SOLUTION BRIEF

Comprehensive Next Generation Endpoint Protection with Digital Defense Frontline Active Threat Sweep™ (Frontline ATS™) and Microsoft Defender Advanced Threat Protection (ATP)™

Enhance Protection Of Your Critical Assets By Adding Agentless Threat Assessment Across Hybrid Cloud Environments.

BUSINESS PROBLEM

For years, attackers have successfully exploited different types of vulnerabilities, compromised systems and used advanced tactics for breaching networks by targeting endpoints. They take advantage of infrastructure blind spots, un-patched devices and overwhelming alerts, making it impossible for security teams to identify attack campaigns and prioritize investigations and remediation efforts. Even with anti-virus installed, without today's advanced endpoint tools like Endpoint Detection and Response (EDR) with associated agents, it can be extraordinarily difficult for organizations without experienced security teams to identify infected assets. In addition, new assets will be left unprotected in many cases until an agent can be installed and active threat monitoring can begin.

Identifying under-attack assets in real-time and automating response capabilities enables security teams to go on the offensive for preventing a successful breach. Even better, security teams can eliminate all the noise from traditional threat detection methods including false positive alert fatigue when time is of the essence in the race against attackers.

FRONTLINE.CLOUD AND FRONTLINE ATS™

Frontline Active Threat Sweep™ (Frontline ATS™) is part of the Digital Defense Frontline.Cloud platform that is purpose-built to be deployed and operate in today's multi-tenant hybrid cloud enterprise environments that require a real-time approach to understanding risks and threats for effective remediation. Frontline ATS provides on-demand agentless threat detection to pro-actively analyze assets for indications of a malware infection before other agent-based security tools can be deployed.

With Frontline ATS, you can also pinpoint assets with out-of-date or disabled endpoint protections to quickly flag at risk devices and prioritize investigation and remediation. Frontline ATS enumerates running processes and persistent auto-run code to verify trusted publisher signatures, compare information to cloud anti-virus and compromised feeds. In addition, know with certainty which hosts have been compromised and identify breaks in static protection software deployments.

WHAT FRONTLINE OFFERS:

COVERAGE

- Provides comprehensive view of the network
- Identify most modern antivirus products
- Check persistent and running code on Windows machines against known malware signatures
- Spot outliers and anomalies on network shares for lateral movement

SCALABILITY

- On demand SaaS system sweeps entire network for threats
- Lightweight scanning footprint minimizes network impact
- Agent-less technology for less maintenance overhead
- Customizable role-based user access control
- Flexible deployment: service enabling device available as physical hardware, virtual or cloud appliance

REPORTING

- Built-in trending and analysis
- Advanced filtering and data segmentation capabilities
- PDF and CSV based reporting formats overhead

MICROSOFT DEFENDER ATP

Microsoft Defender Advanced Threat Protection is a unified endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Using the following combination of technology built into Windows 10 and Microsoft's robust cloud service.

Endpoint behavioral sensors: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Microsoft Defender ATP.

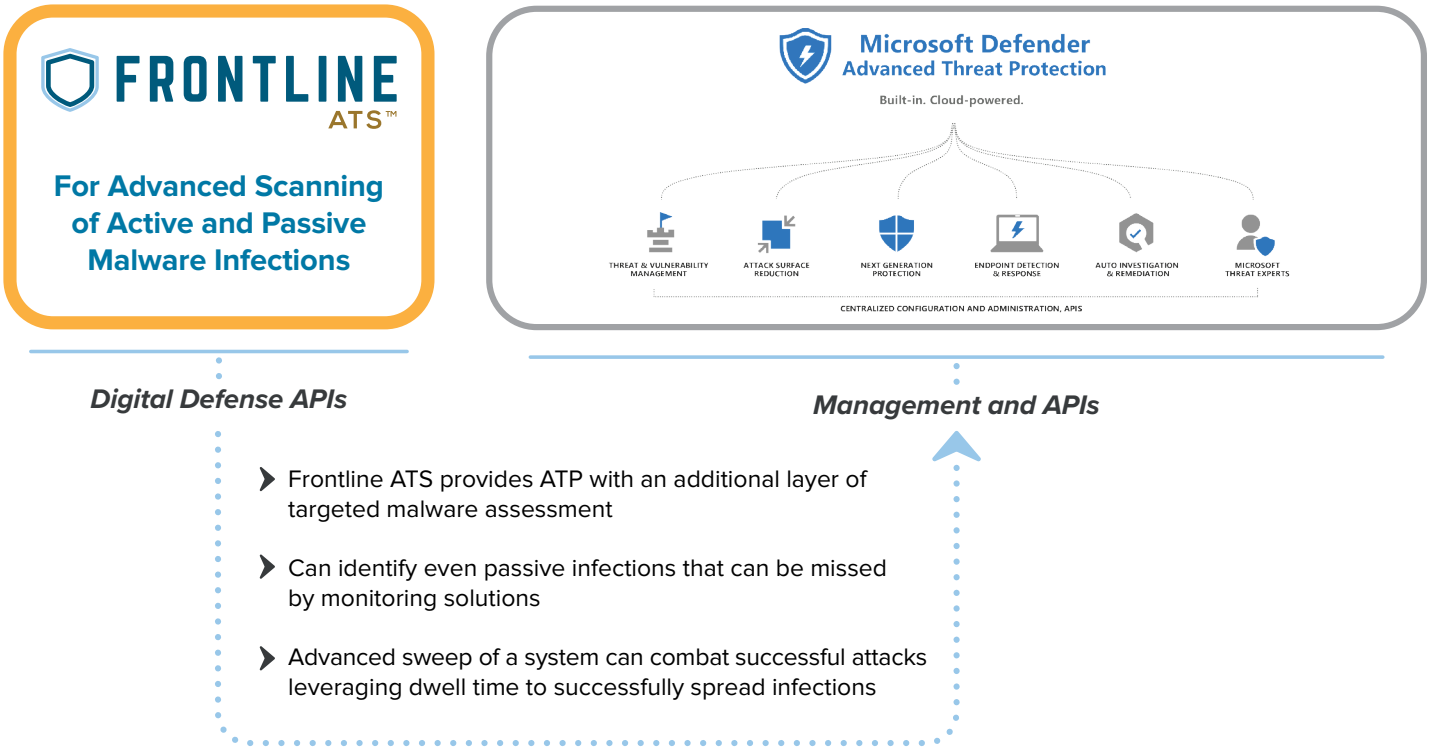
Cloud security analytics: Leveraging big-data, machine-learning, and unique Microsoft optics into signals and threats across domains including endpoints, email, and identities, behavioral signals are translated into insights, detections, and automated responses to advanced threats.

Threat intelligence: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Microsoft Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.

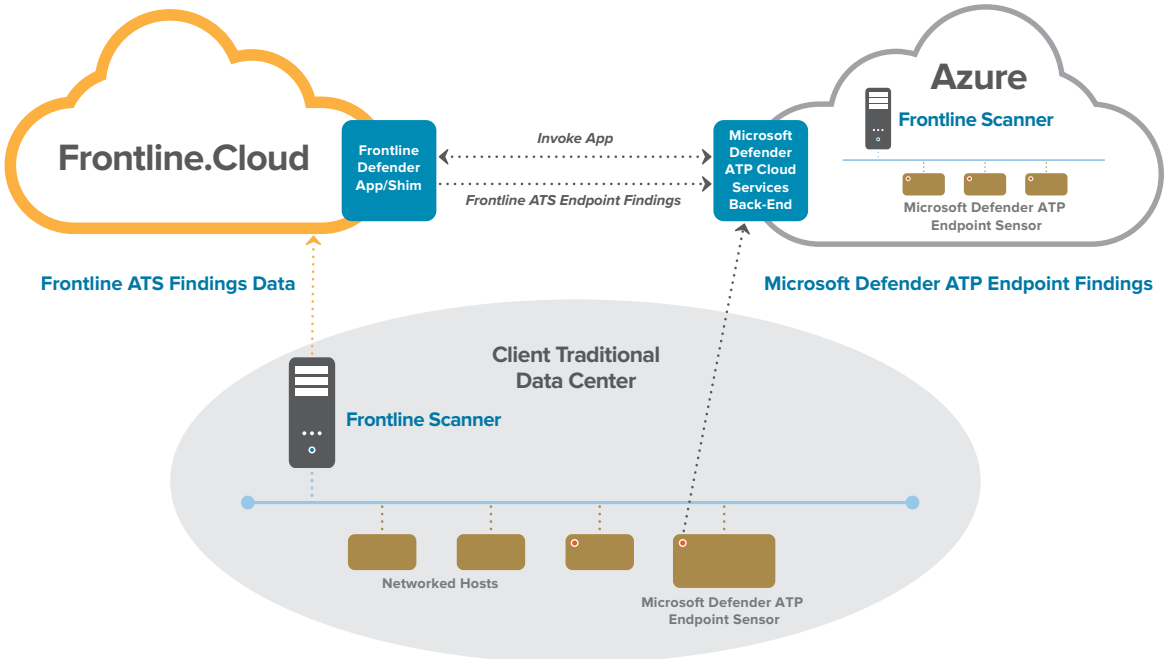
SOLUTION SUMMARY

Digital Defense's Frontline ATS, integrated with Microsoft Defender ATP puts the power of on-demand agent-less threat detection at your fingertips. Proactively analyze assets for indications of a malware infection before other agent-based security tools can be deployed and thwart attacks that take advantage of dwell time to evade endpoint monitoring. Identify out-of-date or disabled endpoint protections to quickly flag at-risk devices and prioritize investigation and remediation. The combined solution increases Microsoft Defender ATP's already proven security coverage and efficacy beyond current endpoint detection and response solutions.

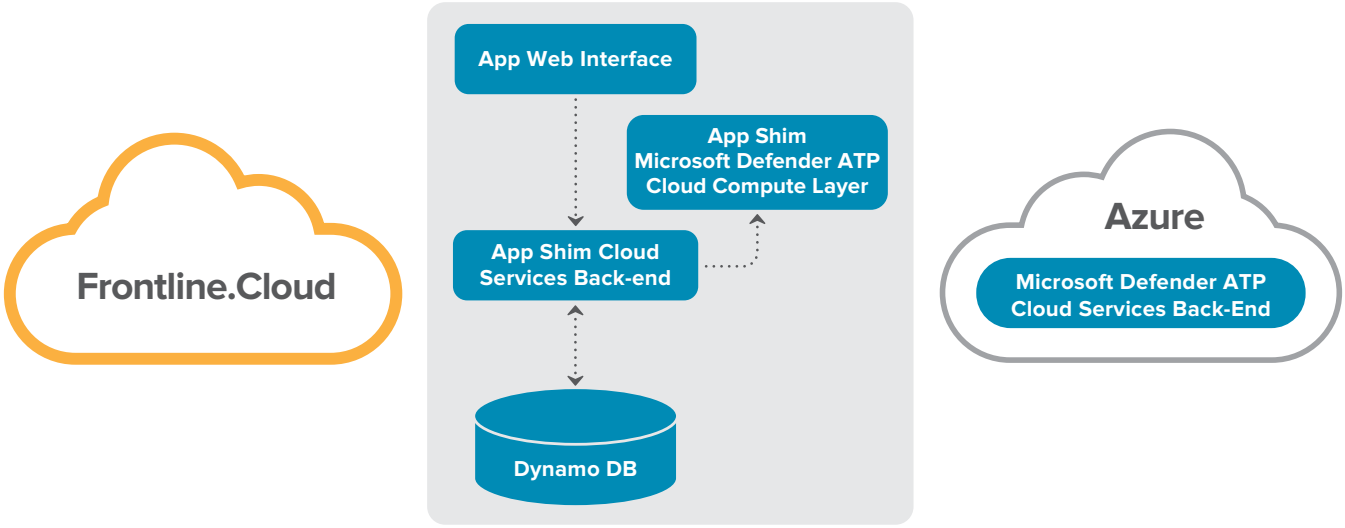
DIGITAL DEFENSE FRONTLINE ATS AND MICROSOFT DEFENDER ATP: A COMPREHENSIVE ENDPOINT PROTECTION SUITE



FRONTLINE ATS - MICROSOFT DEFENDER ATP INTEGRATION



APPLICATION SHIM DETAILED DESIGN



SOLUTION BENEFITS

- Better visibility and early detection of both passive and active threats
- Enhanced threat detection by combining targeted active threat scanning with AI-based Behavioral Anomaly Detection, Malware Signature and File Analysis
- Ability to root out small passive attack artifacts that are extremely difficult to find and planted by attackers for infecting or even re-infecting assets
- Immediately clean up infections before patching efforts can be implemented

TO LEARN MORE ABOUT HOW DIGITAL DEFENSE AND MICROSOFT CAN OFFER BETTER ENDPOINT PROTECTION:

Contact us at:
sales@digitaldefense.com

For more information visit:
www.DigitalDefense.com

About Digital Defense

Founded in 1999, Digital Defense, Inc. is an industry recognized provider of security assessment solutions. Digital Defense provides vulnerability and threat assessment Software-as-a-Service (SaaS) solutions and services purpose-built to operate in today's hybrid cloud enterprise environments. Digital Defense's proprietary platform, Frontline.Cloud, incorporates patented technologies and offers multiple software security systems focused on pro-actively hardening business critical assets from being compromised and breached. The Frontline.Cloud platform supports Frontline Vulnerability Manager™ (Frontline VM™), Frontline Web Application Scanning™ (Frontline WAS™), and Frontline Active Threat Sweep™ (Frontline ATS™) that provide agent-less discovery, vulnerability and threat assessment of dynamic assets, while eliminating manual processes and integrating with market-leading 3rd party security and IT offerings to eliminate gaps in visibility and enable faster remediation. Frontline.Cloud is the only solution in the market that is built to be scaled across any size organization and operate on premise, in the cloud or in hybrid network-based implementations.

About Microsoft

Microsoft Corporation is a technology company. The Company develops, licenses, and supports a range of software products, services and devices. The Company's segments include Productivity and Business Processes, Intelligent Cloud and More Personal Computing. The Company's products include operating systems; cross-device productivity applications; server applications; business solution applications; desktop and server management tools; software development tools; video games, and training and certification of computer system integrators and developers. It also designs, manufactures, and sells devices, including personal computers (PCs), tablets, gaming and entertainment consoles, phones, other intelligent devices, and related accessories, that integrate with its cloudbased offerings. It offers an array of services, including cloud-based solutions that provide customers with software, services, platforms, and content, and it provides solution support and consulting services.