WildFire

Eliminieren von Gefahren evasiver Malware

Hier zählen Sekunden: Warum traditionelle Malwareanalyse und Sandboxing nicht wirken

Die Hacker von heute haben leichten Zugang zu einer gut funktionierenden Cloud-Infrastruktur sowie zu maschinellem Lernen, und können auf diese Weise evasive schädliche Dateien schnell unter Endbenutzer bringen. Separate Sicherheitstools können mit der heutigen Malware, die sich mit einer Geschwindigkeit von 1.000 neuen Bedrohungen alle fünf Minuten verbreitet und fünf Minuten später bis zu 10.000 Varianten aufweist, einfach nicht Schritt halten.

Unternehmensvorteile

Seien Sie nicht das erste Opfer einer neuen Bedrohung. Die neue Inline-Prävention stoppt noch nie dagewesene Bedrohungen in gängigen Dateitypen auf der ML-basierten Next-Generation Firewall (NGFW), ohne die Produktivität zu beeinträchtigen.

Eliminieren Sie das Risiko zu langer Verweildauer. Verkürzen Sie die Reaktionszeit auf Bedrohungen von Stunden oder Minuten auf Sekunden durch die automatisierte Bereitstellung von koordiniertem Schutz auf dem gesamten Netzwerk, den Endpunkten und in der Cloud.

Reduzieren Sie Ereignisse, die eine Handlung erfordern, und eine durch Sicherheitsmaßnahmen verursachte Arbeitslast. Inline-Präventionsfunktionen auf der ML-basierten NGFW stoppen die ursprüngliche Bedrohung und erfordern weniger Aktionen zum Untersuchen und Eindämmen des Angriffs.

Verringern Sie die Gesamtbetriebskosten mit einer cloudbasierten Architektur. Eliminieren Sie die Kosten für Bereitstellung, Verwaltung, Korrektur und Wartung anwendungsbasierter Sandboxes.

Erlangen Sie umfassende Analysekapazitäten ohne steigende Kosten. Unser Abonnementmodell bietet Ihnen die erforderliche Rechenleistung und Skalierbarkeit ohne kapazitätsbasierte Gebühren.

Vermeiden Sie manuelle Integrationen. Alle neu erstellten Daten werden automatisch wieder in das Ökosystem der Palo Alto Networks eingespeist, wodurch manuelle Tools oder Integrationen überflüssig werden.

Unternehmen, die Zero-Day-Angriffe oder hochentwickelte Dauerbedrohungen (APTs) verzeichnen, die zu Datenlecks führen, können folgende Probleme bekommen:

- **Reputationsrisiko** – Medien- und Presseberichterstattung, bedingt durch Behörden- und Branchenauflagen und verstärkt durch den Umfang und die Art der verloren gegangenen Daten.
- **Regulatorisches Risiko** – Von Behörden verhängte Strafmaßnahmen sowie erhöhte Anforderungen an Compliance und Bewertung, je nachdem, welche Daten gehackt wurden (z. B. persönlich identifizierbare Informationen [PII], Kontoinformationen, geistiges Eigentum von Unternehmen oder Kunden).
- **Finanzielles Risiko** – Möglicher Einnahmenverlust in Verbindung mit geringerem Käufervertrauen, Ransomware und verschärften Vorschriften (z. B. Ausfallzeiten, Verkaufseinbußen, Erhöhung der Complianceanforderungen, Kosten der Datenabfrage).
- **Rechtliches Risiko** – Haftung aufgrund zivilrechtlicher Klagen und Due-Diligence-Problemen, die sich aus dem Verlust von Kundendaten und der Einhaltung von Vorschriften ergeben (z. B. HIPAA, DSGVO, US-Staatsgesetzgebung [CCPA, NYDFS Cybersecurity Regulation usw.], australische Datenschutzbestimmungen).

Um die mit evasiven Angriffen verbundenen Risiken zu mindern, nutzen Unternehmen für die Analyse von Malware Netzwerk-Sandboxing-Lösungen. Leider beeinträchtigen all diese traditionellen Lösungen die Produktivität der Benutzer und liefern verzögerte Ergebnisse, unterbrechen Arbeitsabläufe, indem sie Dateien zur Analyse verwenden, beanspruchen Inhalte, während sie gescannt werden, oder ändern Inhalte und machen viele Dateien unlesbar. Darüber hinaus weisen diese Lösungen ein weiteres fatales Problem auf: Sie können nur dann vor neuen Bedrohungen schützen, wenn das erste Opfer in einer Organisation (alias Patient Null) bereits identifiziert oder geschädigt wurde.

Sofortige Prävention dank endlos skalierbarer Analysemöglichkeiten in der Cloud

Der Malwarepräventionsdienst von Palo Alto Networks WildFire® gewährleistet gleichzeitig Sicherheit und Leistung und ermöglicht es Organisationen, die Prävention an die erste Stelle zu setzen. Als branchenweit fortschrittlichste cloudbasierte Analyse- und Präventionsengine für Malware untersucht WildFire alle unbekannten Dateien auf böswillige Absichten und setzt dann in Rekordzeit Präventionsmaßnahmen, um das Risiko eines ersten Opfers – und jeder nachfolgenden Bedrohung – zu reduzieren.

Im Gegensatz zu herkömmlichen Lösungen, die ausschließlich die Offline- oder verzögerte Analyse unbekannter Malware nutzen, fließen alle WildFire-Analyseinformationen und -daten direkt in maschinelle Lernmodelle ein, die lokal auf Firewallebene wirken und bis zu 95 % neuer Bedrohungen inline stoppen. Für den Rest verwendet WildFire ein innovatives, auf mehreren Technologien aufsetzendes Verfahren, um Signaturen in Sekundenschnelle an jede ML-basierte NGFW zu verteilen.

Keine andere Malwareanalyse-Engine bietet Prävention, ohne die Produktivität zu beeinträchtigen. WildFire kombiniert die dynamische und statische Analyse, innovative maschinelle Lernverfahren, die rekursive Analyse und eine bahnbrechende, speziell entwickelte Analyseumgebung, um selbst die fortschrittlichsten und evasivsten Bedrohungen zu analysieren, zu identifizieren und zu verhindern. Neben den Analysefähigkeiten punktet WildFire auch mit Automatisierung: WildFire nutzt schnelle und konsistente Prävention am Netzwerkperimeter, im Rechenzentrum, in der Cloud, innerhalb von SaaS-Anwendungen (Software-as-a-Service) und an Endpunkten.

Wichtige Funktionen

Verhindert unbekannte Bedrohungen auf Firewallebene mit Inline Machine Learning

WildFire basiert auf Bedrohungsmodellen, die kontinuierlich in der Cloud verbessert werden, und beinhaltet eine auf maschinellem Lernen basierende Inline-Engine, die in unsere Hardware und virtuellen ML-basierten NGFWs integriert ist. Diese innovative, signaturlose Funktion verhindert böswillige Inhalte in gängigen Dateitypen vollständig inline – wie z. B. in portablen ausführbaren Dateien und dateilosen Angriffen, die von PowerShell® stammen. Dabei ist weder eine Cloud-Analyse erforderlich, noch werden Inhalte beschädigt oder die Benutzerproduktivität beeinträchtigt. Unabhängig davon, ob eine unbekannte Datei mit einer vorhandenen Signatur übereinstimmt oder von einer ML-basierten NGFW klassifiziert wird, führt WildFire immer eine vollständige Analyse durch und extrahiert wertvolle Informationen und Daten. So erhalten Sicherheitsanalysten den nötigen Kontext, werden Schulungsupdates für die maschinellen Lernmodelle generiert und Informationen mit anderen Abonnements ausgetauscht, um andere Angriffsvektoren zu verhindern.

Liefert in Sekunden globale Prävention im gesamten WildFire-Ökosystem

Bei speziell auf ein Unternehmen zugeschnittenen Bedrohungen, die durch die lernfähige Inline-Prävention von WildFire nicht gestoppt werden können, wird eine leistungsstarke cloudbasierte Analyse angewendet, um Prävention in Netzwerken, Clouds, Endpunkten oder an anderen WildFire-aktivierten Sensoren zu gewährleisten. Im Zusammenspiel mit den neuen Fähigkeiten von PAN-OS® erzeugt

WildFire innerhalb von Sekunden nach der ersten Analyse für den Großteil neuer Bedrohungen eine globale Präventionsmaßnahme und stellt diese bereit. Diese innovative, über die Cloud skalierte Bereitstellung von evasionsresistenten Signaturen verhindert, dass Angreifer bösartige Inhalte erfolgreich verbreiten können.

Nutzt Signaturen, keine Hashes

Da WildFire anstelle von Hashes Inhaltssignaturen zur Prävention verwendet, kann es mit einer einzigen Signatur mehr Malware identifizieren. Deshalb schützt WildFire verglichen mit den meist hashbasierten Systemen, die ein Verhältnis von 1:1 erfordern, mit den gleichen Ressourcen vor mehr Angriffen. Eine einzige WildFire-Signatur kann vor bis zu mehreren Millionen von polymorphen Varianten einer einzigen Malware schützen.

Verhindert schädliches Verhalten im gesamten Netzwerkverkehr

WildFire identifiziert Dateien mit potenziell schädlichem Verhalten und beurteilt sie auf Grundlage ihrer Aktionen, indem neben den innovativen Funktionen auch Bedrohungsinformationen, Analysen und Korrelationen anwendet werden:

- **Durch die vollständige Sichtbarkeit von schädlichem Verhalten** werden Bedrohungen im gesamten Netzwerkverkehr in Hunderten von Anwendungen identifiziert. Dazu zählen u. a. der Webdatenverkehr, E-Mail-Protokolle wie SMTP, IMAP und POP sowie Dateifreigabeprotokolle wie SMB und FTP unabhängig von Ports oder Verschlüsselung.
- **Bei der Analyse des verdächtigen Netzwerkverkehrs** werden alle Netzwerkaktivitäten, die durch eine verdächtige Datei erzeugt werden, überwacht. Hierzu gehören u. a. die Erstellung von Backdoors, das Herunterladen von komplexer Malware, der Besuch von Domänen mit geringer Reputation, die Netzwerkerkundung (Network Reconnaissance) und vieles mehr.
- **Durch die Erkennung dateiloser Angriffe/Skripte** wird festgestellt, ob potenziell bösartige Skripte, wie JScript und PowerShell, das Netzwerk durchqueren. Diese werden dann zur Analyse und Ausführung an WildFire weitergeleitet.

Die leistungsstarken Erkennungs- und Analysefunktionen von WildFire sind nahtlos in zahlreiche Produkte aus dem Portfolio von Palo Alto Networks sowie in führende Partnerlösungen für E-Mail- und Cloud-Plattformen integriert.

Aufdecken neuer Bedrohungen mit einem Verfahren, das mehrere Methoden umfasst und evasiven Angriffen standhält

WildFire geht über die traditionellen Sandboxing-Methoden hinaus, die zur Erkennung unbekannter Bedrohungen in einer Cloud-Analyseumgebung verwendet werden, indem mehrere Verfahren kombiniert werden:

- Die dynamische Analyse beobachtet Dateien bei ihrer Ausführung in einer speziell entwickelten, ausweichsicheren virtuellen Umgebung und ermöglicht dadurch die Erkennung von zuvor unbekannter Malware anhand von Hunderten von Verhaltensmerkmalen.
- **Maschinelles Lernen** extrahiert Tausende einzigartige Merkmale aus jeder Datei und trainiert ein prädiktives maschinelles Lernmodell, um neue Malware zu identifizieren, was durch statische oder dynamische Analyse allein nicht möglich wäre.
- **Statische Analyse** ergänzt die dynamische Analyse durch die wirkungsvolle Erkennung von Malware und ermöglicht die unmittelbare Identifizierung von Malwarevarianten. Die statische Analyse nutzt darüber hinaus das dynamische Entpacken, um Bedrohungen zu analysieren, die versuchen, durch den Einsatz von Verpackungstools unerkannt zu bleiben.

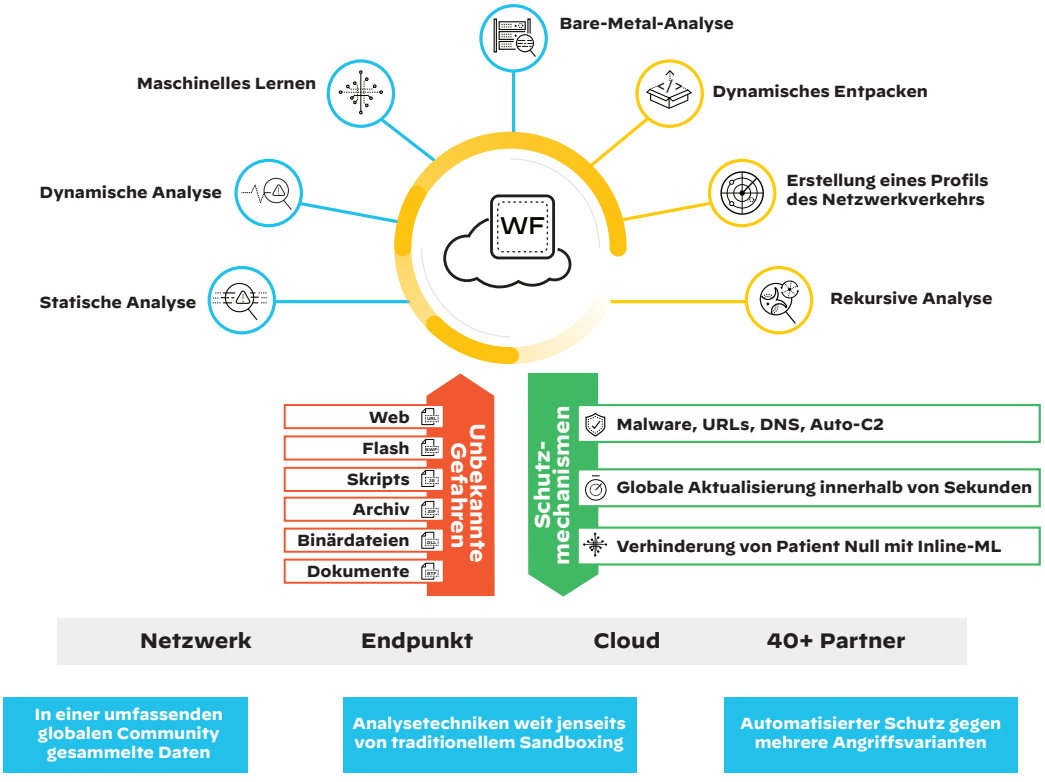

Abbildung 1: WildFire: die globale Zentrale für die Analyse von Malware

- **Bare-Metal-Analyse** führt evasive Bedrohungen in einer realen Hardwareumgebung aus, um die Fähigkeit des Gegners, Anti-VM-Analysetechniken einzusetzen, wirkungslos zu machen.
- **Ein speziell entwickelter, robuster, proprietärer Hypervisor** verhindert Umgehungstaktiken durch Angreifer, indem er keine Open-Source-Projekte oder proprietäre Software nutzt, zu der Angreifer Zugang haben.

Kombiniert ermöglichen diese einzigartigen Methoden WildFire, unbekannte Malware mit hoher Wirksamkeit und nahezu null Fehlalarmen zu analysieren und zu verhindern.

Stoppen komplexer, mehrstufiger Angriffe

Angreifer entwickeln laufend Malware, um bestehende Analysetechniken zu umgehen, indem sie Angriffe in verschiedene Komponenten und Phasen zerlegen, mehrere gleichzeitige Übertragungsvektoren verwenden und seriöse Cloud-Dienste nutzen, um nicht entdeckt zu werden. Aufgrund dieser Strategien wird die herkömmliche einstufige Malwareanalyse mit nur einem Vektor wirkungslos.

Durch die Kombination der Cloud-Skalierbarkeit von WildFire mit erweiterter Dateianalyse und URL-Crawling bietet die Multi-Vector Recursive Analysis (MVRA) eine einzigartige und umfassende Lösung zur Verhinderung der ausgeklügelten mehrstufigen Multi-Hop-Angriffe von Hackern. Im Gegensatz zu anderen Lösungen kann WildFire bei der Dateianalyse mehrere Angriffsphasen verfolgen, selbst wenn die Durchführung in einer bestimmten Phase fehlschlägt. Dieser Workflow ermöglicht die einheitliche Analyse von Web- und Dateiangriffsvektoren und gewährt so eine einzigartige, ganzheitliche Sicht auf einen Angriff über mehrere Phasen hinweg. Angreifer können Schadinhalte nicht mehr hinter mehreren Phasen gutartiger URLs oder seriöser Dokumentenaustausch-Websites verstecken.

Operative Vorteile

- **Automatisierte Neuprogrammierung von Sicherheitskontrollen, um unbekannte Bedrohungen zu blockieren:** Gemeinsam genutzte Echtzeitinformationen von mehr als 35.000 Abonnenten ermöglichen die automatische Aktualisierung und Verhinderung von Bedrohungen auf Netzwerken, Endpunkten und Clouds.
- **Detaillierte Informationen zu den analysierten Bedrohungen:** Erhalten Sie detaillierte Berichte über alle schädlichen Dateien, die an WildFire gesendet werden. Unterstützt werden zahlreiche Betriebssystemumgebungen und Anwendungsversionen.
- **Nahtlose Integration mit bestehenden Sicherheitstools:** Nutzen Sie die offene API-Integration mit SIEM-, TIP-, Ticketing-, SOAR- oder XDR-Tools, um Kompromissindikatoren (IOCs) zu verarbeiten.
- **Verwertbare Erkenntnisse über Bedrohungen:** Zusammen mit der kontextbezogenen Bedrohungsanalyse AutoFocus™ können Sie Angreifer und ihre Absichten verstehen und Kampagnen verfolgen, um sicherzustellen, dass Sie die richtigen Schritte setzen.

Einsatz in einer sicheren, skalierbaren cloudbasierten Architektur

Die cloudbasierte Architektur von WildFire unterstützt in großem Maßstab die Analyse und Prävention unbekannter Bedrohungen auf Netzwerken, Endpunkten und Clouds. Die Dateien werden an die globale WildFire-Cloud übermittelt, wodurch Skalierbarkeit und hohe Geschwindigkeit gewährleistet sind. Alle Kunden von Palo Alto Networks können den Dienst schnell aktivieren, einschließlich der Benutzer von Hardware und virtuellen ML-basierten NGFWs, öffentlichen Cloud-Angeboten, Prisma™ SaaS und CCortex XDR™-Agenten. Palo Alto Networks verwaltet die WildFire-Infrastruktur direkt. Das Unternehmen folgt dabei den branchenüblichen Best Practices für Sicherheit und Vertraulichkeit und führt regelmäßige SOC 2-Konformitätsprüfungen durch. Weitere Informationen finden Sie im WildFire-Datenblatt zum Datenschutz.

Um Bedenken hinsichtlich der Datenhoheit und des Datenschutzes auszuräumen, betreiben wir verteilte regionale WildFire-Clouds, die Ihnen mehr Kontrolle über den Speicherort Ihrer Daten geben. Diese Clouds bieten dieselben Erkennungs- und Präventionsfunktionen wie die öffentliche WildFire-Cloud und ermöglichen es Ihnen, Übermittlungen an lokale Datenschutzanforderungen anzupassen.

Integrierte Protokollierung, Berichterstattung und Forensik

WildFire-Benutzer erhalten integrierte Protokolle, Analysen und Einblicke in böswillige Ereignisse über die PAN-OS-Verwaltungsoberfläche, das Netzwerksicherheitsmanagement Panorama™, über AutoFocus, Cortex XDR, Cortex™ XSOAR oder das WildFire-Portal, sodass Teams die in ihren Netzwerken beobachteten Ereignisse schnell untersuchen und zuordnen können. Mit diesen Informationen können Sicherheitsteams unabhängig von der verwendeten Anwendung die Daten, die für zeitnahe Ermittlungen und die Reaktion auf Vorfälle benötigt werden, schnell lokalisieren und entsprechende Maßnahmen ergreifen.

Die Leistungen der Palo Alto Networks-Sicherheitsabonnements

In letzter Zeit haben Cyberangriffe an Umfang und Komplexität zugenommen, wobei fortschrittliche Methoden zur Umgehung von Netzwerksicherheitsgeräten und -tools verwendet werden. Dies stellt Unternehmen vor die Herausforderung, ihre Netzwerke zu schützen, ohne die Arbeitslast der Sicherheitsteams zu erhöhen oder die Produktivität des Unternehmens zu verringern. Unsere cloudbasierten Sicherheitsabonnements, die nahtlos in die branchenweit erste ML-basierte NGFW-Plattform integriert sind, koordinieren die Informationen und bieten Schutz gegen alle Angriffsvektoren, verfügen über erstklassige Funktionalität und eliminieren gleichzeitig die Lücken, die durch separate Netzwerksicherheitstools entstehen. Nutzen Sie die Vorteile marktführender Funktionen mit der langjährigen Erfahrung einer Plattform, und schützen Sie Ihr Unternehmen vor selbst den fortschrittlichsten und evasivsten Bedrohungen. Profitieren Sie von WildFire oder einem unserer Sicherheitsabonnements:

- **Abwehr von Bedrohungen:** Gehen Sie über herkömmliche IPS-Lösungen (Intrusion Prevention System) hinaus und verhindern Sie automatisch alle bekannten Bedrohungen des gesamten Datenverkehrs in einem einzigen Verfahren.
- **URL-Filtering:** Ermöglichen Sie die sichere Nutzung des Internets, indem Sie den Zugang zu bekannten und neuen schädlichen Websites verhindern, bevor sie von Benutzern aufgerufen werden können.
- **DNS-Sicherheit:** Vereiteln Sie Angriffe, die DNS für Command-and-Control-Bedrohungen und Datendiebstahl nutzen, ohne dass Änderungen an Ihrer Infrastruktur erforderlich sind.
- **IoT-Sicherheit:** Schützen Sie IoT-(Internet-of-things-) und OT-Devices in Ihrem Unternehmen mit der ersten einsatzbereiten IoT-Sicherheitslösung der Branche.
- **GlobalProtect™-Netzwerksicherheit für Endpunkte:** Erweitern Sie die ML-basierten NGFW-Funktionen auf Ihre Remotebenutzer, um überall in Ihrer Umgebung konsistente Sicherheit zu gewährleisten.

Tabelle 1: Funktionen und Lizenzierung	
Mit einem WildFire-Abonnement aktivierte Funktionen	
Erweiterte Analyse, Prävention und Anti-Evasion-Verfahren	**Statische Analyse** – kombiniert Speicheranalyse, maschinelles Lernen und Analyse von Dateianomalien, schädliche Muster und bekannte schädliche Codes. **ML-basierte Inline-Prävention (an der Firewall)** – blockiert unbekannte schädliche ausführbare Dateien und PowerShell-Angriffe. **Dynamische Analyse** – beinhaltet einen speziellen Hypervisor, Verhaltensscoring, Netzwerkprofiling und Mehrversionsanalyse. **MVRA** – kombiniert erweiterte Dateianalyse mit URL-Crawling zur Verhinderung mehrstufiger Multi-Hop-Angriffe. **Bare-Metal-Analyse** – ermöglicht eine vollständige dynamische Analyse auf der Hardware, ohne virtuelle Umgebung und ohne Hypervisor.
Unterstützte Betriebssysteme	macOS, Android, Windows XP/7/10
Unterstützte Dateien	PE-Dateien (EXE, DLL und andere), alle Microsoft-Office-Dateitypen, Mac OS X-Dateien, Linux-Dateien (ELF), Android Package Kit-Dateien (APK), Adobe Flash- und PDF-Dateien, Archivdateien (RAR und 7-Zip), Skriptdateien (BAT, JS, VBS, PS1, Shell Script und HTA), Analyse von Links in E-Mail-Nachrichten und verschlüsselte Dateien (TLS/SSL).
Unterstützte Protokolle	SMTP, POP3, SMB, FTP, IMAP, HTTP, HTTPS
Dateianalyse pro Tag	Elastisch
Signaturtyp	• Auf der Basis von neuer/Zero-Day-Malware beim Webdatenverkehr (HTTP/HTTPS), in E-Mail-Protokollen (SMTP, IMAP und POP) und beim FTP-Datenverkehr. • Auf der Malware-Payload des Musters generiert und auf Genauigkeit und Sicherheit getestet
Sicherheitsupdates für unbekannte Malware	• Sekunden, mit Zero-Delay-Signaturen an die verbundene Next-Generation Firewall.*
Regionale Cloud-Standorte	• Nordamerika (2; global und regional), Amsterdam, Singapur und Japan.
Schlüsselintegrationen	• Mit Palo Alto Networks, einschließlich aller aus der Cloud bereitgestellten Sicherheitsabonnements, AutoFocus, Cortex XDR und Prisma SaaS. • Mit Technologiepartnern zur Entscheidungsfindung über Dienste Dritter mit der WildFire-API
Management und Reporting	• Palo Alto Networks Panorama und WebUI, API
Forensik	• Detaillierte Analyse aller an WildFire gesendeten schädlichen Dateien in verschiedenen Betriebssystemumgebungen, einschließlich host- und netzwerkbasierter Aktivitäten • Zugriff auf das Originalmalwaremuster für Reverse Engineering, mit vollständigen PCAPs von dynamischen Analysesitzungen. • Offene API für die Integration mit Sicherheitstools von Drittanbietern, wie z. B. Sicherheitsinformations- und Ereignisverwaltungssystemen (SIEMs).
Vertraulichkeit und Datenschutz	• Palo Alto Networks verfügt über strenge Datenschutz- und Sicherheitskontrollen, um unbefugten Zugriff auf sensible oder persönlich identifizierbare Informationen zu verhindern. Wir wenden branchenübliche Best Practices für Sicherheit und Vertraulichkeit an. Zusätzliche Informationen finden Sie in unseren Datenblättern zum Datenschutz.

Tabelle 1: Funktionen und Lizenzierung (Fortsetzung)	
Lizenzierung und Anforderungen	
Anforderungen	Zur Nutzung des Abonnements von Palo Alto Networks WildFire benötigen Sie Folgendes: • Palo Alto Networks Next-Generation Firewalls mit PAN-OS • Palo Alto Networks Threat Prevention-Lizenz
Vollständige WildFire-Lizenz	WildFire erfordert eine Stand-alone-Lizenz, die als integriertes, cloudbasiertes Abonnement für Palo Alto Networks Next-Generation Firewalls bereitgestellt wird. Sie ist auch im Rahmen der Palo Alto Networks Subscription ELA, der VM-Series ELA oder Prisma Access erhältlich.
Empfohlene Umgebungen	Palo Alto Networks Next-Generation Firewalls, die an beliebigen Standorten eingesetzt werden, da sowohl interne als auch externe Quellen dateibasierte Bedrohungen in das Netzwerk einbringen können.
Allgemeine WildFire-Lizenz	Die grundlegende WildFire-Funktionalität ist als Teil der Palo Alto Networks Next-Generation Firewall mit einem eingeschränkten Satz von Funktionen enthalten und ermöglicht ausschließlich: • Weiterleitung von EXE- und DLL-Dateitypen, einschließlich komprimierter und verschlüsselter Inhalte (nur Windows XP/7) für die WildFire-Analyse. • Abruf von WildFire-Signaturen über Antivirus- und/oder Threat Prevention-Updates. • Automatische Aktualisierungen alle 24 bis 48 Stunden bei aktivem Threat Prevention-Abonnement (ohne Unterstützung von Inline-Prävention auf der Basis von maschinellem Lernen und verzögerungsfreien Signaturen).

* Erfordert PAN-OS 10.0.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1 408 75 34 000
Vertrieb: +1 866 32 04 788
Support: +1 866 898 9087

www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks ist eine eingetragene Marke von Palo Alto Networks. Eine Liste unserer Marken ist unter https://www.paloaltonetworks.com/company/trademarks.html abrufbar. Alle anderen in diesem Dokument erwähnten Marken sind Eigentum der jeweiligen Unternehmen. wildfire-ds-061220