Preventing the Unknown With WildFire

The Industry's Largest Malware Analysis Solution

Table of Contents

1. Executive Summary 3
2. The Attacker's Advantage 4
3. Why Traditional Solutions Can't Keep Up..... 5
4. Stop Advanced Attacks Using WildFire 6

Executive Summary

In recent years we have seen cybercrime levels double due to several factors including the adoption of hybrid work, the shift to Cloud, and rapid growth in the use of IoT and SaaS applications. The combination of these events has led to an expanded attack surface, creating the perfect environment for organizations to be exploited by malicious actors - as seen recently with the largest amount of zero-day exploits in a single year.

Advanced evasion techniques such as packing, encryption, and the use of fileless or memory-only malware, have also added complexity in detecting new and sophisticated malware. With these various methods of obfuscation, traditional file analysis solutions using AV scanning are unable to analyze many of today's threats.

The WildFire malware analysis service has assisted many customers in securing their organizations as they move towards cloud adoption and a Zero Trust architecture. These organizations are using WildFire's advanced analysis capabilities to stay ahead of the latest attack techniques with automated malware prevention using threat intelligence from a global community of 85,000 customers. This enables up to 95% prevention of file-based threats, turning detections into preventions 180x faster than the nearest competitor.

92.7%

Increase in reported cyber attacks[1]

2x

Increase in zero-day exploits year over year[2]

6,397

Files not seen by any other vendor in the industry[3].

[1]Source: Security Magazine "Ransomware attacks nearly doubled in 2021"
[2]Source: Mandiant "Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before"
[3]Source: Palo Alto Networks WildFire Engineering Team (Jan - Jun 2022)

Recognizing Advantages that Attackers Have

The first advantage is **speed**. Adversaries are leveraging cloud scale, personalization, and professional techniques to drive the spread of malware.

With the emergence of Ransomware-as-a-Service offerings, ransomware accessibility and reach is expanded. Malicious actors can now deploy a ransomeware campaign within minutes without having much technical expertise[4].

The second advantage is **polymorphism**. Using machine-learning and automation to constantly change and mutate attacks, adversaries can evade detection. Many attacks are variations of a basic attack, with changes to domains or techniques allowing them to look like new attacks, thus avoiding static signature protections.

Today's Threat Capabilities

330K new malware types per day, more than 1K every 5 minutes.

In **5 minutes** today's malware can spread to over 9K endpoints and encrypt 373 MB per second.

Ransomware starts encrypting file types that are most likely to contain **sensitive** or **business data first**.

Hybrid infrustructure, IoT and Cloud have **increased the attack surface**. Attackers have more opportunities to get into your network and exfiltrate data.

[4] Source: https://blog.emsisoft.com/en/29220/ransomware-as-a-service/

Limitations of Today's Conventional File Analysis Solutions

Traditional sandboxing solutions struggle to keep pace with the changing threat landscape due to inefficient detection methods. Coupled with a lack of a global presence and cloud scale, these solutions have limited innovations they can build. Many of these solutions were also built with endpoint integration focus and lack comprehensive protection across the enterprise.

1 Dynamic Analysis

The ever-evolving polymorphic attacks of today use advanced evasion capabilities such as packing, encryption, and memory-only methods to avoid detection. Dynamic analysis alone is not enough to detect these new types of sophisticated malware. In addition, dynamic analysis takes an average of 5-7 minutes per file to complete.

2 On-premises Deployments

In today's highly-distributed enterprise, the physical box approach becomes difficult to scale and costly. Standard on-premises solutions are cumbersome to deploy because they require complex traffic redirection. With multiple sites and remote working locations, the infrastructure must be duplicated repetitively and could require additional VPN routing. In addition, detection updates take months to deploy, creating opportunities for malicious actors to infiltrate your network.

3 Limited Visibility

On-premises solutions are unable to determine the global prevalence of an attack due to not having visibility of threats outside of an organization's network. This leads to not seeing all malware samples associated with a current campaign and missed indicators of compromise (IOC). Cloud-based solutions may also fall victim to this if they are not ingesting malware samples from various industries, locations, and threat vectors. Missing these IOCs cause an increase in missed detections.

4 Hash-Based Signatures

Hash-based signatures require a 1-to-1 match, limiting the ability for threat signatures to provide protections against polymorphed variants. These large datasets require time to sort through all hashes to find an associated campaign. Plus, updates are typically provided every 4-6 hours, leaving a large window of opportunity for malicious actors to infiltrate an organization's network. Today's landscape requires near real time updates.

Detection to Prevention Stopping Attacks Using WildFire

As threats grow more sophisticated and evasive, it is critical that security solutions continue to innovate. Organizations need a solution that can integrate with the whole security ecosystem, is self maintaining, and offers a wide range of detection techniques.

WildFire: Stop Malware in its Tracks with the Industry's Largest, Most Integrated Malware Prevention Solution

Palo Alto Networks' WildFire cloud-based malware analysis service is the industry's most advanced analysis and prevention engine for highly evasive zero-day malware, delivering signatures 180x faster than the nearest competitor.

The WildFire service employs a unique multi-technique approach, combining dynamic and static analysis and innovative machine learning techniques, to detect and prevent even the most evasive threats. The cloud-based architecture of WildFire supports unknown threat analysis and prevention at massive scale across an organization's network, endpoints, and cloud.

Stop Known, Unknown, and Zero-day Threats

Prevents up to 95% of new file-based threats inline; Turns unknown threats into prevention 180x faster

Worldwide Presence

Industry-leading 10 points-of-presence in major worldwide locations to comply with local data regulations

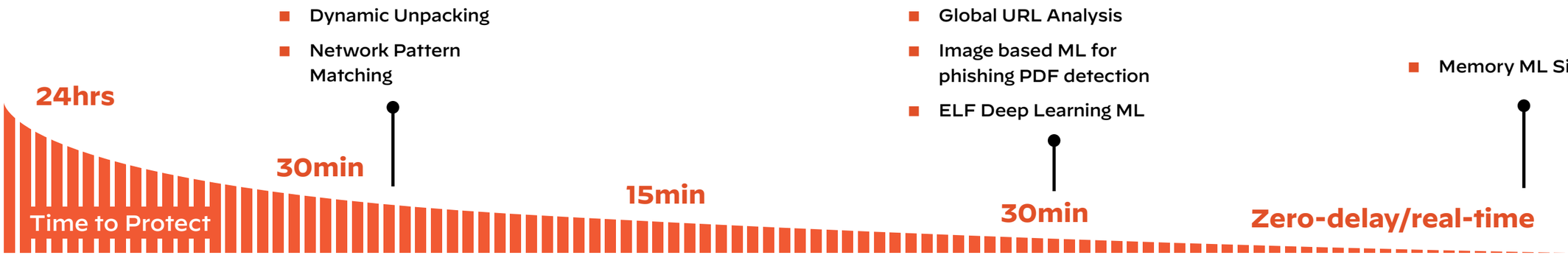
Integrated across Network, Endpoint, SaaS, IaaS

Leverages a global network of 85K+ customers with millions of sensors across SaaS, IaaS, Endpoint, Network and 3rd-party partners

11 Years of Innovation: Stopping Known, Unknown, and Zero-Day Threats

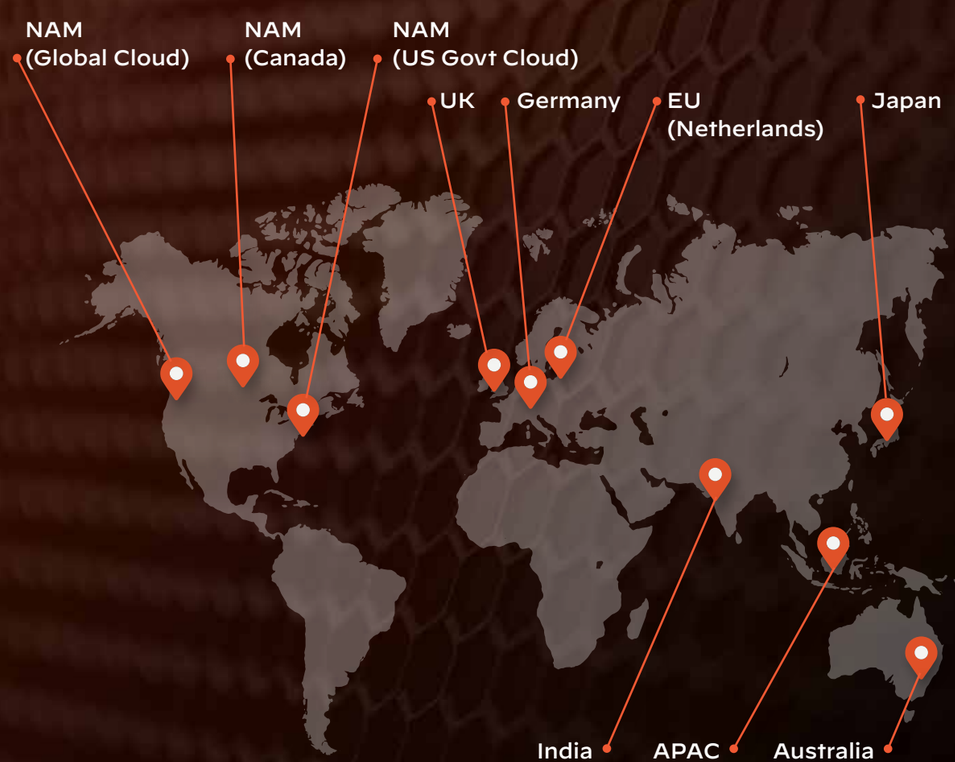
WildFire launched in 2011 supporting just five file types and delivering signature updates every 24 hours. As of 2022, WildFire supports over 70 different file types and delivers signature updates immediately.

As the threat landscape has evolved, WildFire has developed new techniques to detect malicious files as fast as possible with the highest of accuracy. WildFire has 27 patents based on innovations in detection methods, with over 12 different machine learning models running in production and five that run inline on the NGFW.



Data Residency

WildFire has **10 regional clouds**. This enables our customers to select a location that best fits their needs. Every year we continue to add more locations.



Worldwide Presence with Added Privacy by Design

Compliance Certfications

As WildFire evolves to analyze threats in new regions and from new enforcement points, it aims to meet or exceed the compliance certification obligations of customers. Data that does not aid in the analysis of a submission is either not collected or is destroyed after analysis. Benign submissions are automatically deleted, and customers are able to delete submitted files.

https://www.paloaltonetworks.com/legal-notices/trust-center/tech-certs

Integrated Security for Protection Across Your Organization

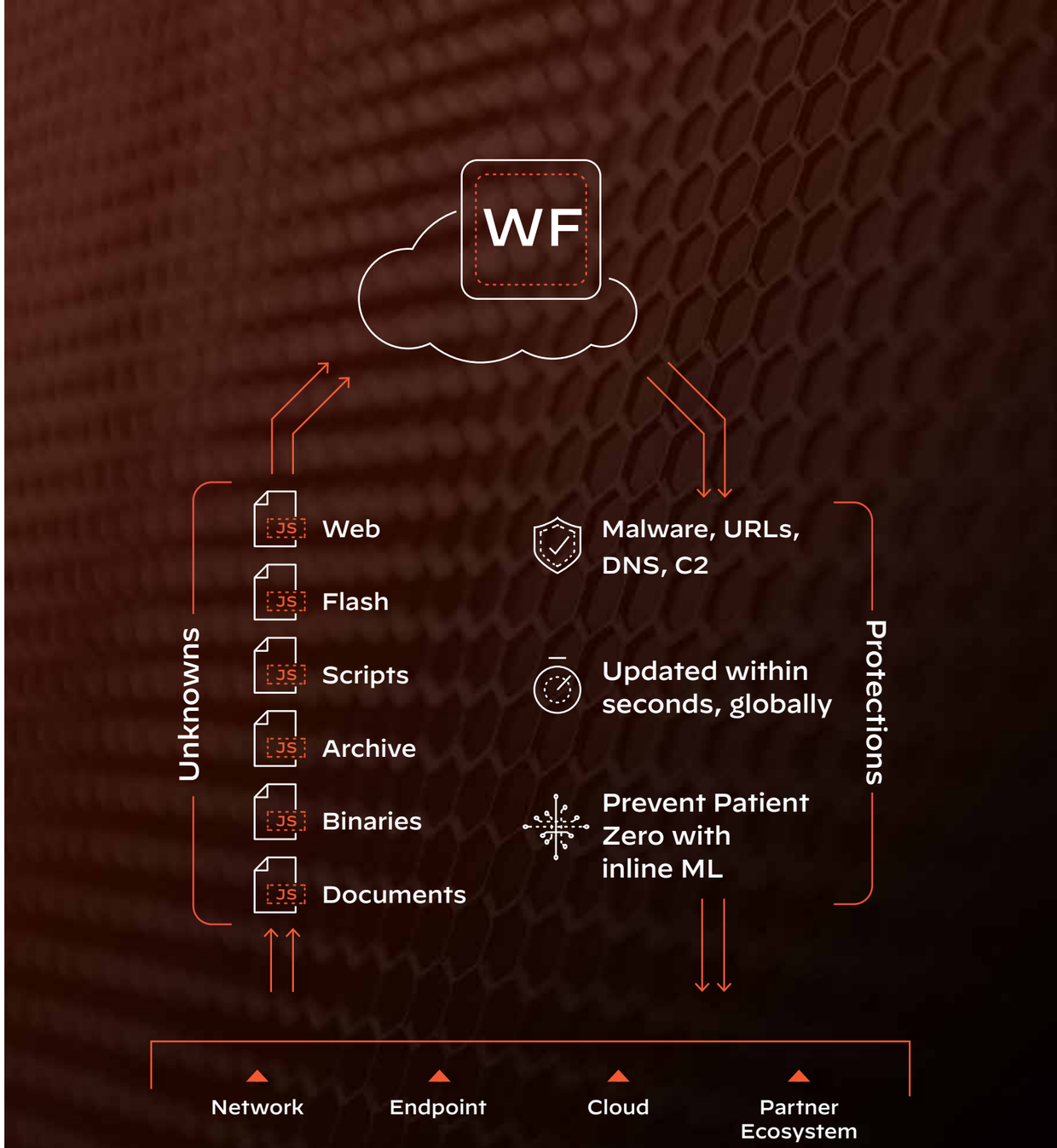
Palo Alto Networks has automated protections so you can focus your time on what matters and let our service handle the manual, repetitive tasks.

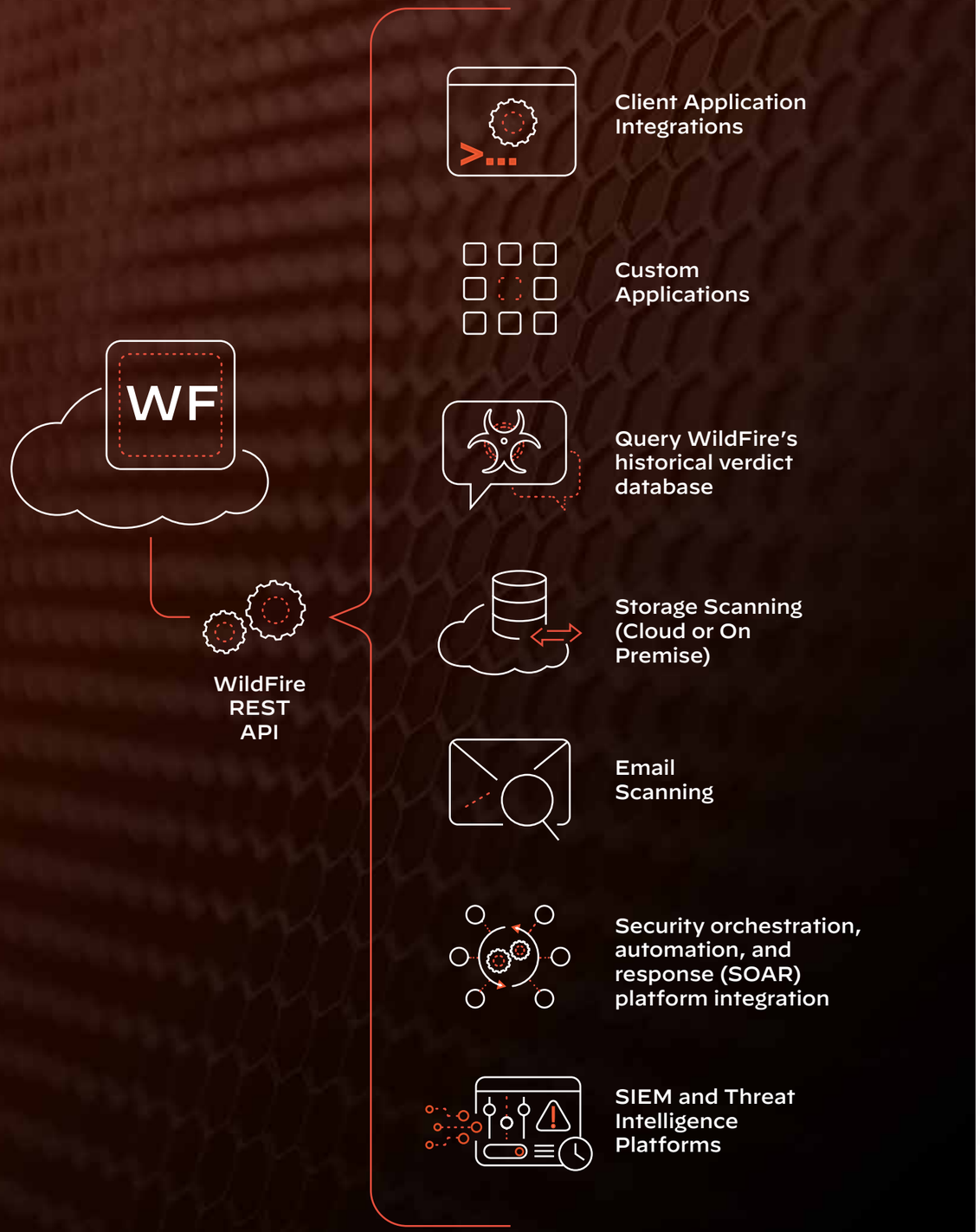
Here is an example of what this automation looks like for identifying and preventing advanced threats:

With WildFire, unknown files from all your NGFWs, as well as cloud instances and endpoints, are sent to a regional WildFire Cloud for analysis.

If WildFire declares the verdict to be malicious for the unknown file, artifacts are extracted and protections are automatically delivered across the platform in real-time. This allows the Palo Alto Networks ecosystem to reprogram itself against new threats without any human intervention, 24 hours a day, 7 days a week, 365 days a year.

This information is shared with other tooling through the open WildFire API. Proofpoint, Mimecast, Tanium and many others integrate via the API in order to holistically block previously unknown threats across all vectors.





Inspecting Every Transaction: Extending WildFire to the New Enterprise Architecture and Enabling Zero Trust

With the recent trend towards digitization, transactions that used to be in person have now been brought online.

These attack vectors, such as customer support, government, and financial portals, must be secured. Recent supply chain attacks have motivated many organizations to adopt a Zero Trust Security Model. To enable organizations to adapt to these changes and address their increasing security needs, WildFire released REST API, allowing customers to integrate WildFire analysis into many other data transaction points, ensuring consistent protection across the entire organization.

WildFire in Action

One of the largest news stories of 2021 was the July 2nd Kaseya ransomeware attack. While many had thought the initial detections were on July 2nd, it actually started in April.

WildFire's global cloud presence was well ahead of Kaseya as it had detected many of the files associated with the main attack in April. WildFire was also able to detect all variants associated with this particular ransomware attack. As each new variant was detected, malware signature updates were immediately distributed to protect all WildFire customers.

WildFire has over 48,000 customers across the globe submitting files for analysis, enabling WildFire to analyze these new variants before any other solution. As the largest cloud-based malware analysis service, the scale and scope of WildFire gives our customers an edge on protections.

There are **14 known variants** associated with the Kaseya Ransomware attack. WildFire's continued innovations enabled it to detect all of them.

4/20/21 — First samples seen and classified as malware by WildFire.

4/22/21 — Apple's upcoming product plans were stolen from their supplier Quanta Computer's database.

5/30/21 — JBS S.A, the largest meat processing company in the world, suffers a cyber attack impacting facilities in the United States, Canada, and Australia.

6/11/21 — Colonial Pipeline reports they were attacked by ransomware. Later, REvil claims responsibility.

7/2/21 — Hundreds of managed service providers had REvil ransomware dropped on their systems through Kaseya desktop management software. REvil demanded $70 million to restore encrypted data.

7/13/21 — REvil websites and other infrastructure vanished from the internet.

Palo Alto Networks
WildFire Malware Analysis and Prevention Solution

Palo Alto Networks WildFire protects you

from becoming the first victim of a new threat, delivering prevention at scale in seconds. With its unique patented detection technology, WildFire prevents up to 95% of unknown file-based threats, 180x faster than the nearest competitor. It is often said "Malware never sleeps". Well, neither does WildFire.

Take the Ultimate Test Drive

To learn how the WildFire security service

can help protect your organization against evasive malware, take the ultimate test drive to get hands-on with WildFire's unique detections or sign up for a 30-day free trial to experience the best-class malware analysis engine in action.

WildFire **30 Day FREE Trial**

For more information and resources

about Palo Alto Networks' WildFire malware analysis solution:

Palo Alto Networks WildFire

www.paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087