Secure the Enterprise (Strata) - continued

Subscription services

In order for your next-generation firewall to gain complete visibility and apply full threat prevention on your network, you must activate the licenses for each of the subscription services:

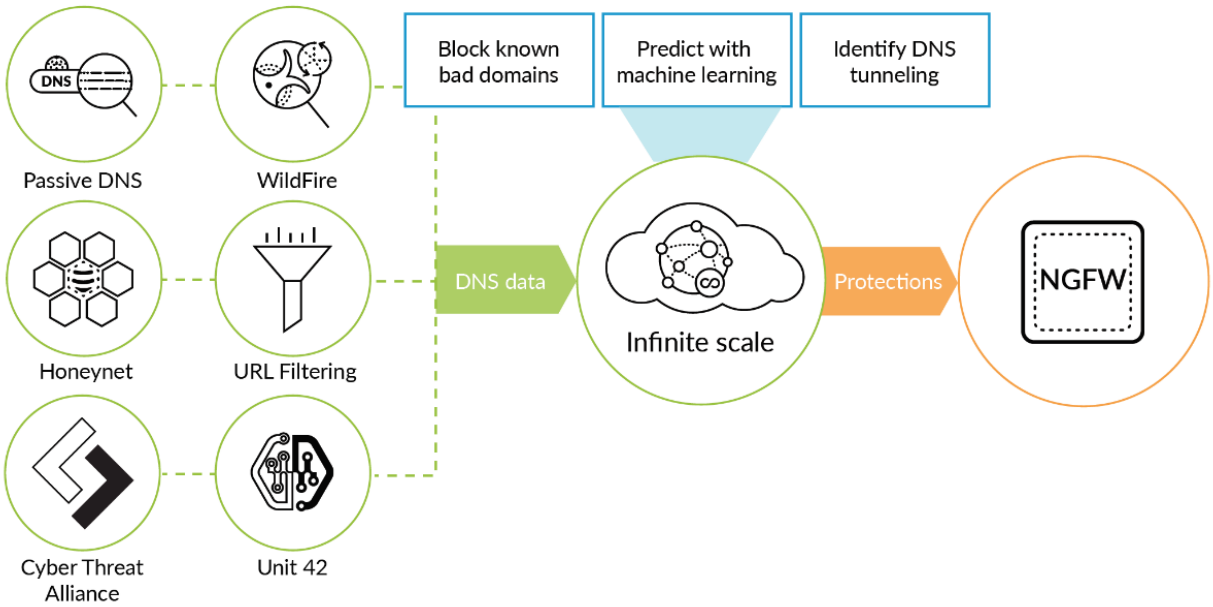
- DNS Security
- URL Filtering
- Threat Prevention
- WildFire

DNS Security service

The Palo Alto Networks DNS Security service applies predictive analytics to disrupt attacks that use DNS for C2 or data theft. Tight integration with Palo Alto Networks next-generation firewalls gives you automated protection and eliminates the need for independent tools. Threats hidden in DNS traffic are rapidly identified with shared threat intelligence and machine learning. Cloud-based protections scale infinitely and are always up to date, giving your organization a critical new control point to stop attacks that use DNS (see Figure 2-22).

Figure 2-22

Rich DNS data powers machine learning for protection.



Predict and block new malicious domains

DNS is a massive and often overlooked attack surface present in every organization. Adversaries take advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack, including reliable C2. Security teams struggle to keep up with new malicious domains and enforce consistent protections for millions of emerging domains at once.

The DNS Security service takes a different approach to predicting and blocking malicious domains, giving the advantage back to overwhelmed network defenders.

Next-generation firewalls protect you against tens of millions of malicious domains identified with real-time analysis and continuously growing global threat intelligence. Your protection continues to grow with data from a large, expanding threat intelligence-sharing community. The Palo Alto Networks malicious domain database has been gathered over years, with sources including:

- WildFire malware prevention service to find new C2 domains, file download source domains, and domains in malicious email links
- URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators
- Passive DNS and device telemetry to understand domain resolution history seen from thousands of deployed next-generation firewalls, generating petabytes of data per day
- Unit 42 threat research to provide human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots
- More than 30 third-party sources of threat intelligence to enrich understanding

With the DNS Security service, your next-generation firewalls can predict and stop malicious domains from domain generation algorithm-based malware with instant enforcement. Malware's use of domain generation algorithms (DGAs) continues to grow, limiting the effectiveness of blocking known malicious domains alone. DGA malware uses a list of randomly generated domains for C2, which can overwhelm the signature capability of traditional security approaches. DNS Security deals with DGA malware by using:

- **Machine learning** to detect new and never-before-seen DGA domains by analyzing DNS queries as they are performed
- **Easy-to-set policy** for dynamic action to block DGA domains or sinkhole DNS queries
- **Threat attribution and context** to identify the malware family with machine learning for faster investigation efforts

A cloud-based database scales infinitely to provide limitless protection against malicious domains. Your protections are always up to date, whether 10,000 or 100 million new malicious domains are created in a single day. As part of the cloud-based service, all DNS queries are checked against the Palo Alto Networks infinitely scalable, cloud-based database in real time to determine appropriate enforcement action. The DNS Security service removes one of the most effective and widely used methods by which attackers establish C2, and its protection scales infinitely, ensuring your next-generation firewalls can get ahead of new malicious domains before any harm is done.

Neutralize DNS tunneling

Advanced attackers use DNS tunneling to hide data theft or C2 in standard DNS traffic. The sheer volume of DNS traffic often means defenders simply lack the visibility or resources to universally inspect it for threats. The DNS Security service enables you to:

- Use machine learning to quickly detect C2 or data theft hidden in DNS tunneling. With historical and real-time shared threat intelligence, Palo Alto Networks algorithms observe the features of DNS queries, including query rate and patterns, entropy, and *n*-gram frequency analysis of the domains to accurately detect tunneling behavior.
- Extend PAN-OS signature-based protection to identify advanced tunneling attempts. DNS Security expands the native ability of next-generation firewalls to detect and prevent DNS tunneling. Protections are scalable and evasion-resistant, covering known and unknown variants of DNS tunneling.
- Rapidly neutralize DNS tunneling with automated policy action. DNS tunneling is automatically stopped with the combination of easy-to-set policy actions on the next-generation firewall and blocking the parent domain for all customers.

Simplify security with automation and replace standalone tools

Security teams need integrated innovations that extend the value of their existing security investments without complicating operations. DNS Security takes advantage of the next-generation firewall to stop attacks using DNS, with full automation to reduce manual effort.

Tight integration with the next-generation firewall provides a critical new control point to stop attacks that use DNS. The service ensures that you have one device to deploy, with a single set of policies to manage. Alerts are coordinated across your entire security stack, including firewall policy violations, IDS/IPS, web security, and malware analysis.

When attacks using DNS are identified, security administrators can automate the process of sinkholing malicious domains on the firewall to cut off C2 and rapidly identify infected users on the network. Combining malicious domain sinkholing, DAGs, and logging actions automates detection and response workflows, saving analysts time by removing slow and manual processes.

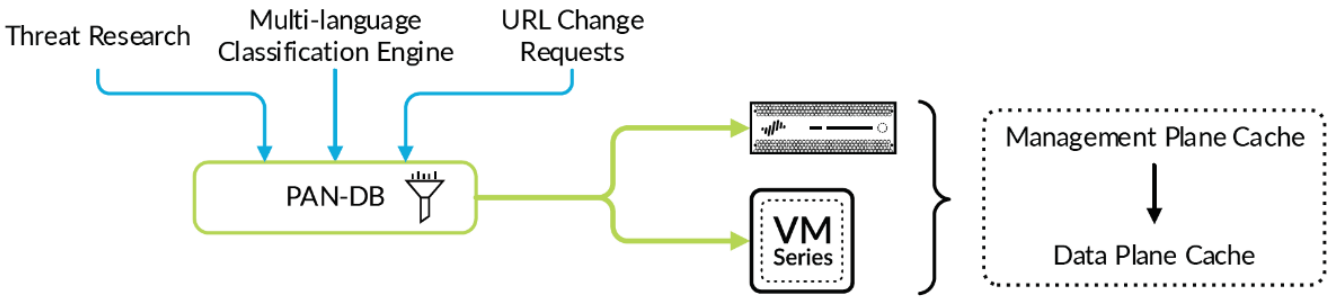
The DNS Security service is built on a modular, cloud-based architecture to seamlessly add new detection, prevention, and analytics capabilities with zero impact to production next-generation firewalls.

URL Filtering service

To complement the threat prevention and application control capabilities, a fully integrated, on-box URL filtering database enables security teams to not only control end-user web surfing activities but also to combine URL context with application and user rules. The URL Filtering service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages. You can use the URL category as a match criterion in policies, which permits exception-based behavior and granular policy enforcement. For example, you can deny access to malware and hacking sites for all users but allow access to users who belong to the IT security group.

When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN-DB, which contains millions of URLs that have been grouped into approximately 65 categories. The malware and phishing URL categories in PAN-DB are updated in real time, which can enforce subsequent attempts to access the site based on the URL category, instead of treating it as unknown. User-credential detection, a part of URL Filtering, allows you to alert on or block users from submitting credentials to untrusted sites. If corporate credentials are compromised, user-credential detection allows you to identify who submitted credentials so that you can remediate (see Figure 2-23).

Figure 2-23 URL Filtering service



The on-box URL database can be augmented to suit the traffic patterns of the local user community with a custom URL database. For fast and easy access to frequently visited URLs, PAN-DB provides high-performance local caching, and URLs that are not categorized by the local URL database can be pulled into cache from a hosted URL database. In addition to database customization, administrators can create unique URL categories to further customize the URL controls to suit their specific needs.

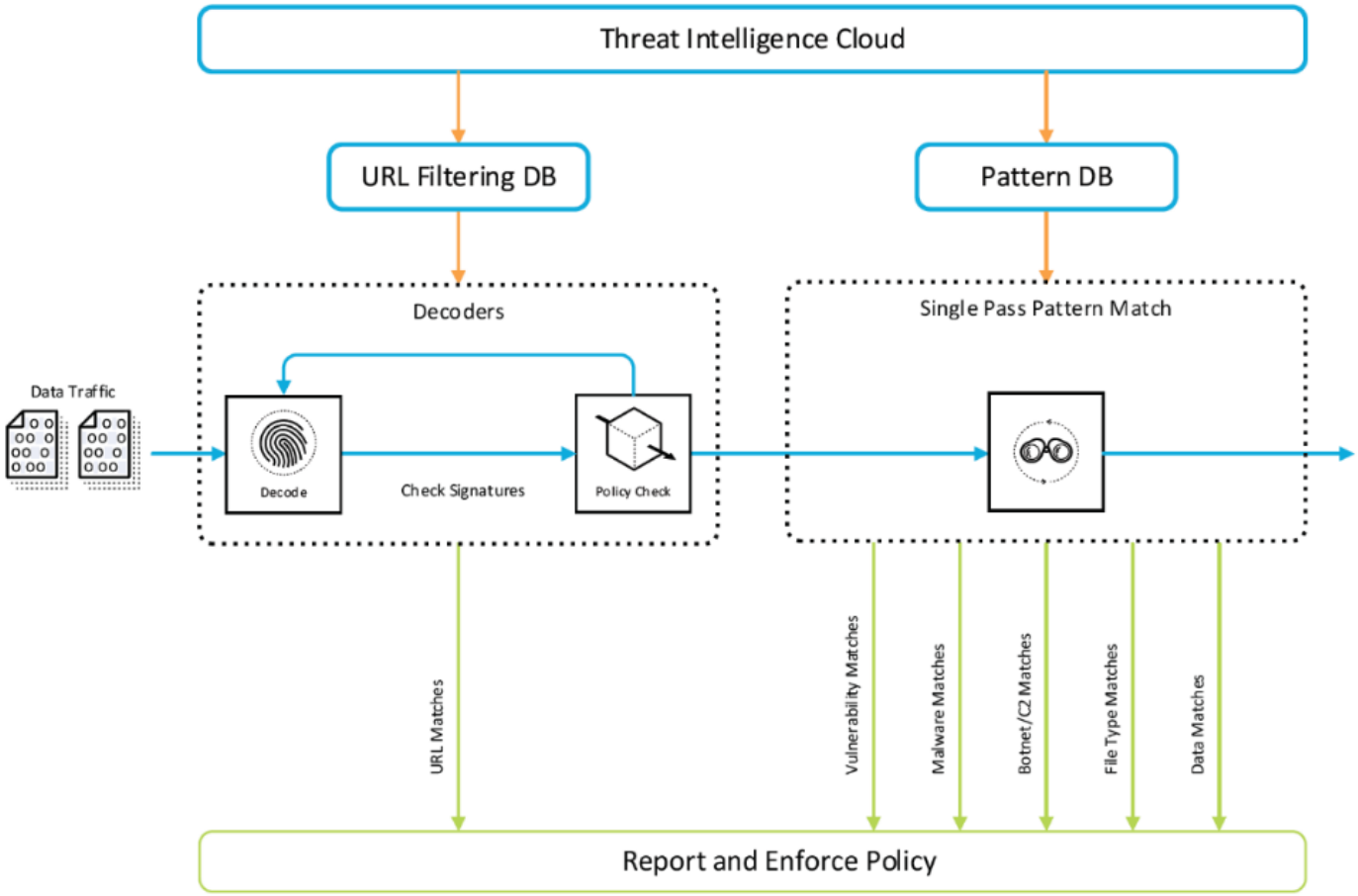
URL categorization can be combined with application and user classification to further target and define policies. For example, SSL decryption can be invoked for select high-risk URL categories to ensure that threats are exposed, and QoS controls can be applied to streaming media sites. URL filtering visibility and policy controls can be bound to specific users through transparent integration with enterprise directory services (such as Active Directory, LDAP, and eDirectory), with additional insight provided through customizable reporting and logging.

Administrators can configure a custom block page to notify end users of any policy violations. The page can include references to the username, the IP address, the URL they are attempting to access, and the URL category. To place some of the web activity ownership back in the user's hands, administrators can allow users to continue to the website or webpage after being presented with a warning page, or they can use passwords to override the URL filtering policy.

Threat Prevention service (antivirus, anti-spyware, and vulnerability protection)

Threat Prevention blocks known malware, exploits, and C2 activity on the network. Adding the Threat Prevention subscription brings additional capabilities to your next-generation firewall that identify and prevent known threats hidden within allowed applications. The Threat Prevention subscription includes malware/antivirus, C2, and vulnerability protection (see Figure 2-24).

Figure 2-24 Threat Prevention service



Malware/antivirus protection

Using content-based signatures, inline malware protection blocks malware before it ever reaches the target host. Signatures based on content detect patterns in the body of the file that identify future variations of the files, even when the content is modified slightly. This ability allows the next-generation firewall to identify and block polymorphic malware that otherwise would be treated as a new unknown file.

The stream-based scanning engine protects the network without introducing significant latency, which is a serious drawback of network antivirus offerings that rely on proxy-based scanning engines. The stream-based malware scanning inspects traffic when the first packets of the file are received, eliminating threats as well as performance issues typical of traditional standalone solutions. Key anti-malware capabilities include:

- Inline, stream-based detection and prevention of malware hidden in compressed files and web content
- Protection against payloads hidden in common file types, such as Microsoft Office documents and PDF files

Command-and-control (spyware) protection

There are no silver bullets when it comes to preventing all threats from entering the network. After the initial infection, attackers communicate with the compromised device through a C2 channel, using it to pull down additional malware, issue further instructions, and steal data. C2 protections focus on those unauthorized communication channels and cut them off by blocking outbound requests to malicious domains and from known C2 toolkits installed on infected devices.

The C2 protection provides sinkhole capabilities for outbound requests to malicious domains, accurately identifying the compromised device and preventing data exfiltration. You can configure the sinkhole so that any outbound request to a malicious domain or IP address is redirected to one of your network's internal IP addresses. This policy effectively blocks C2 communication, preventing those requests from ever leaving the network. A report of the hosts on your network making such requests is compiled even though those hosts sit behind the DNS server. You have a daily list of potentially compromised devices on which to act, without the added stress of remediation crunch time, because communications with the attacker have already been severed.

Vulnerability protection

The next-generation firewall's vulnerability protection and intrusion prevention capabilities detect and block exploit attempts and evasive techniques at both the network and the application layers. These exploits can include port scans, buffer overflows, remote code execution, protocol fragmentation, and obfuscation. Vulnerability protections are based on signature matching and anomaly detection, which decode and analyze protocols and use the information learned to block malicious traffic patterns and provide visibility through alerts. Stateful pattern matching detects attacks across multiple packets, considering arrival order and sequence – ensuring that all allowed traffic is well-intentioned and devoid of evasion techniques.

Protocol decoder-based analysis decodes the protocol and then intelligently applies signatures to detect network and application exploits. Because there are many ways to exploit a single vulnerability, the intrusion prevention signatures are based on the vulnerability itself, providing more thorough protection against a wide variety of exploits. A single signature can stop multiple exploits of a known system or application vulnerability. Protocol anomaly-based protection detects non-Request for Comments (RFC) compliant protocol use, such as an overlong uniform resource identifier (URI) or FTP login. Finally, easy-to-configure, custom vulnerability signatures allow you to tailor intrusion prevention capabilities to your network's unique needs.

Zero-day malware prevention (WildFire)

The WildFire cloud-based malware analysis environment is a cyberthreat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. WildFire automatically disseminates updated protections in near real time to immediately prevent threats from spreading – without manual intervention. Although basic WildFire support is included as part of the Threat Prevention license, the WildFire subscription service provides enhanced services for organizations that require immediate coverage for threats, frequent WildFire signature updates, advanced file type forwarding (APK, PDF, Microsoft Office, and Java Applet), as well as the ability to upload files by using the WildFire API.

As part of the next-generation firewall's inline threat prevention capability, the firewall performs a hash calculation for each unknown file, and the hash is submitted to WildFire. If any WildFire subscriber has seen the file before, then the existing verdict for that file is immediately returned. Links from inspected emails are also submitted to WildFire for analysis. Possible verdicts include:

- **Benign.** Safe and does not exhibit malicious behavior
- **Grayware.** No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects)
- **Malware.** Malicious in nature and intent and can pose security threat (for example, viruses, worms, Trojans, rootkits, botnets, and remote-access toolkits)
- **Phishing.** Malicious attempt to trick the recipient into revealing sensitive data

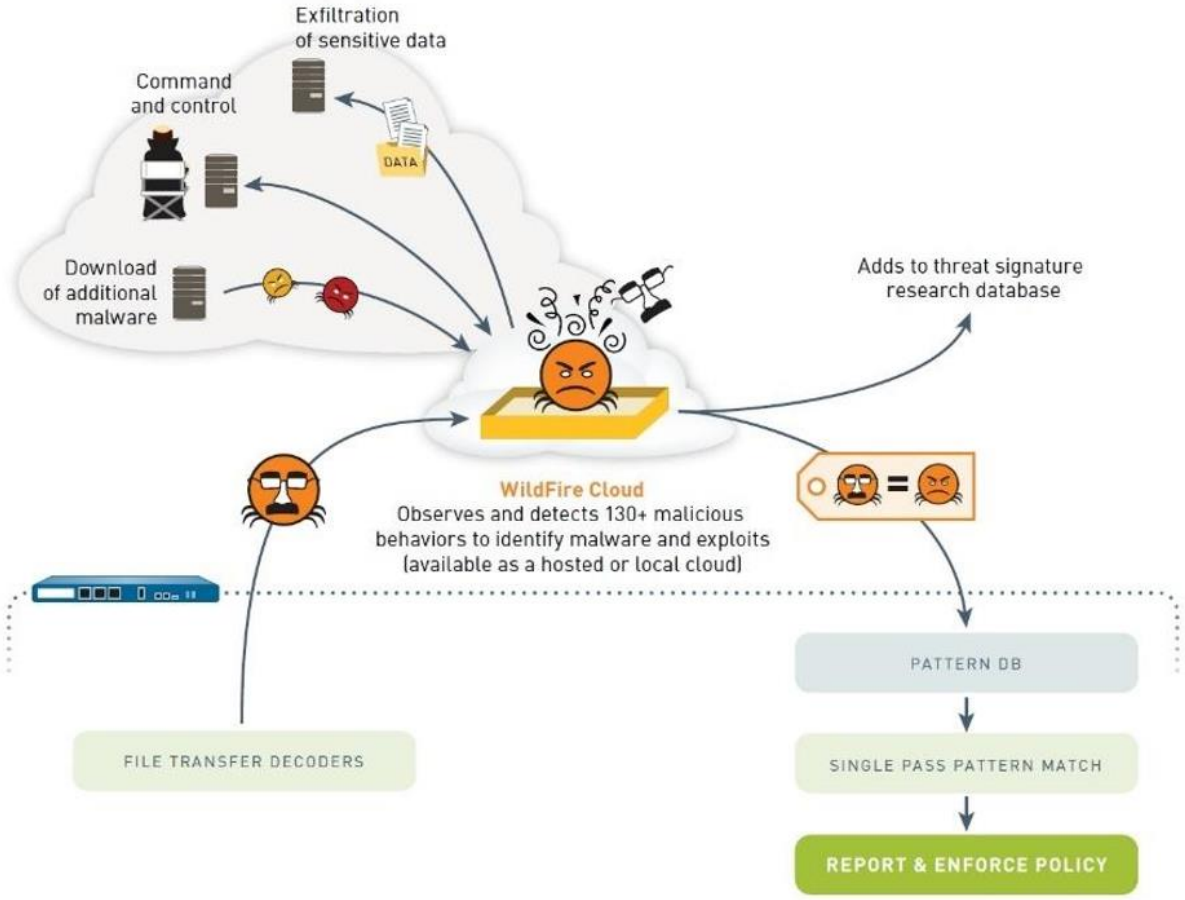
If WildFire has never seen the file, the next-generation firewall is instructed to submit the file for analysis. If the file size is under the configured size limit, the next-generation firewall securely transmits the file to WildFire. Next-generation firewalls with an active WildFire license perform scheduled auto-updates to their WildFire signatures, with update checks configured as often as every minute.

WildFire leverages inline machine learning based malware and phishing prevention (real-time WildFire verdict and anti-malware dynamic classification) to determine if the corresponding webpages for email links submitted to the service host any exploits, malware, or phishing capabilities. The behaviors and properties of the website are taken into consideration when making a verdict on the link.

WildFire significantly improves security posture and protection against unknown malware. WildFire processes about 5 million unique files daily and about 30,000 to 50,000 unique malware files that are sent to WildFire by customer-deployed Palo Alto Networks next-generation firewalls. Typically, 60 percent of these malware files are not detected by any of the major antivirus vendors when first submitted to WildFire, and 30 days later 25 to 50 percent are still not detected by the major antivirus vendors.

To support dynamic malware analysis across the network at scale, WildFire is built on a cloud-based architecture (see Figure 2-25). Where regulatory or privacy requirements prevent the use of public cloud infrastructure, a private cloud solution can be built in an on-premises data center.

Figure 2-25 WildFire provides cloud-based malware analysis and threat prevention.



In addition to leveraging either public cloud or private cloud deployments, organizations can use both within the same environment. The hybrid cloud capabilities of WildFire allow security teams more file analysis flexibility because they can define which file types are sent to the WildFire public cloud versus the on-premises appliance, or private cloud. The WildFire hybrid cloud capability enables organizations to alleviate privacy or regulatory concerns by using the WildFire appliance for file types containing sensitive data. Organizations also benefit from the comprehensive analysis and global threat intelligence services of the WildFire public cloud for all others. AutoFocus is the centerpiece of WildFire threat intelligence.

The Security Operating Platform proactively blocks known threats, which provides baseline defenses against known exploits, malware, malicious URLs, and C2 activity. When new threats emerge, the Security Operating Platform automatically routes suspicious files and URLs to WildFire for deep analysis.

WildFire inspects millions of samples per week from its global network of customers and threat intelligence partners looking for new forms of previously unknown malware, exploits, malicious domains, and outbound C2 activity. The cloud-based service automatically creates new protections that can block targeted and unknown malware, exploits, and outbound C2 activity by observing their actual behavior, rather than relying on pre-existing signatures. The protections are delivered globally in minutes. The result is a closed-loop, automated approach to preventing cyberthreats that includes:

- Positive security controls to reduce the attack surface
- Inspection of all traffic, ports, and protocols to block all known threats
- Rapid detection of unknown threats by observing the actions of malware in a cloud-based execution environment
- Automatic deployment of new protections back to the frontline to ensure that threats are known to all and blocked across the attack lifecycle

Behavior-based cyberthreat discovery

To find unknown malware and exploits, WildFire executes suspicious content in the Windows, Android, and macOS operating systems, with full visibility into common file types, including:

- Executables (EXEs), dynamic-link libraries (DLLs), compressed files (ZIP), and Portable Document Format (PDF)
- Microsoft Office documents, spreadsheets, and presentations
- Java files
- Android application packages (APKs)
- Adobe Flash applets and webpages (including high-risk embedded content, such as Java and Adobe Flash files/images)

WildFire identifies hundreds of potentially malicious behaviors to uncover the true nature of malicious files based on their actions, including:

- **Changes made to host.** WildFire monitors all processes for modifications to the host, including file and registry activity, code injection, memory heap spraying (exploits), *mutexes*, Windows service activity, the addition of auto-run programs, and other potentially suspicious activities.
- **Suspicious network traffic.** WildFire performs analysis of all network activity produced by the suspicious file, including backdoor creation, downloading of next-stage malware, visiting low-reputation domains, network reconnaissance, and more.

- **Anti-analysis detection.** WildFire monitors techniques used by advanced malware that is designed to avoid virtual machine-based analysis, such as debugger detection, hypervisor detection, code injection into trusted processes, disabling of host-based security features, and more.

Key Terms

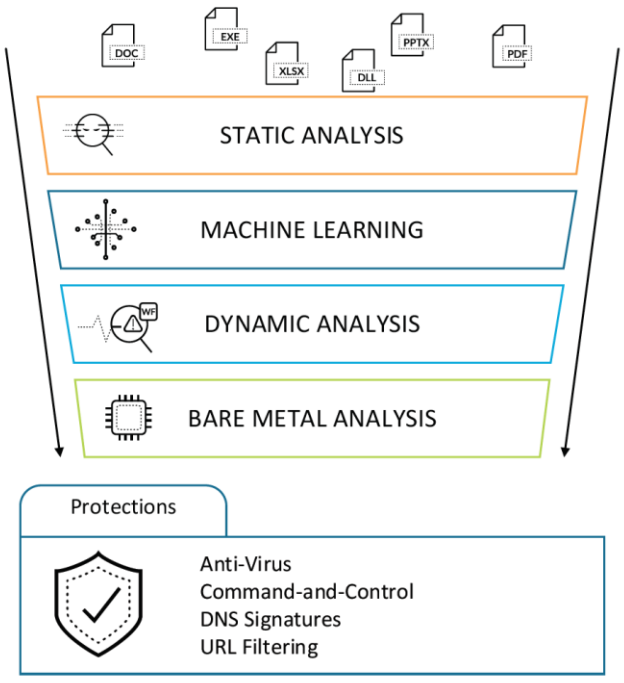
A *mutex* is a program object that allows multiple program threads to share the same resource, such as file access, but not simultaneously.

WildFire is natively integrated with the Security Operating Platform, which includes Cortex XDR endpoint protection and Prisma SaaS, and it can classify all traffic across hundreds of applications. WildFire uniquely applies this behavioral analysis to web traffic, email protocols (SMTP, IMAP, and POP3), and FTP, regardless of ports or encryption.

WildFire applies the following analysis methods to submitted files (see Figure 2-26):

- **Machine learning/static analysis.** Identification of variants of known threats by comparing malware feature sets against a dynamically updated classification system. Detection of known threats by analyzing the characteristics of samples before execution.
- **Dynamic analysis.** A custom-built, evasion-resistant virtual environment in which previously unknown submissions are executed within a virtualized test environment to determine real-world effects and behavior.
- **Bare-metal dynamic analysis.** Fully hardware-based analysis environment specifically designed for advanced VM-aware threats. Samples that display the characteristics of an advanced VM-aware threat are steered toward the bare-metal appliance by the heuristic engine.

Figure 2-26 WildFire analysis



The dynamic updates from the Threat Intelligence Cloud coordinate threat prevention across the platform and are key to the prevention capabilities it provides. The unknown-threat handling methodology essentially turns unknown threats into known threats.

In addition to protecting you from malicious and exploitive files and links, WildFire looks deeply into malicious outbound communication, disrupting command-and-control (C2) activity with anti-C2 signatures and DNS-based callback signatures. WildFire also feeds this information into URL Filtering with PAN-DB, which automatically blocks newly discovered malicious URLs. This correlation of threat data and automated protections is key to identifying and blocking ongoing intrusion attempts and future attacks on your organization, without requiring policy updates and configuration commits.

Furthermore, Palo Alto Networks promotes information sharing and industry advocacy by contributing structured intelligence derived from its Threat Intelligence Cloud to the Cyber Threat Alliance (CTA). Co-founded by Palo Alto Networks and other industry leaders, the CTA is an organization working to improve the cybersecurity of the global digital ecosystem by enabling near real-time, high-quality cyberthreat information sharing within the cybersecurity community. CTA and its members share timely, actionable, contextualized, and campaign-based intelligence that they can use to improve their products and services in order to better protect their customers, more systematically thwart adversaries, and improve the security of the digital ecosystem.

Threat prevention with global intelligence sharing

When an unknown threat is discovered, WildFire automatically generates protections to block it across the Cyber-Attack Lifecycle, and it shares these updates with all global subscribers within as little as 5 minutes. These quick updates can stop rapidly spreading malware. And these updates are payload-based, so they can block proliferation of future variants without any additional action or analysis.

WildFire protects organizations from malicious and exploitive files and links, and it also looks deep into malicious outbound communication and disrupts C2 activity with anti-C2 signatures and DNS-based callback signatures. The information is also used for URL Filtering with PAN-DB, where newly discovered malicious URLs are automatically blocked. This correlation of threat data and automated protections is key to identifying and blocking ongoing intrusion attempts and future attacks against your organization.

Integrated logging, reporting, and forensics

WildFire provides access to integrated logs, analysis, and visibility into WildFire events, through the management interface, the WildFire portal, AutoFocus, and Panorama. This access enables security teams to quickly investigate and correlate events observed in their networks to rapidly locate the data needed for timely investigations and incident response.

Host-based and network-based *indicators of compromise* (IoCs) become actionable through log analysis and custom signatures. To aid security and incident response teams in discovering infected hosts, WildFire also provides:

- Detailed analysis of every malicious file sent to WildFire across multiple operating system environments, including host-based and network-based activity.
- Session data associated with the delivery of the malicious file, including source, destination, application, User-ID, and URL.
- Access to the original malware sample for reverse engineering and full packet captures (pcaps) of dynamic analysis sessions.
- An open application programming interface (API) for integration with best-in-class security information and event management (SIEM) tools (such as the Palo Alto Networks application for Splunk), and leading endpoint agents. This analysis provides numerous IoCs that can be applied across the attack lifecycle.
- Native integration with Cortex XDR endpoint protection and Prisma SaaS.
- Access to the actionable intelligence and global context provided by AutoFocus threat intelligence.
- Native integration with the correlation engine in Palo Alto Networks next-generation firewalls.

Key Terms

An *indicator of compromise* (IoC) is a network or operating system (OS) artifact that provides a high level of confidence that a computer security incident has occurred.

A *packet capture* (pcap) is a traffic intercept of data packets that can be used for analysis.