ATP enhances the detection and prevention capabilities, offering a robust defense against known malware threats.



#### Cloud Lookup Engine

Versa ATP's Cloud Lookup Engine enhances real-time threat identification. It utilizes Yara signatures along with a combination of third-party and in-house threat intelligence feeds to detect malicious files effectively. This engine performs real-time cloud lookups to rapidly identify threats, providing organizations with timely and accurate threat information. By leveraging the cloud, this engine ensures that threat intelligence is always up-to-date and comprehensive.

#### Metadata Analysis Engine

Versa ATP's Metadata Analysis Engine conducts static analysis by examining file attributes without executing the file. This engine checks file hashes, digital signatures, packer information, and various metadata attributes, such as Portable Executable (PE) structure and Exchangeable image file format (Exif) attributes. By analyzing these metadata attributes, the engine can identify potentially malicious files based on their characteristics, adding an extra layer of scrutiny.

#### Dynamic Analysis Engine

The Dynamic Analysis Engine, composed of a multi-sandbox architecture, performs dynamic analysis by executing files in a sandbox environment to observe their behavior. This engine utilizes multiple sandbox environments to enhance the effectiveness of threat detection. It supports major operating systems, including Windows, Android, OS X, and Linux, ensuring broad coverage across different platforms. By observing file behavior in a controlled environment, this engine can detect and mitigate threats that might not be identified through static analysis alone.

#### AI/ML Engine

The AI/ML Engine in Versa ATP leverages artificial intelligence and machine learning for advanced behavior analysis. This engine classifies files based on their behavior, enabling the identification of zero-day malware as malicious. Through predictive analysis, the AI/ML Engine anticipates and mitigates emerging threats, providing a proactive approach to threat detection. By continuously learning from vast amounts of data, this engine enhances the overall efficacy of Versa ATP in detecting and responding to advanced threats.

## Features

### Advanced Threat Prevention - cloud delivered

- Zero-day protection against unknown threats, zero-day vulnerabilities, ransomware, polymorphic threats
- Static or metadata analysis analyzing file attributes, file hashes, Yara signatures
- Support for multiple malware, anti-virus engines
- AI/ML based engine for predictive, non-signature-based detection
- Dynamic analysis - sandbox for file detonation and execution
- Extensive file type support (office set, executables, PDF and many more)
- Support for commonly used client operating systems (Windows, MacOS, Linux)
- Email notifications

## Conclusion

Versa Advanced Threat Protection (ATP) is a dynamic, adaptable, and comprehensive defense system designed to protect organizations in an increasingly hostile cyber environment. By integrating multiple advanced technologies and adopting a comprehensive multi-layered defense approach, Versa ATP enables businesses to stay ahead of evolving threats.

For more information on Versa Advanced Threat Protection and how it can enhance your organization's security posture, visit [Versa Networks](#).