Panda Adaptive Defense 360 Technologien

Starke Erkennung, zuverlässige Bekämpfung

Panda Adaptive Defense 360

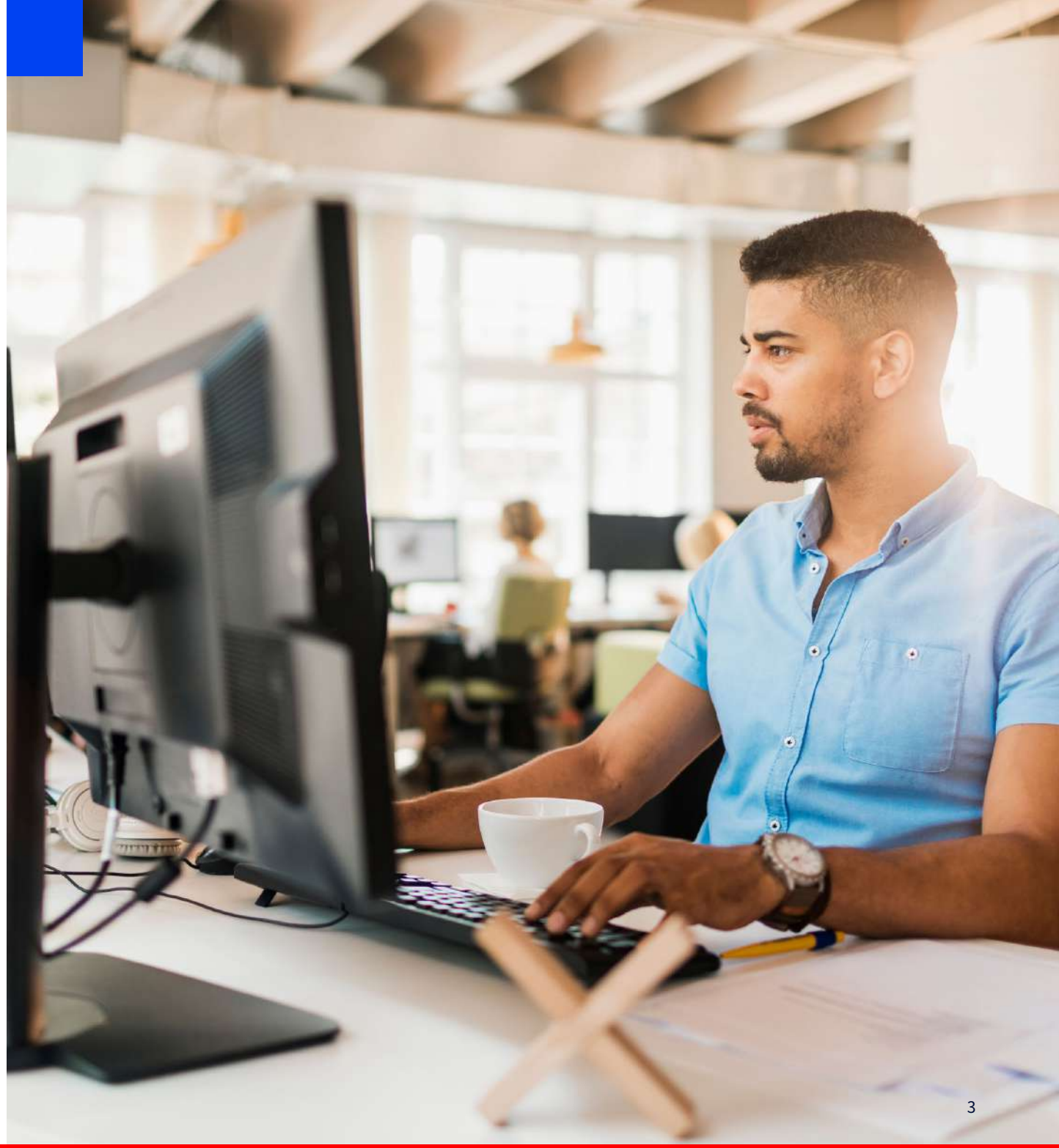
Index

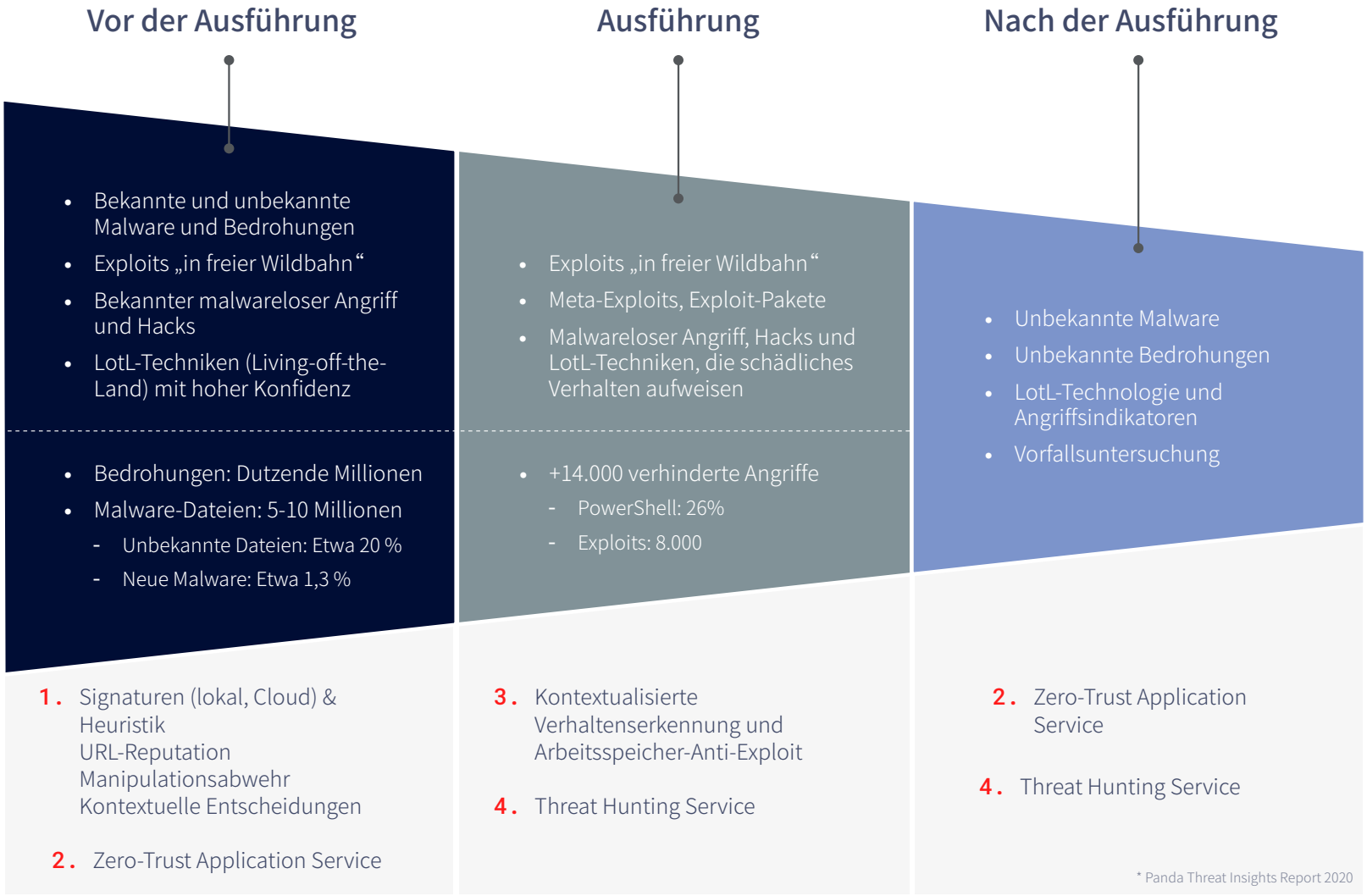
Technologien und Dienste von Panda Adaptive Defense 360

Einführung

In diesem Dokument wird erläutert, wie die **Technologien und Dienste von Panda Adaptive Defense 360** zusammenarbeiten. Die EDR-Fähigkeiten (Endpoint Detection and Response) und die Nutzung von künstlicher Intelligenz sind die Alleinstellungsmerkmale.

Im folgenden Diagramm ist dargestellt, wo jede Technologie arbeitet und mit welchen Techniken Angreifer so schnell wie möglich blockiert wird, wodurch Angriffe auf Endpoints abgewehrt werden und Angreifer erkannt, eingedämmt und abgewehrt werden, bevor Schaden angerichtet wird.





Folgende Hauptgruppen an Vorbeugungs-, Erkennungs- und Abwehrtechnologien und Dienste sind in Panda Adaptive Defense 360 integriert:

1. **Pandas vollständiger Endpoint Protection-Technologiestack**
2. **Zero-Trust Application Service**
3. **Kontextbezogene Verhaltenserkennung und Arbeitsspeicher-Anti-Exploit**
4. **Threat Hunting Service**

In diesem E-Book betrachten wir, wie diese Technologien zusammenarbeiten, um **mit minimalem Aufwand mehr Schutz zu bieten**.

1. Vollständiger EPP-Technologiestack (Endpoint Protection)

Proaktiver EPP-Technologiestack	Panda Adaptive Defense 360
Generelle Signaturen und Heuristiken	✓
Cloudbasierte Suche in Collective Intelligence (Bedrohungsinformationen)	✓
Verhaltensanalyse und IoA-Erkennung (Indicators of Attack, Angriffsindikatoren)	✓
Firewall, Intrusion Detection (IDS)/Intrusion Prevention (IPS), Netzwerkpaket-Inspektion	✓
Manipulationsabwehr	✓
Gerätesteuerung	✓
URL-Reputation	✓
Anwendungskontrolle	✓
Anti-Spam, Anti-Phishing, Inhaltsfilterung für MS Exchange-Server	✓
Mailbox-Schutz und Scan für MS Exchange-Server	✓
Schwachstellenanalyse und Patch-Management*	✓

*Panda Patch Management

Ein häufiges Missverständnis bei EPP-Technologien ist, dass es sich hierbei nur um herkömmliche, signaturbasierte Antivirus-Programme handelt, die durch beliebige EDR-Lösungen ersetzbar sind.

Tatsächlich verhält es sich so, dass diese Technologien neben der signaturbasierten Analyse auch generische Signaturen, Heuristiken, Firewall, URL-Reputation, kontextuelle Entscheidungen, Schwachstellenmanagement, Anwendungskontrolle und weitere Funktionen kombinieren, die eine erhebliche Risikominderung erzielen können.

Mit diesen Präventionstechnologien, die mit EDR-Lösungen zusammenarbeiten, gehen erhebliche Vorteile einher, darunter:

- **Erhebliche Risikominderung.** Zur Erkennung von Malware muss keine Datei ausgeführt werden, und es ist nur eine Internetverbindung zur Abfrage der Cloud erforderlich.
- **Sehr geringe Anzahl falsch positiver Treffer.** EPP-Technologien, die autonomen Schutz bieten können, werden breit auf einer großen Anzahl von Endpoints eingesetzt, und können auf minimale falsch positive Treffer konfiguriert werden.
- **Leistungsoptimierung.** Die Technologien arbeiten integriert zusammen, um Redundanz zu vermeiden und die Leistungsbeeinträchtigung der geschützten Endpoints zu minimieren.

2. Zero-Trust Application Service

KI als disruptive Innovation in der Sicherheit

Ein Managed Service ist im Rahmen der Lizenz von **Panda Adaptive Defense und Adaptive Defense 360** enthalten. Dieser Dienst klassifiziert Dateien als Malware oder vertrauenswürdig und lässt nur die Ausführung vertrauenswürdiger Dateien auf Endpoints zu. Da es sich um einen vollständig automatisierten Dienst handelt, erfordert er keine Eingabe oder Entscheidungen vom Endanwender oder den Sicherheits- oder IT-Teams.

Der Zero-Trust Application Service verfügt über drei Schlüsselkomponenten:

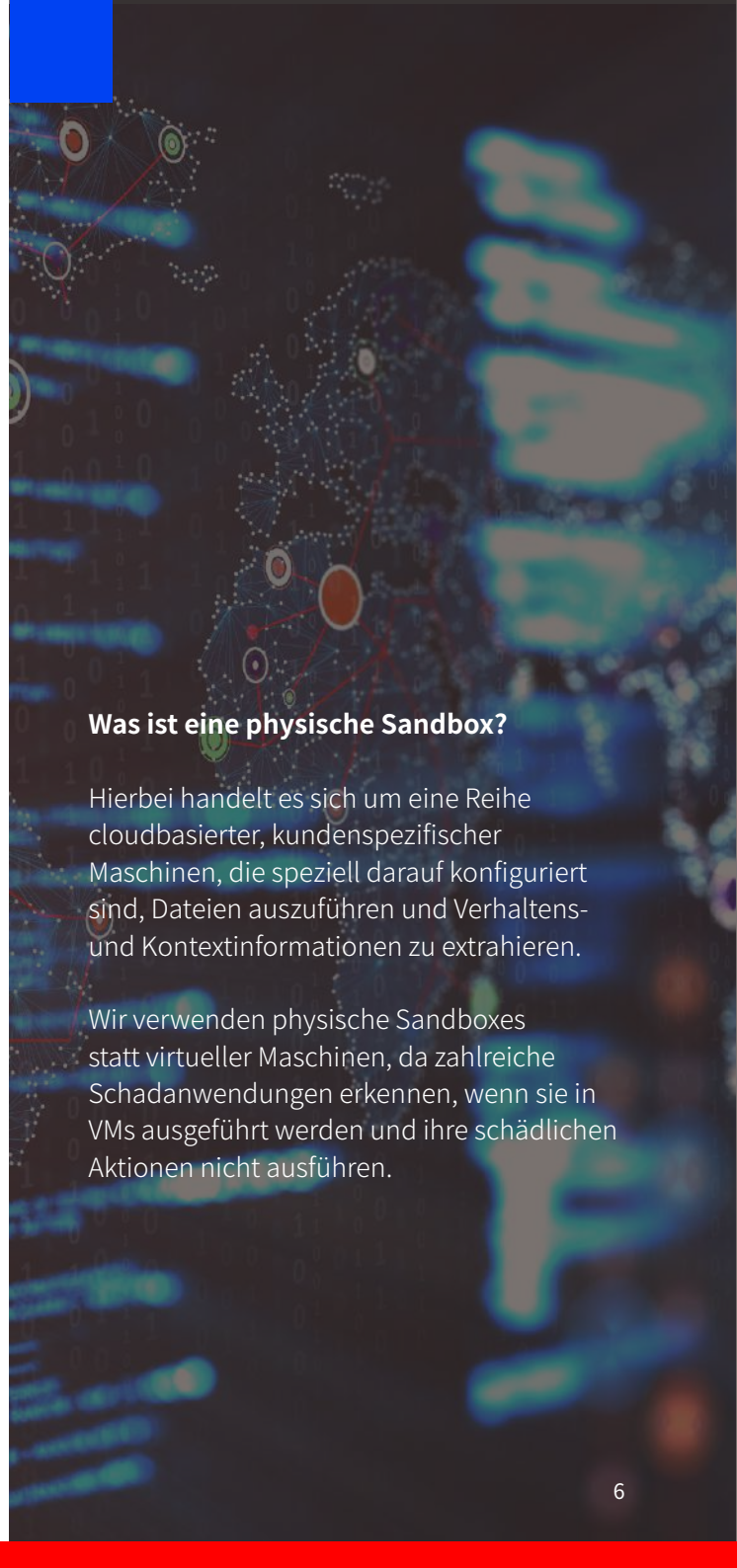
1. **Kontinuierliche Überwachung der Endpoint-Aktivität über eine cloudnative Plattform.**

   Kontinuierliche Überwachung der Endpoint-Aktivität über eine cloudnative Plattform. Die Aktivität jeder Anwendung am Endpoint, unabhängig ihrer Natur, wird überwacht und zur kontinuierlichen Klassifizierung an die Cloud gesendet. So können Malware-Ausführungen und selbst hochentwickelte Bedrohungen wie Supply-Chain-Angriffe verhindert werden.

2. **Automatisierte, KI-basierte Klassifizierung.**

   Automatisierte Klassifizierungen werden über ein cloudbasiertes KI-System vorgenommen, in dem eine Reihe von Machine-Learning-Algorithmen (ML) ausgeführt wird, die Hunderte statischer Attribute sowie Verhaltens- und Kontextattribute in Echtzeit verarbeiten. Die Attribute werden aus der Telemetrie der geschützten Umgebung und einem Satz **physischer Sandboxes**, in denen ausführbare Dateien ausgeführt werden, extrahiert.

Die Rate der automatisierten Klassifizierung beträgt heute 99,98 %; nur 0,02 % aller Prozesse benötigen Eingriffe durch unsere Experten. Das KI-Klassifizierungssystem ist daher eigenständig, auf große Dateivolumen skalierbar, arbeitet in Echtzeit und benötigt keine Eingaben vom Endanwender.



Was ist eine physische Sandbox?

Hierbei handelt es sich um eine Reihe cloudbasierter, kundenspezifischer Maschinen, die speziell darauf konfiguriert sind, Dateien auszuführen und Verhaltens- und Kontextinformationen zu extrahieren.

Wir verwenden physische Sandboxes statt virtueller Maschinen, da zahlreiche Schadanwendungen erkennen, wenn sie in VMs ausgeführt werden und ihre schädlichen Aktionen nicht ausführen.

3. Risikobasierte Anwendungskontrolle.

Bezieht sich auf die Betriebsmodi des Protection-Agents, der auf den Endpoints ausgeführt wird. Es gibt zwei Schutzebenen:

- **Hardening-Modus:** Unbekannte Anwendungen oder Binärdateien mit externer Quelle (Web-Downloads, E-Mail, Wechseldatenträger, Remote-Standorte usw.) werden standardmäßig abgelehnt.

- **Lock-Modus:** Unbekannte Anwendungen oder Binärdateien werden unabhängig von der Quelle (aus dem Netzwerk, innerhalb des Endpoint oder extern) standardmäßig abgelehnt. Dies stellt sicher, dass alle laufenden Prozesse vertrauenswürdig sind.

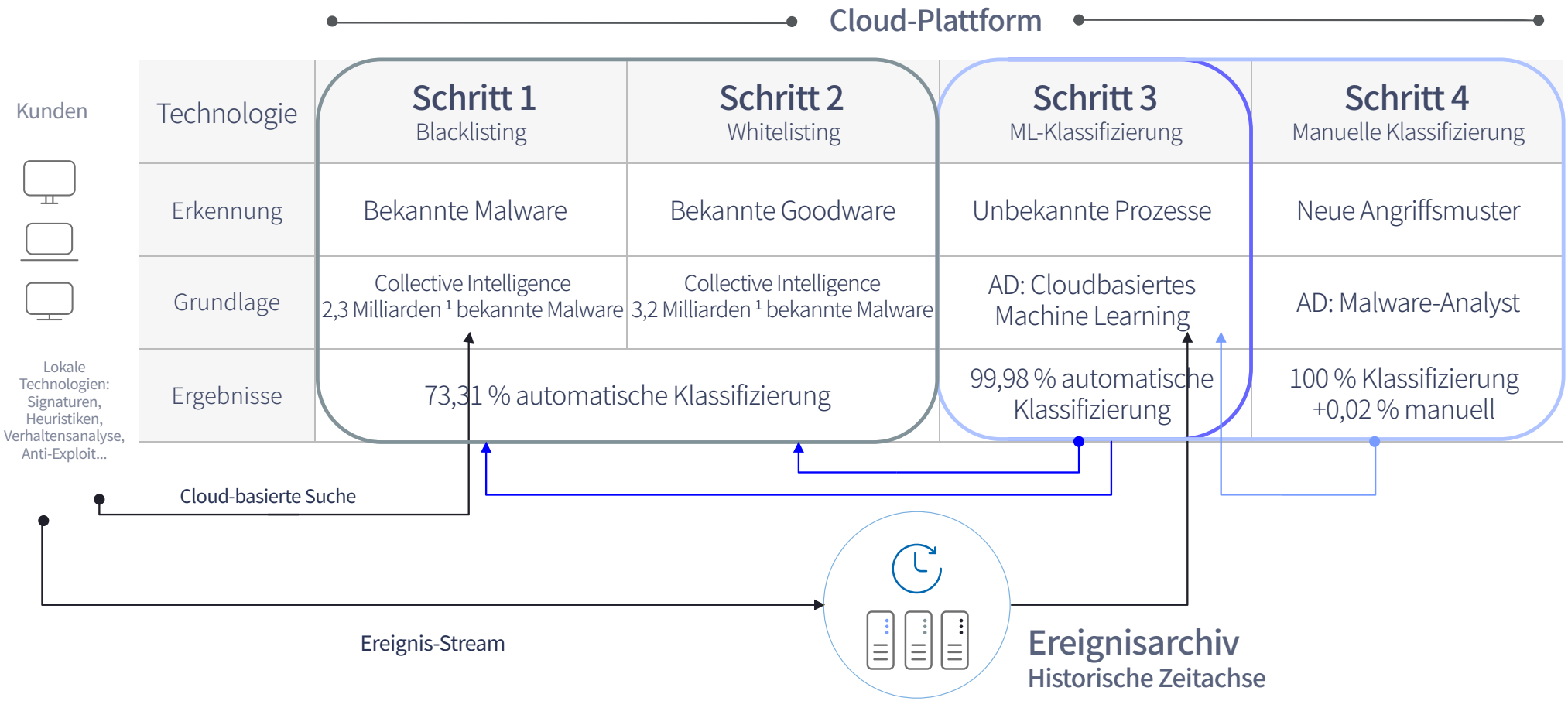
Panda Security Collective Intelligence.
Diese Schlüsselkomponente wird auf einer cloudbasierten Plattform gehostet und ermöglicht das neue Schutzmodell, das die Effizienz des Zero-Trust Application Service steigert.

Collective Intelligence umfasst das zusammengefasste, inkrementelle Wissens-Repository aller Anwendungen, Binärdateien und anderen Dateien mit interpretiertem Quellcode, sowohl vertrauenswürdig als auch schädlich.

Dieses Cloud-Repository wird kontinuierlich vom KI-System und Sicherheitsexperten mit Informationen versorgtund zugleich von den Lösungen und Diensten von Panda Security vor jeder Ausführung abgefragt.

- Das folgende Diagramm stellt dar, wie die Technologien des Stacks nahtlos zusammenarbeiten und so eine Klassifizierung aller Anwendungen, Binärdateien und Dateien mit interpretiertem Quellcode in Echtzeit ermöglichen.

Funktionsweise des Zero-Trust Application Service



3. Kontextbezogene Verhaltenserkennung und Arbeitsspeicher-Anti-Exploit

Die kontinuierliche Überwachung der Endpoint-Aktivität ermöglicht es dem Agent, als Sensor zu fungieren und die Cloud-Plattform darüber zu informieren, welche Dateien ausgeführt werden und in welchem Kontext (was vor der Ausführung geschehen ist, welche Anwender welche Anwendung oder welchen Befehl ausführen, welcher Netzwerk-Traffic erzeugt wird, auf welche Dateien zugegriffen wird, welche Parameter vorliegen usw.).

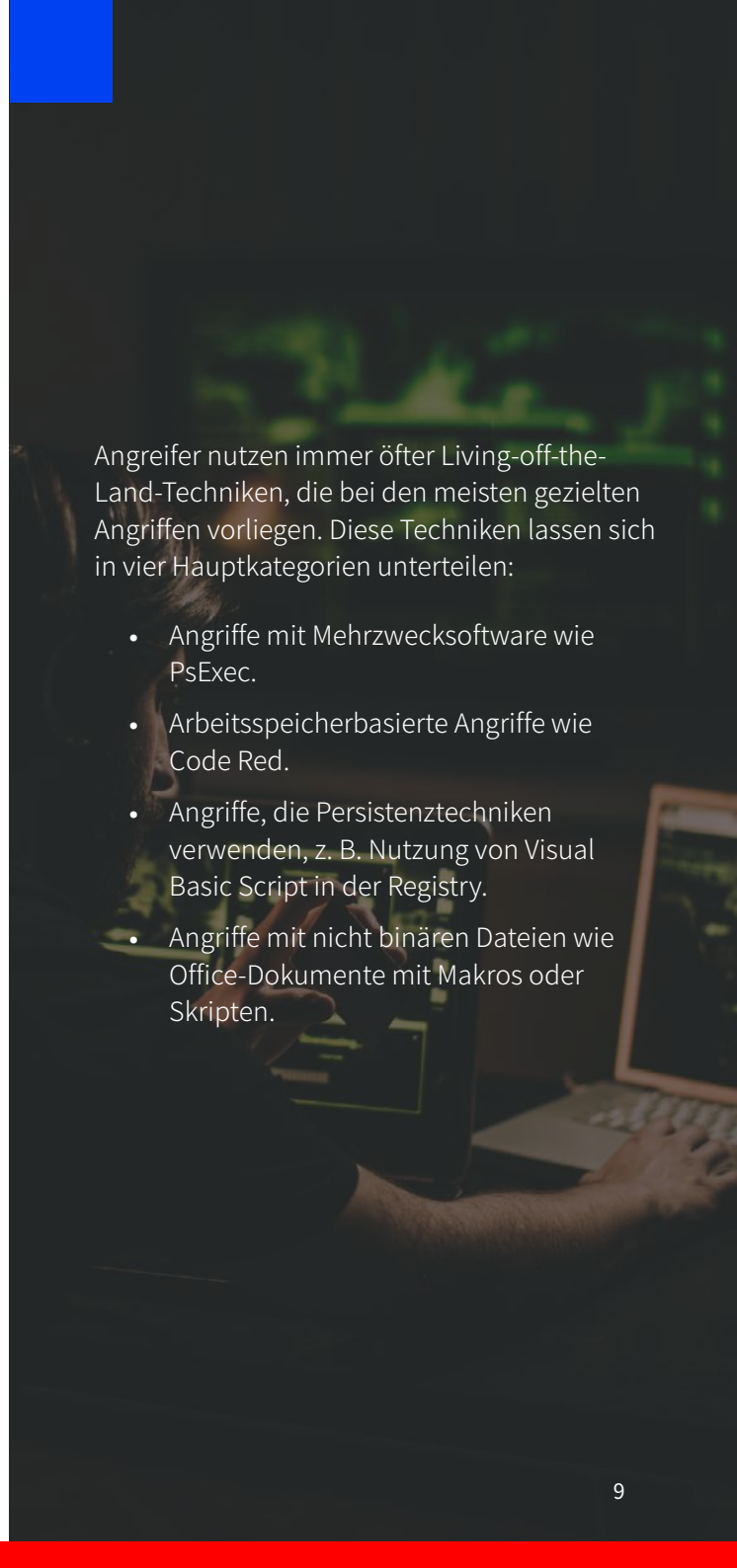
Dies ermöglicht eine Erkennung von abnormalem oder verdächtigem Verhalten am Endpoint und die Kategorisierung als Angriffsindikatoren (IoA) mit hohem Konfidenzniveau und ohne falsch positive Treffer.

Oft stehen IoAs mit bestimmten Phasen der **Cyber Kill Chain** oder den Taktiken des **MITRE ATT&CK Framework** in Zusammenhang[1]:

- Erster Zugriff
- Ausführung
- Persistenz
- Erlangung zusätzlicher Berechtigungen
- Umgehen der Verteidigung
- Zugriff auf Zugangsdaten
- Entdeckung
- Laterale Bewegung
- Erfassung
- Command and Control
- Exfiltration
- Wirkung

Die Erkennung von IoAs vor einer Daten-Exfiltration (oder Verschlüsselung bei einem Ransomware-Angriff) ist ein sehr wirksamer Verteidigungsmechanismus, insbesondere gegen LotL-Angriffe (Living-off-the-Land), selbst wenn Endpoints bereits beeinträchtigt sind.

Panda Adaptive Defense und Panda Adaptive Defense 360 umfassen im Protection-Agent einen vollständigen Technologiestack zur Erkennung von IoAs in verschiedenen Angriffsphasen. Es handelt es sich hierbei um keine statische Technologie: Vielmehr werden die Technologien kontinuierlich mit neuen, vom Threat Hunting and Investigation Service (THIS) entdeckten Angriffsmustern und Techniken aktualisiert.



Angreifer nutzen immer öfter Living-off-the-Land-Techniken, die bei den meisten gezielten Angriffen vorliegen. Diese Techniken lassen sich in vier Hauptkategorien unterteilen:

- Angriffe mit Mehrzwecksoftware wie PsExec.
- Arbeitsspeicherbasierte Angriffe wie Code Red.
- Angriffe, die Persistenztechniken verwenden, z. B. Nutzung von Visual Basic Script in der Registry.
- Angriffe mit nicht binären Dateien wie Office-Dokumente mit Makros oder Skripten.

Unter den zahlreichen Angriffsindikatoren, die der Agent erkennt, finden sich die folgenden Kategorien:

1. Angriffsindikatoren von Exploits „in freier Wildbahn“

Über diese Verhaltens- und Kontext-Angriffsindikatoren lassen sich Exploits „in freier Wildbahn“ ebenso wie Exploit-Pakete erkennen und vor der Ausführung blockieren, was einen der Hauptvektoren für Angreifer schließt.

Zudem erkennt die proprietäre „**Virtual Patching**“-Firewalltechnologie durch Überwachung des eingehenden Traffics Versuche zur Ausnutzung von Schwachstellen und blockiert diese.

Beispielsweise lässt sich diese Technologie nutzen, um Exploits der BlueKeep-Schwachstelle zu erkennen und zu blockieren; hierbei werden während einer RDP-Sitzung bestimmte Verbindungen aufgebaut. Werden diese Verbindungen nicht blockiert, erlauben sie es einem Angreifer, Code aus der Ferne auszuführen (RCE, Remote Code Execution).

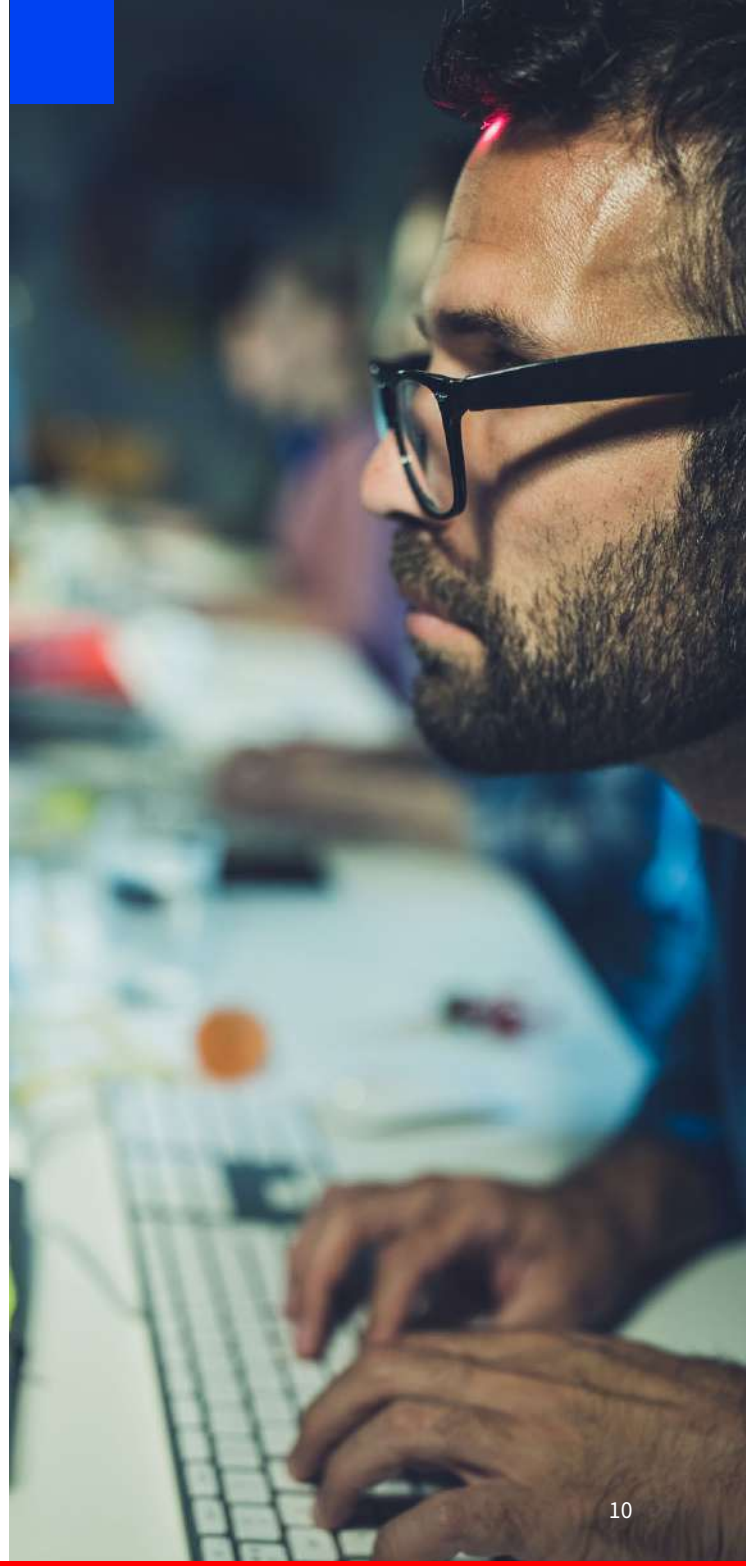
Die Virtual Patching-Technologie erkennt derartige Verbindungen und lehnt sie automatisch ab. Erkennungen werden in der Cloud aufgezeichnet und in der Web-Benutzeroberfläche von Panda Adaptive Defense 360 dargestellt, wodurch Administratoren sofort eingreifen können.

Sie können zur Eindämmung Konfigurationsänderungen vornehmen und beispielsweise NLA (Network Level Authentication) aktivieren oder nicht wesentliche RDP-Dienste an den Endpoints deaktivieren, die Systeme patchen, so möglich, und so effektiv die Angriffsoberfläche reduzieren.

2. Arbeitsspeicher-Angriffsindikatoren: Dynamische Anti-Exploit-Technologie

Panda Adaptive Defense 360 umfasst dynamische Anti-Exploit-Technologie.

Diese Technologie, die in Panda Adaptive Defense 360 integriert wurde, ist von den Microsoft EMET Technologien unabhängig und basiert weder auf einer morphologischen Dateianalyse noch auf zusätzlichen Schutzmaßen vor nicht von Windows abgedeckten Exploit-Techniken (ASR, EP, EAF usw.), oder auf spezifischer Erkennung bekannter Schwachstellen. Diese Techniken reichen nicht aus, um Angriffe auf Zero-Day-Schwachstellen aufzuhalten.



Die dynamische Anti-Exploit-Technologie überwacht das interne Verhalten von Prozessen und sucht nach Anomalien. Dies ist hochgradig wirksam, unabhängig von dem beim Angriff verwendeten Exploit, und wird durch eine proprietäre **Arbeitsspeicher-Frameworkanalyse** ergänzt, bei der ein Arbeitsspeicherabschnitt zu bestimmten Zeitpunkten nach Auslösung bestimmter Ereignisse oder Verhaltensweisen untersucht wird. So können neue Angriffsmuster mit verschiedenem Typ erkannt werden.

Diese Technologien bieten einen wirksamen Schutz vor allen Arten von Exploits, insbesondere Zero-Day-Exploits, die folgendes anzielen:

- **Schwachstellen in Webbrowsern:** Internet Explorer, Firefox, Chrome, Opera und weitere Browser

- **Gebräuchliche Anwendungen,** die oft das Ziel von Angriffen sind, wie Java, Adobe Reader, Adobe Flash, Microsoft Office, Multimedia-Player usw.

- **Schwachstellen in nicht unterstützten Betriebssystemen** wie Windows XP und weitere.

3. Angriffsindikatoren zur Erkennung von Living-off-the-Land-Angriffen und schädlicher Nutzung von Administratortools

Um diesen Typ von Indikator zu erkennen, werden von Skripte-Interpretern ausgeführte Skripte korreliert (PowerShell, Visual Basic, Javascripts usw.), ebenso Makros/Skripte in MS Office, WMI-Aktivität usw.

Weitere Indikatoren dienen zur Ablehnung der Ausführung bestimmter Prozesse durch andere Prozesse und je nach Kontext zum Blockieren von malwarelosen Angriffen mittels Administrator-Tools und Befehlszeilensequenzen. Zudem werden einige weitere Arbeitsspeicher-Angriffe erkannt, wie Code Injections in den Arbeitsspeicher, bei denen keine Dateien auf der Festplatte vorliegen.

4. Threat Hunting Service

Das Unsichtbare enthüllen

Der Threat Hunting and Investigation Service, der Teil von Panda Adaptive Defense und Panda Adaptive Defense 360 ist, wird vollständig von den Analysten von Panda Security verwaltet und betrieben.

Die Experten betreiben eine cloudnative, proprietäre Threat Hunting and Incident Response-Plattform zur Koordination von L1-, L2- und L3-Analysten sowie Threat Huntern und Incident Respondern, um die MTTD und MTTR (Mean Time To Detect/Mean Time To Respond, mittlere Zeit bis zur Erkennung/Reaktion) zu minimieren.

Zudem können Analysten neue Regeln für neue Angriffsindikatoren festlegen. Diese Angriffsindikatoren mit hohem Konfidenzniveau können auf die Endpoints aufgespielt werden und schützen auf diese Weise so früh wie möglich vor Angreifern, die mittels Techniken wie dateilosen Angriffen, LotL usw. andere Maßnahmen umgehen.

Diese neuen Angriffsindikatoren sind das Ergebnis eines kontinuierlichen Prozesses zur Erkennung von Bedrohungen mittels hochentwickelter Datenanalyse, unseren firmeneigenen Bedrohungskenntnissen und dem Fachwissen unserer Analysten.

Dieser Dienst umfasst die Cyber Intelligence, die wir aus jahrelanger Erfahrung im Bereich Bedrohungsforschung gewonnen haben, kombiniert mit der historischen Transparenz, die das Register des Verhaltens von Anwendungen, Anwendern und Maschinen über mehr als 30 Jahre hinweg bietet und unseren Allianzen mit internationalen Organisationen wie der Cyber Threat Alliance, in der wir Angriffs- oder Schadensindikatoren und Abwehrmethoden austauschen.

Zertifizierungen, Auszeichnungen und Beiträge

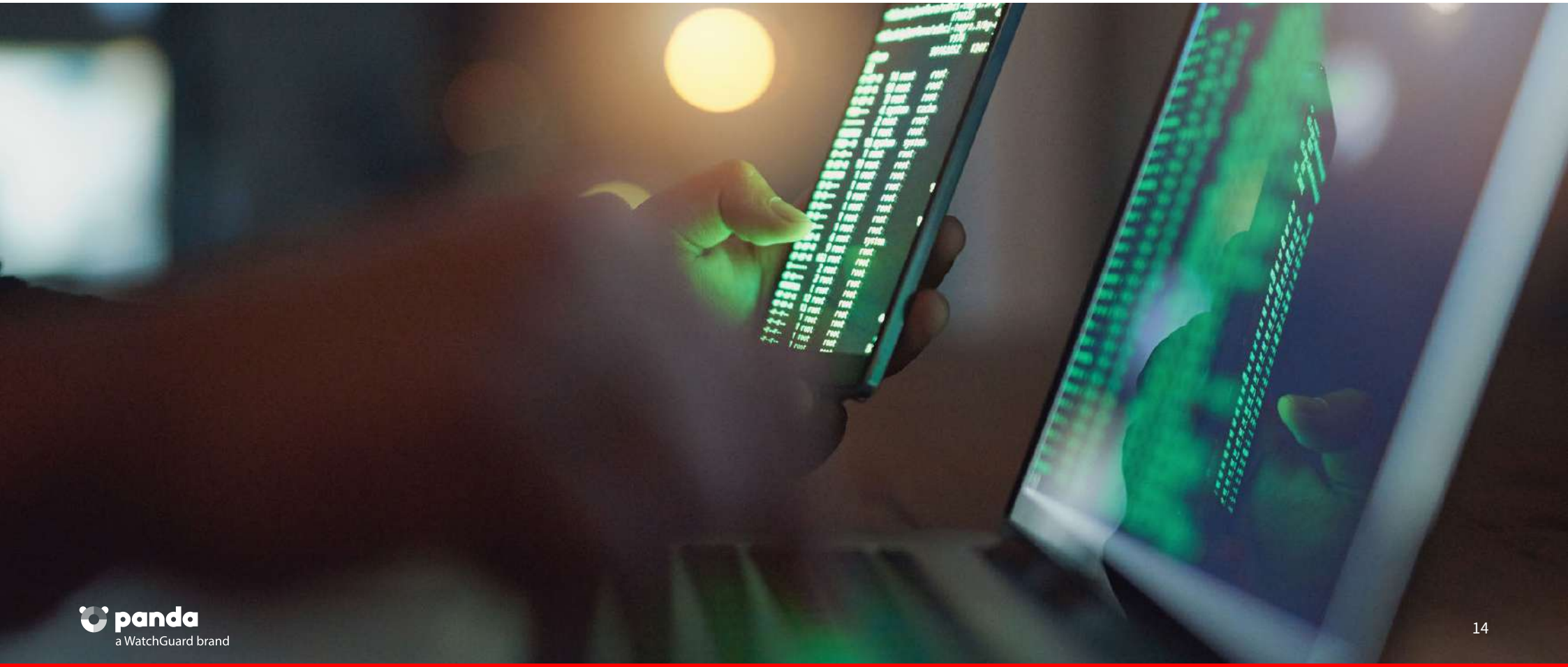
Panda Security nimmt regelmäßig an Analyse-Wettbewerben von Virus Bulletin, AV-Comparatives, AV-Test und NSSLabs teil und hat bereits mehrere Auszeichnungen für Sicherheit und Leistung erhalten. Panda Adaptive Defense erhielt die Zertifizierung EAL2+ in Rahmen der Prüfung für den Common Criteria Standard.

BEITRAGENDES MITGLIED

Hinweise

1. Angriffe auf die Lieferkette sind eine neue Bedrohung, die auf Entwickler und Softwareanbieter zielt. Das Ziel liegt darin, auf Quellcode zuzugreifen, Prozesse zu erstellen oder Aktualisierungsmechanismen zu beeinträchtigen, indem legitime Anwendungen infiziert werden, um Malware zu verteilen.

2. MITRE ATT&CK Framework: **https://attack.mitre.org/**



Panda Adaptive Defense 360

Grenzlose Sichtbarkeit, absolute Kontrolle

VERTRIEB DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.com/de | pandasecurity.com