
# Global and Regional WildFire Clouds

## Enabling Data Residency and Security

Of the business challenges faced by today's organizations, cybersecurity is becoming top of mind in both IT and the boardroom. Our interconnected, digital world provides significant agility and opportunities for enterprises to thrive while enabling them to bring great value to their customers, which increases profitability. However, it also comes with increased cyber risks that, if not secured and managed properly, can have a devastating impact on business. Cybercriminals are aware of this and continue to take advantage of the evolving, growing attack surface, which might result in serious security breaches.

## Introduction

As these attacks grow in volume and sophistication, organizations need to deploy equivalent countermeasures to eradicate them. Lack of resources, high cost, corporate processes, security point products, and manual responses to security incidents are keeping them one step behind their adversaries.

Here, Palo Alto Networks leads the cybersecurity battlefield by offering the natively integrated, best-of-breed security capabilities of the ML-Powered Next Generation Firewall (NGFW). Palo Alto Networks delivers automated, integrated protection by combining cloud-based and inline machine learning, known and unknown malware analysis, and contextual threat intelligence. Organizations need to face advanced adversaries head on, and Palo Alto Networks can provide complete, automated protection able to evolve and adapt with minimum human intervention.

## WildFire

The WildFire® malware prevention service brings together the benefits of multiple independent techniques—dynamic analysis, static analysis, machine learning, Multi-Vector Recursive Analysis, and bare metal analysis—for high-fidelity, evasion-resistant discovery. These complementary techniques work to investigate and provide verdicts on known and unknown threats, with each serving a particular function:

- **Dynamic analysis** observes files as they detonate in a custom-built, evasion-resistant virtual environment, enabling detection of zero-day malware and exploits by examining hundreds of behavioral characteristics.
- **Static analysis** is highly effective at detecting malware and exploits that attempt to evade dynamic analysis, as well as instantly identifying variants of existing malware.
- **Machine learning** extracts thousands of unique features from each file, training a predictive classifier to identify new malware and exploits in a manner not possible with static or dynamic analysis alone.
- **Bare metal analysis** uses a real hardware environment for automatic detonation of evasive threats, entirely removing an adversary's ability to deploy anti-VM analysis techniques.
- **Multi-Vector Recursive Analysis** combines cloud scale with advanced file analysis and URL crawling to prevent multi-stage, multi-hop attacks employed by sophisticated threat actors.

As an extension of WildFire, our contextual threat intelligence service hunts through contextualized data to correlate indicators of compromise (IOCs) and samples with human intelligence from the Unit 42 threat research team and many third-party threat intelligence feeds, and then turns that raw intelligence into automatic protection. Organizations need to deploy more security automation and orchestration, not more human resources. From common volumetric attacks to

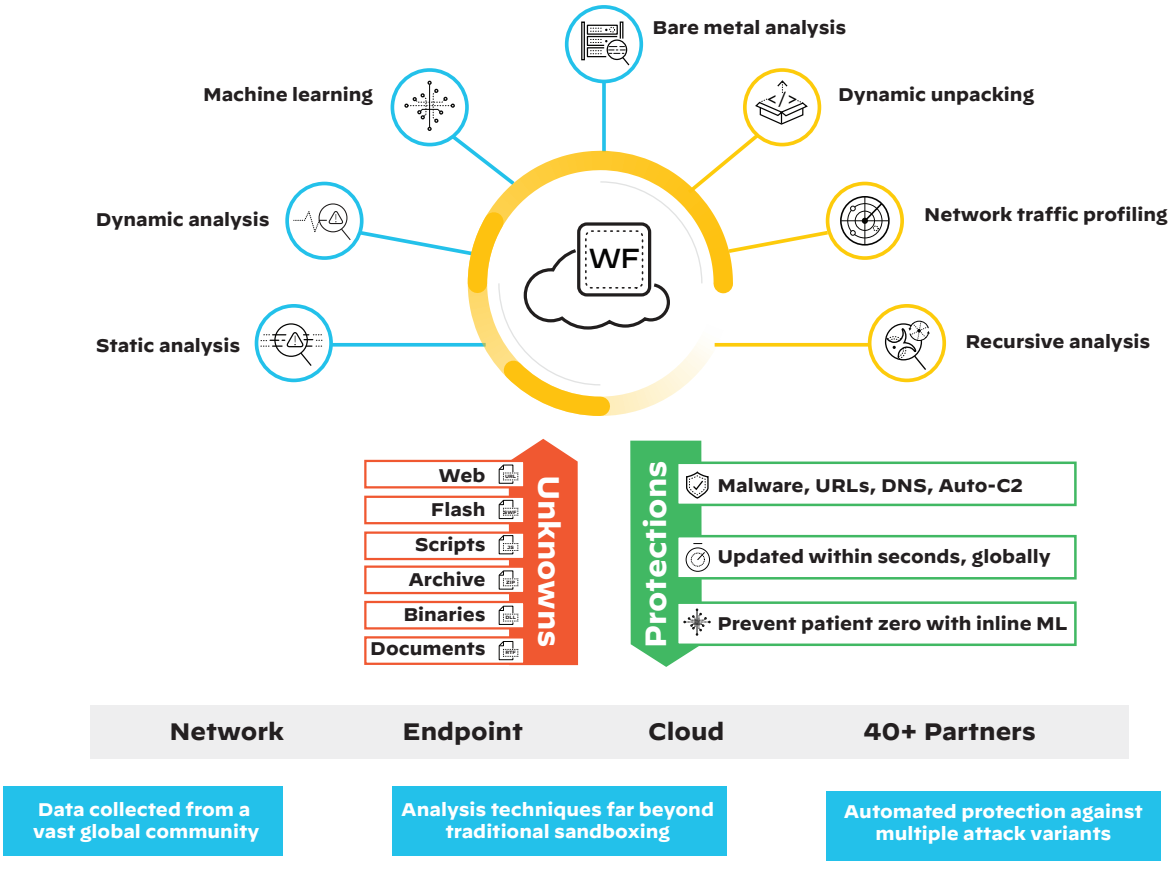



**Figure 1:** WildFire ecosystem

advanced zero-day attacks, the majority of today's threats use automated tools in some shape or form, and it's time for organizations to do the same.

Palo Alto Networks continues to expand its global cloud infrastructure, driven in large part by the power of WildFire. WildFire's cloud-delivered infrastructure collects hundreds of millions of never-before-seen samples each month from more than 37,000 enterprise, government, and service provider customers worldwide. Once an unknown file is classified as known malware, WildFire extracts the relevant IOCs and delivers a verdict: benign, malicious, grayware, or phishing. WildFire automatically deploys these findings in the form of protection packages to the platform in near-real time, enabling all customers to proactively eradicate any evolving threat.

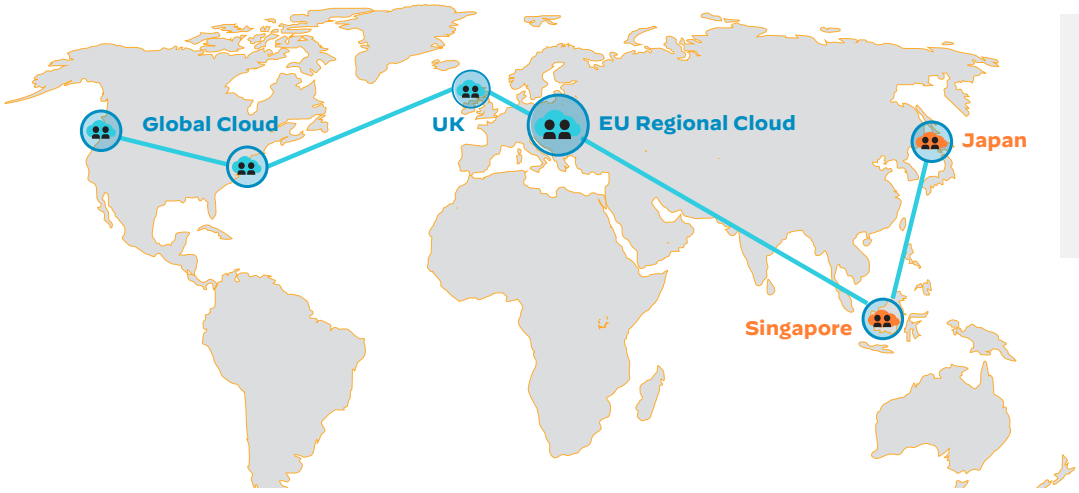
## Distributed Regional WildFire Clouds

Many organizations around the globe are concerned about data privacy, and this can affect their readiness to share data with a global cloud, even for the purposes of security.

Regional WildFire clouds enable customers to fully utilize the industry's most advanced cloud-based threat analysis and prevention engine while ensuring that files submitted for analysis stay in the defined region to address data privacy and sovereignty concerns. Today, regions include the United States (global cloud), the Netherlands (EU regional cloud), the United Kingdom (UK), Singapore, and Japan, with plans to introduce more in the future.

Hosted around the globe in secure locations, regional WildFire clouds enable malware analysis while ensuring that files forwarded remain in that region. Files determined to be benign are deleted shortly after analysis, whereas malicious files are retained locally for further analysis as well as the development and testing of new security products.

The regional WildFire cloud infrastructure also provides organizations with the flexibility to submit certain types of files for malware analysis within their regional borders. At the same time, regional WildFire clouds receive automated protections from the global WildFire cloud infrastructure. This global protection capability is key to preventing successful cyber breaches at all stages of the attack lifecycle.




- SOC 2 Type II and ISO 27001:2013 Compliance
- Regional Data Privacy
- Identical Capabilities
- Distributed Threat Research

**Figure 2:** Global WildFire infrastructure provides scale, agility, and leverage

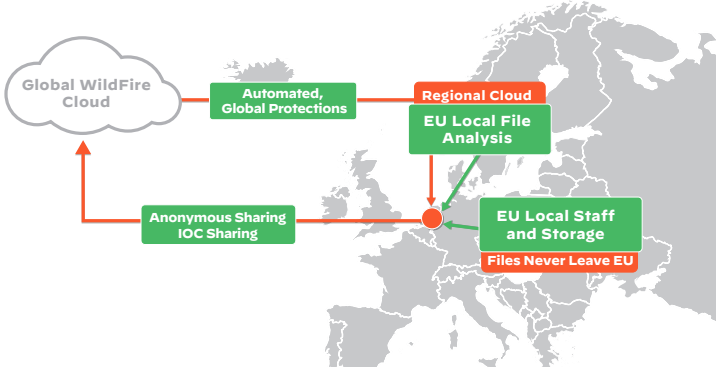



**Figure 3:** EU WildFire cloud

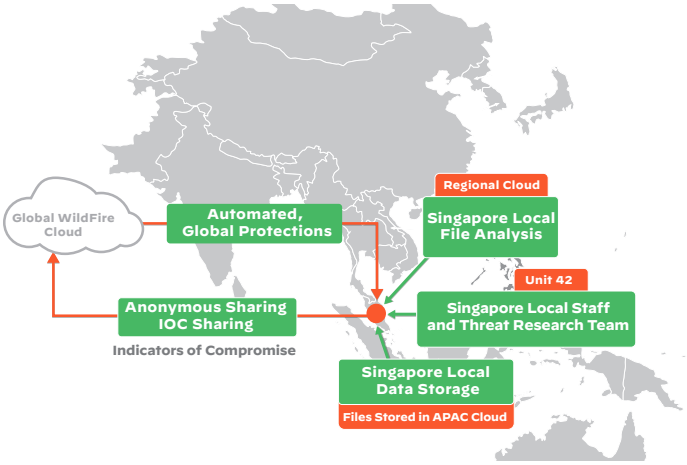



**Figure 4:** Singapore WildFire cloud

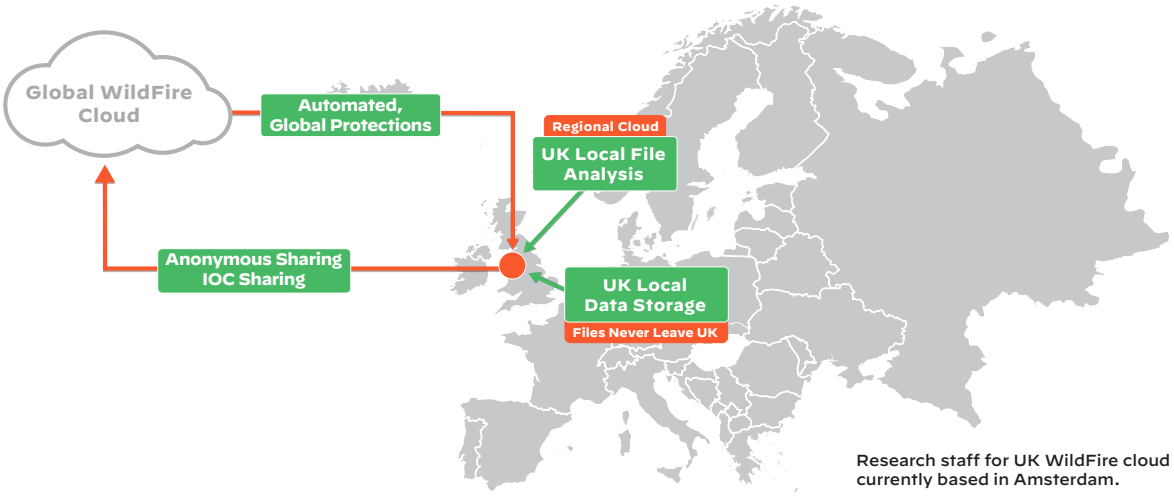



**Figure 5:** UK WildFire cloud

## Conclusion

Today's organizations face serious cyber challenges while doing business. To be successful in today's digital world, they need to prevent threats and respond quickly. This requires effective, automated, and agile threat intelligence. Palo Alto Networks provides this in the form of the global WildFire cloud infrastructure and, for organizations in different regions, the option of a regional WildFire cloud.

Without a fully automated, customized threat intelligence capability, managing today's risks in a way that supports continued growth is more difficult than ever.

See Additional Resources for more detail on how Palo Alto Networks and globally distributed regional clouds can help secure your organization.

## Additional Resources

Palo Alto Networks WildFire Datasheet

Palo Alto Networks WildFire Privacy Datasheet

Palo Alto Networks Cloud-Delivered Services

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com


global-and-regional-wildfire-clouds-wp-081020