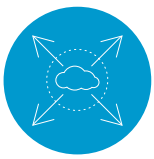
4 REASONS GOVERNMENT SECURITY TEAMS SHOULD CHOOSE CLOUD-BASED MALWARE ANALYSIS OVER LEGACY APPROACHES

For many federal agencies, using cloud services is no longer an "if" but a "when." As cloud adoption use cases in the context of public sector continue to evolve in 2019, using the cloud to protect federal agencies from the ever-increasing threat of state-sponsored adversaries, cybercriminals, and data breaches remains a compelling use case. Today, a large number of federal IT security teams are looking at the value of using cloud services to ensure their mission-serving systems remain protected. That said, a cloud-based malware analysis and prevention engine built into your next-generation firewall framework, sensors, and enforcement points is a critical "must-have" to move beyond traditional approaches in analyzing and preventing malware.

Here are four primary reasons why a cloud-based malware analysis and prevention service is the right choice for your federal agency.



1. Scales with the Increasing Volume of Files and Malicious Code Targeting Government Customer Networks

Thousands of new malware samples are generated every day on average. As the volume of malicious code continues to grow, analyzing and effectively deploying a prevention posture using standard, localized approaches becomes practically impossible. In some cases, state-sponsored adversaries intentionally choose specific times of day to deliver malicious payloads, knowing they can potentially bypass local network malware analysis and prevention systems that are overloaded with analysis of benign data downloaded by an agency's users. A cloud-based malware analysis and prevention service needs to employ a purpose-built virtual sandbox environment that elastically meets utilization requirements and delivers prevention to all enforcement points for high-fidelity, evasion-resistant discovery of unknown threats.

Cloud scale is a necessity when it comes to analyzing highly evasive unknown exploits and malware throughout a diverse series of network locations, across all traffic within your agency's ingress/egress points—network, endpoints, web, email, file sharing protocols, and more. A cloud-based virtualized sandbox environment leverages global threat intelligence data from files submitted via both the private and public sector to automatically create, deliver, and enforce prevention controls without requiring a manual response. Legacy approaches, on the other hand, are fraught with limitations when it comes to analyzing and automating prevention of unknown threats at scale.

2. Leverages Collective Threat Intelligence to Reduce the Number of Truly Unknown Threats

Whether state-sponsored adversaries or commercially motivated cybercriminals determined to steal your agency's intellectual property, adversaries circumvent legacy detection approaches by targeting multiple agencies and departments to maximize the odds of success. Legacy approaches isolate threat data each organization receives and generates, creating silos and reducing the possibility of preventing previously identified threats. Addressing the rise and frequency of threats requires a shift in mindset. Newly uncovered threats must immediately be communicated to all enforcement points across the public, private, and government sectors in near-real time.

With a cloud-delivered malware analysis service, you can leverage collective real-time threat intelligence and prevention from a globally distributed sensor network that delivers malware analysis and protections to tens of thousands of customer subscribers globally. Tapping into the shared protections from a global community of subscribers not only provides collective immunity but also saves your security team valuable time by analyzing unknown threats unique to your environment from the outset.

3. Provides Limitless Scope to Leverage Advanced Machine Learning and Analysis Techniques for Faster Threat Detection and Prevention

The elastic nature of the cloud provides limitless scope for deploying effective machine learning and analysis techniques into the malware analysis service. Machine learning extracts thousands of unique features from files submitted to the malware analysis engine, evaluates them against a predictive model to determine maliciousness, and as a result, uncovers threats that don't match known indicators of compromise.

When fending off the automated techniques used by cybercriminals today, security analysts cannot depend on manual analysis and standard detection methods alone. Instead, they must rely on automation combined with machine learning, dynamic analysis occurring across multiple virtual operating systems, and static analysis that is only possible at cloud scale. By utilizing advanced machine learning techniques available natively in a cloud-delivered malware analysis service, defenders can avoid risks caused by manual errors and analyze unique threats more quickly.

4. Optimizes Security Operations to Free Up Human Resources and Capital

A cloud-based virtual malware analysis service supports automated orchestration that rapidly updates your agency's network, endpoint, and cloud enforcement points with protections that prevent the latest threats within seconds or minutes, not hours or days.

The automation aspect of a cloud-based malware analysis eliminates the need for human intervention. As a result, your agency security teams are free to focus on areas that matter more to the organization. Optimizing security operations with cloud-enabled automation also frees up capital and operational expenses previously required to purchase and maintain on-premises threat detection and analysis hardware. With a cloud-based malware detection service, you simply enable your subscription and leave behind the worry of a cumbersome hardware installation.

Palo Alto Networks has received FedRAMP Moderate Authorization from the General Services Agency (GSA) for WildFire®, our cloud-based malware analysis and prevention service. WildFire: U.S. Government is the first and only cloud-based cyberthreat analysis service authorized for use by the U.S. government. Using this purpose-built instance for the U.S. federal government, federal agencies can leverage the power of the cloud to automatically detect and stop unknown attacks.

GET A COPY OF WILDFIRE: U.S. GOVERNMENT AT-A-GLANCE