Betriebliche Effizienz für moderne Endpoint-Sicherheit

> Intelligenter arbeiten, schneller reagieren.

INHALTSVERZEICHNIS

01 Einführung

Eine unbequeme Wahrheit: Die Beurteilung einer Sicherheitslösung anhand der Anzahl der von ihr generierten Sicherheitswarnungen führt zu einer **mangelhaften betrieblichen Effektivität.**

Nicht weil die Erkennung von Bedrohungen unwichtig ist, sondern weil diese Metriken ohne Kontext irreführend sind.

Eine Flut von Signalen ohne Kontext ist kein Schutz, sondern führt zu einem **Übermaß an Benachrichtigungen**. Durch zu viele unwichtige Benachrichtigungen verschwenden Analysten wertvolle Zeit, das Wesentliche wird verschleiert und Angreifer werden oftmals nicht entdeckt.

In diesem E-Book wird eine bessere Metrik vorgestellt: die **betriebliche Effizienz.** Das ist die Fähigkeit, Warnmeldungen in Sicherheitsvorfälle umzuwandeln und so viele wie möglich automatisch zu blockieren – ohne False Positives zu erzeugen, die Probleme für das Unternehmen verursachen – noch bevor eine Untersuchung durchgeführt wird. So kommen menschliche Talente dort zum Einsatz, wo ihre Arbeit wirklich einen Unterschied macht.

> Durch zu viele unwichtige Benachrichtigungen verschwenden Analysten wertvolle Zeit, das Wesentliche wird verschleiert und Angreifer werden oftmals nicht entdeckt.

Weniger unwichtige Benachrichtigungen

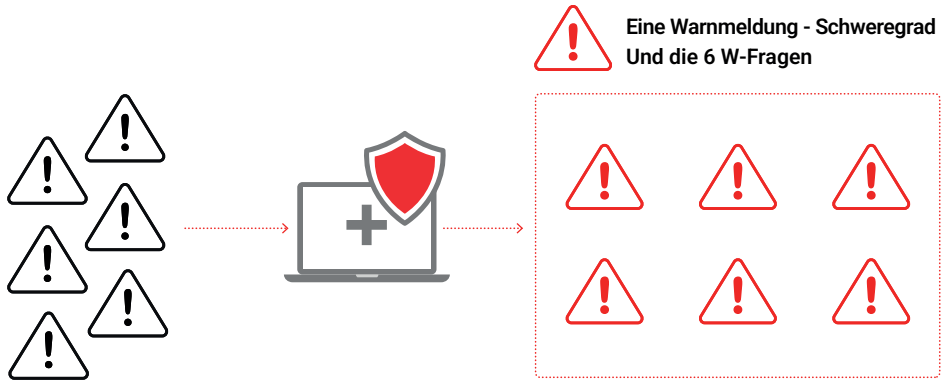
Vollständiger Verlauf des Angriffs

Schnellere Entscheidungen

02 Betriebliche Effizienz: Schutz pro Aufwandseinheit

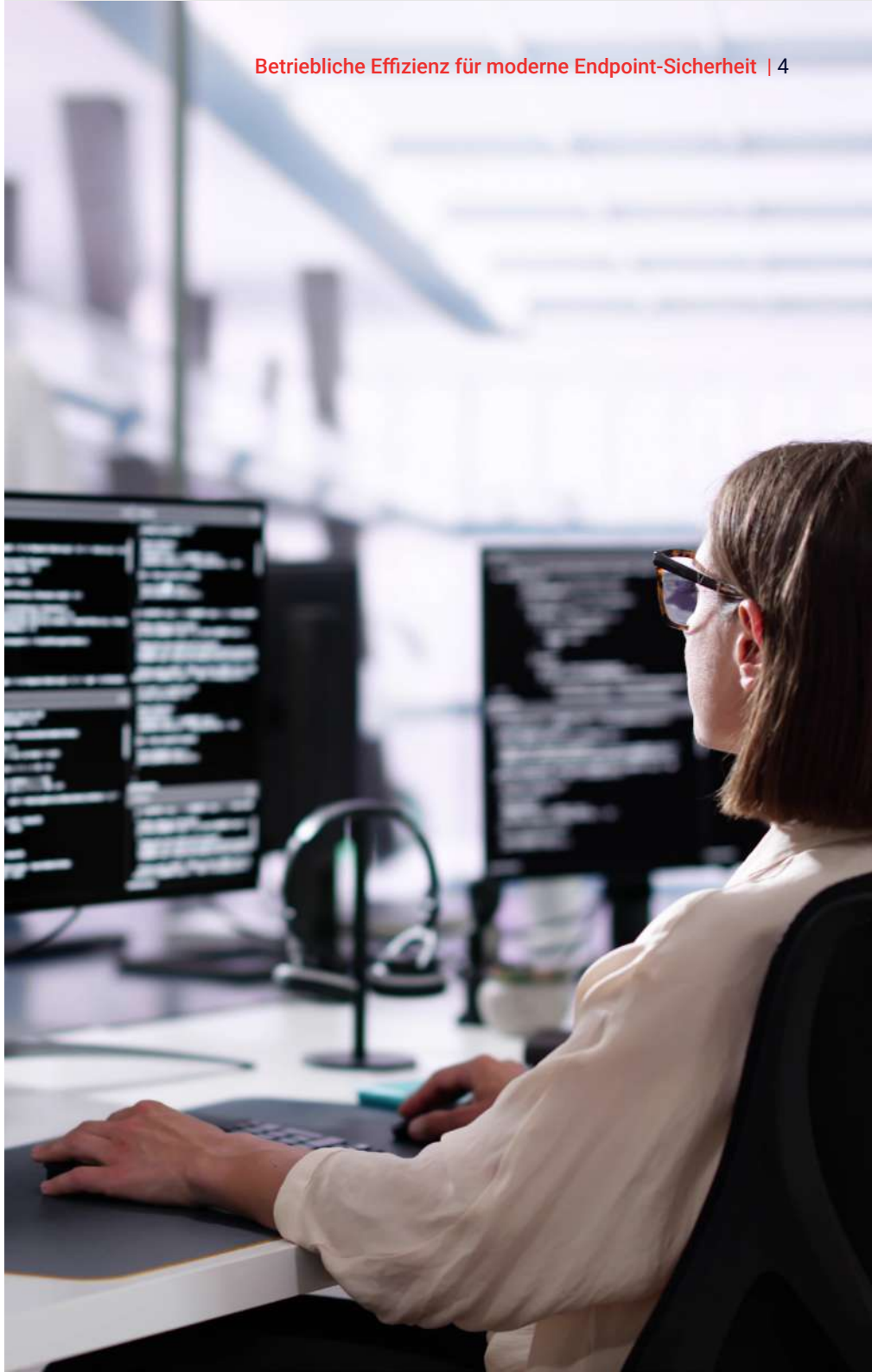
Eine Warnmeldung ohne Kontext ist eine Einzelaufnahme. Ein Vorfall ist ein ganzer Film. Wenn wir einen Vorfall nach der Anzahl der Einzelaufnahmen beurteilen, verlieren wir den Blick für das Ganze. Die Sichtbarkeit zerfällt in unzusammenhängende Momente, und das Team muss alles von Hand wieder zusammensetzen. Das Ergebnis: Frust, Rückstau und kritische Fälle, die „morgen untersucht werden sollen“ ... und morgen ist es zu spät.

Bei vielen Warnmeldungen fehlt der Kontext: für sich genommen sind sie wenig aussagekräftig. Hunderte von schwachen Signalen anzuhäufen bedeutet nicht, mehr zu sehen; es bedeutet, dass die Untersuchung viel Zeit in Anspruch nimmt und es keine Garantie gibt, dass brauchbare Ergebnisse generiert werden. In der realen Welt ist die Zeit von Analysten äußerst knapp bemessen. Wenn wir sie damit verschwenden, unwichtige Benachrichtungen zu bearbeiten, untersuchen wir nicht das, worauf es ankommt, und der Angriff wird einfach fortgesetzt.



Nicht zusammenhängende Warnmeldungen

WatchGuard Endpoint Security Elite



03 Der Wechsel: Von „Mehr Warnmeldungen“ zu „Mehr Effizienz“

An dieser Stelle kommt die Korrelation ins Spiel. Es geht nicht darum, irgendeine Art von Gruppierung vorzunehmen; es geht darum, passende Verhaltensweisen miteinander zu verknüpfen – diejenigen, die zusammen genommen einen Angriff beschreiben – und sie als einen einzigen Vorfall mit Zeitleiste, Entitäten und Umfang darzustellen. Dieser Wechsel bringt drei unmittelbare Vorteile mit sich:

> **Gesamtansicht:** Von einzelnen Punkten zu einem kohärenten Verlauf.

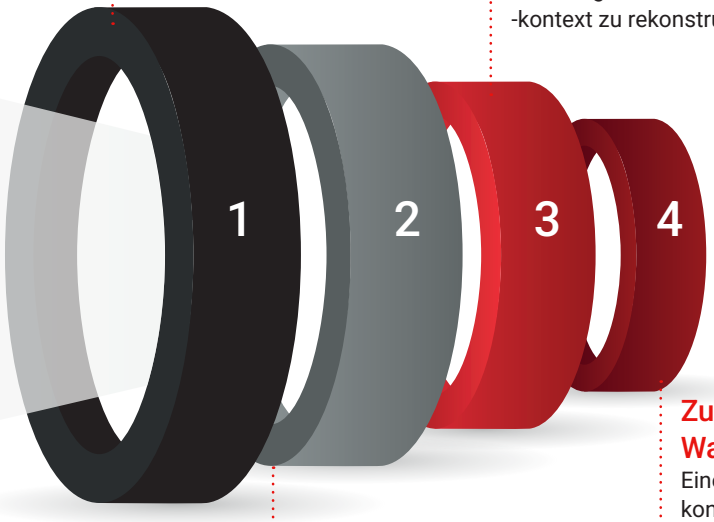
> **Echte Priorität:** Ein Vorfall mit Kontext ist wichtiger als zehn kontextfreie Warnmeldungen.

> **Weniger Probleme, mehr Effizienz**: Die Untersuchung eines Vorfalls ist schneller, als nicht zusammenhängende Warnungen durchzusehen.

Kontextualisierte Ereignisse
Rohe Telemetriedaten, die mit Kontext angereichert wurden, um unwichtige Benachrichtigungen frühzeitig rauszufiltern.

Vorfälle
Verwandte Signale werden korreliert, um den gesamten Angriffspfad und -kontext zu rekonstruieren.

Trichter zur Vermeidung unwichtiger Benachrichti-gungen



Zu bearbeitende Warnmeldungen
Eine Warnmeldung pro Vorfall, klar, kontextbezogen und bereit für die Analyse durch Mitarbeiter.

Erkennung und aggregierte Indikatoren – Signale
KI, maschinelles Lernen und Deep Learning, lokal und in der Cloud angewendet, um die Genauigkeit zu maximieren und False Positives zu minimieren.

> Dynamische Vorfälle in Echtzeit

Ein Vorfall ist keine Momentaufnahme, sondern ein sich veränderndes Objekt, das in Echtzeit angereichert wird. Wenn neue Signale auftauchen, bestimmt die Plattform, ob sie an den aktuellen Vorfall angehängt, ob ein neuer Vorfall eröffnet, ob zwei verwandte Vorfälle zusammengeführt oder ob ein zu umfangreicher Vorfall aufgeteilt werden soll.

Mit jeder Ergänzung werden die Zeitleiste, Entitäten und ATT&CK-Zuordnung (Taktiken/Techniken), das Vertrauen und der Schweregrad aktualisiert.

Analysten erstellen einen Verlauf, der schrittweise ergänzt wird, anstatt einer Abfolge von fragmentierten Warnmeldungen. Bei Abschluss oder wenn später Nachweise hinzukommen, kann das System Signale erneut miteinander verknüpfen und Schlussfolgerungen anpassen, um sicherzustellen, dass die endgültige Visualisierung den gesamten Angriff und seinen Kontext widerspiegelt.

04 Betriebliche Effizienz: Schutz pro Aufwandseinheit

Bei der betrieblichen Effizienz werden zwei Ideen miteinander kombiniert:

1. **Abdeckung der gesamten Angriffsfläche**
   Effizienz bei der Abwehr von Bedrohungen: Wie viel wir stoppen, bevor es zu einem Vorfall kommt, mit möglicht wenigen unwichtigen Benachrichtigungen.
2. **Erkennungseffizienz**
   Wie viel wir korrekt identifizieren, wenn eine Untersuchung erforderlich ist, mit möglicht wenigen unwichtigen Benachrichtigungen und Rollup zu Vorfällen.

Zusammen zeigen diese den bereitgestellten Schutz im Vergleich zur Betriebslast. Diese zusammengesetzte Ansicht ist genauer als einzelne Zahlen wie „Abdeckung“ oder „Anzahl an Warnmeldungen“.

Die operative Effizienz ist das neue Unterscheidungsmerkmal: Schutz pro Aufwandseinheit. Es geht nicht darum, wie viel; es geht darum, wie effizient Sie Bedrohungen verhindern, erkennen und darauf reagieren.

Manchmal helfen Sicherheitstools dem Team und manchmal behindern sie seine Arbeit auch. Was zählt, sind automatische Blockierung, intelligente Korrelation und eine niedrige Anzahl an False Positives.

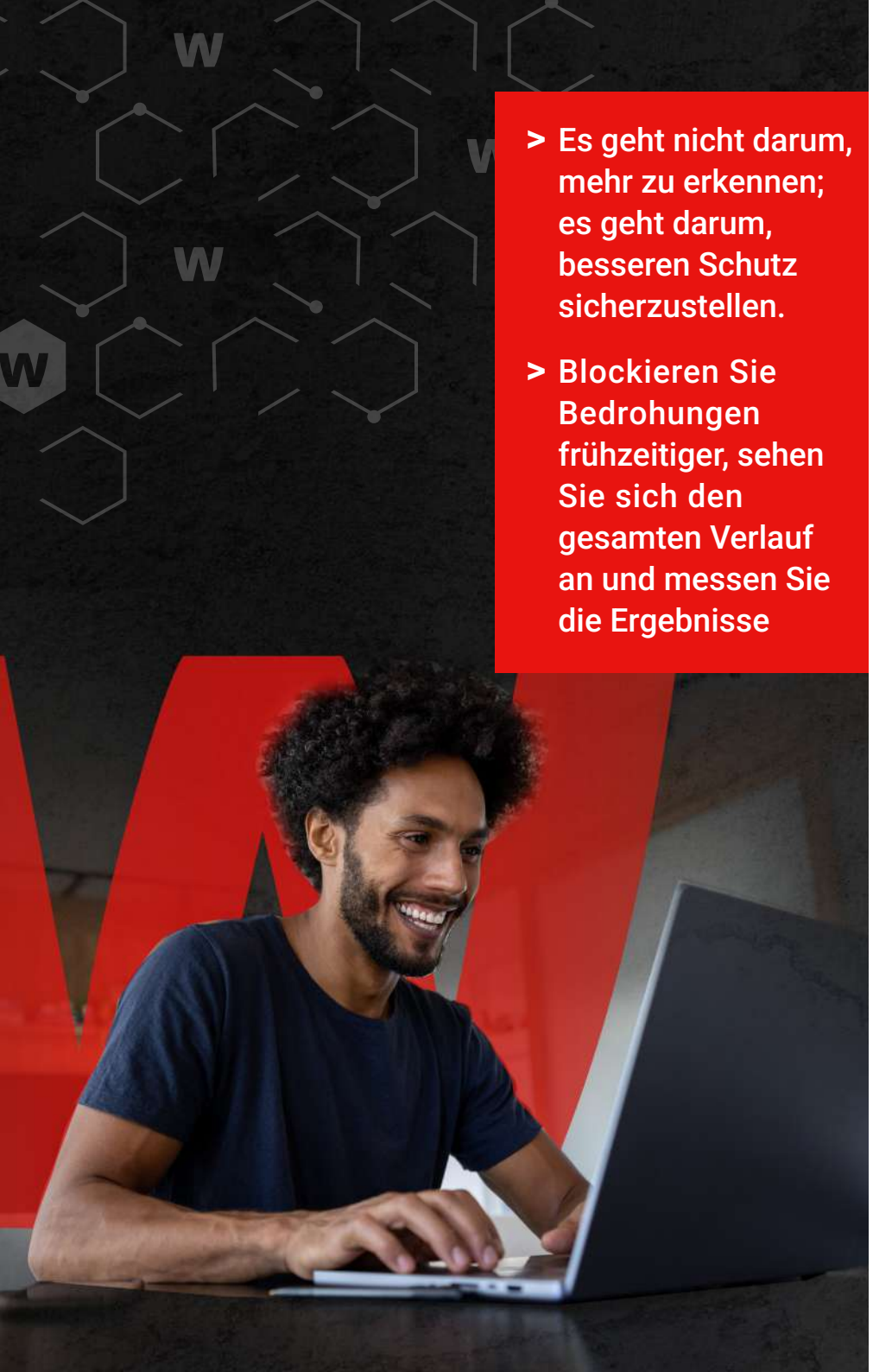
> Was passiert, wenn Sie keine Messungen vornehmen

- **Frust und Verzögerungen:** Die Anzahl an Warnmeldungen nimmt nie ab; kritische Meldungen werden aufgrund von False Positives übersehen.
- **Betriebsblindheit:** Ohne kontextbezogene Vorfälle bringt die Untersuchung nichts.
- **Endlose Feineinstellung:** Stundenlanges Optimieren von Regeln, um die Anzahl an unwichtigen Benachrichtigungen zu reduzieren – ohne großen Erfolg.
- **Fehlende geschäftliche Abstimmung:** Es ist schwer zu erklären, warum es viele Benachrichtigungen gibt, aber wenig Probleme gelöst werden.

Betriebliche Effizienz ≈

$$\frac{\textit{(Prävention + Erkennung)}}{\textit{Unwichtige Benachrichtigungen}}$$

Wobei unwichtige Benachrichtigungen =
False Positives
+
Unnötige Warnmeldungen



> Es geht nicht darum, mehr zu erkennen; es geht darum, besseren Schutz sicherzustellen.

> Blockieren Sie Bedrohungen frühzeitiger, sehen Sie sich den gesamten Verlauf an und messen Sie die Ergebnisse

05 So steigern Sie die Effizienz, ohne auf Schutz zu verzichten

1

Blockieren Sie das Offensichtliche, bevor es kompliziert wird.

Wenn ein Malware-basierter Pfad vor der Ausführung zuverlässig gestoppt werden kann, sollte dafür kein Fall erstellt werden. Dank der Prävention werden unnötige Untersuchungen vermieden und Mitarbeiter haben Zeit, um komplexere Probleme anzugehen.

2

Verwandeln Sie Signale in einen einzigen Vorfall.

Fassen Sie verwandte Endpoint-Signale in einem einzigen Vorfall mit einer klaren Zeitleiste zusammen. Analysten arbeiten an einem Fall, nicht an fünfzig. Priorisieren Sie nach Angriffsstufe und kritischen Assets.

3

Verringeren Sie die Angriffsfläche.

Schließen Sie offensichtliche Lücken standardmäßig: Deaktivieren Sie exponierte Dienste, setzen Sie die Gerätesteuerung durch, legen Sie Firewall-Regeln pro Anwendung und pro Port fest, blockieren Sie eingehenden Traffic von nicht verwalteten Geräten und entfernen Sie nicht verwendete Software. Weniger Einstiegspunkte bedeuten weniger Exposition und weniger Angriffsfläche.

4

Arbeiten Sie mit nützlichen Metriken.

Legen Sie die Sensibilität gegenüber False Positives und der Menge an Warnmeldungen fest, messen Sie die Präventions-/Erkennungseffizienz regelmäßig und verwenden Sie eine sofort einsatzbereite Baseline, um eine Feinabstimmung zu vermeiden, die echte Probleme verbirgt.

06 WatchGuard konzentriert sich auf das Wesentliche. Ihr Team konzentriert sich auf echte Bedrohungen.

Blockieren Sie Bedrohungen, bevor Sie mit der Untersuchung beginnen.
Der Zero-Trust Application Service wendet den Ansatz der standardmäßigen Ablehnung an, verstärkt durch KI-gestützte Entscheidungen in der Cloud und auf Endpoints. Die meisten Malware-basierten Pfade werden direkt am Anfang blockiert, ohne Downstream-Load.

Konsolidierte Signale werden in einem Vorfall zusammengefasst. Erweiterte Endpoint Security Elite konsolidiert Signale in einem einzigen Vorfall mit Kontext, Beziehungen und zeitlicher Abfolge. Das Team verschwendet keine Zeit mehr mit der Bearbeitung isolierter Warnungen , sondern kann sich stattdessen auf das Gesamtbild konzentrieren.

Keine Benachrichtungsüberflutung mehr.
Weniger False Positives und weniger Warnmeldungen dank Kontrollen vor der Ausführung und effektiver Korrelation. Dies erhöht die betriebliche Effizienz.

Einsatz von KI dort, wo es darauf ankommt.
Modelle, die in der Cloud trainiert werden, werden auf Endpoints eingesetzt, um Entscheidungen in Millisekunden zu treffen, wodurch die Latenz und die Abhängigkeit von der Konnektivität reduziert werden.

Einheitliche Abläufe. Eine Konsole. Eine Richtlinie. Jeder Kunde, jeder Endpoint.

Endpoint-KI: Kontinuierlicher Verbesserungskreislauf

> Zwei interagierende Ebenen.

Cloud-KI, einschließlich des Zero-Trust Application Service, führt ein Multi-Model Array (Reputation, dynamische Signaturen, beaufsichtigte und unbeaufsichtigte ML und Deep Learning, Heuristik) aus, um Binärdateien und Prozesse in großem Maßstab zu bestätigen und Echtzeit-Entscheidungen zuzulassen oder abzulehnen. Die Verhaltens-KI auf dem Gerät erkennt verdächtige Muster und Verhaltensweisen, ordnet sie MITRE ATT&CK zu und erstellt einen Vorfall mit umfassendem Kontext

> Zero-Trust Application Service.

Ausführbare Dateien und Bibliotheken werden kontinuierlich mit Cloud-Entscheidungen und einem lokalen Cache bestätigt. Es gilt der Grundsatz der standardmäßigen Ablehnung: Sofern es keine gültige Bestätigung gibt, erfolgt auch keine Ausführung. Das Ergebnis ist eine hohe Präzision bei Malware-Pfaden und weniger False Positives als bei schwachen Regeln.

> Training und Bereitstellung.

Modelle werden auf der WatchGuard Plattform mithilfe von beschriftetem bösartigen und legitimen Verhalten trainiert, werden dann destilliert und aus Effizienzgründen komprimiert und danach als leichte Endpoint-Modelle bereitgestellt. Häufige Updates sorgen für Präzision bei minimalen Auswirkungen auf das Gerät.

> Datennahe Entscheidungen.

Lokale Inferenz liefert Entscheidungen in Millisekunden, sogar offline, was eine sofortige Blockierung und Eindämmung ermöglicht. Unsere KI muss nicht auf die Cloud warten, sie denkt an jedem Endpoint mit.

> Lernschleife.

Endpoints senden Telemetrie und lokale Entscheidungen; die Cloud aggregiert, reichert sie an und korreliert sie mit Vorfällen und trennt echte Angriffe von unnötigen Warnmeldungen. Wenn sich Muster ändern, werden Modelle neu trainiert, validiert und mit Feature Flags und sofortigen Rollback-Funktionen ausgestattet. Endpoints erhalten komprimierte Updates, die die Präzision erhöhen, Probleme verringern und die Präventions- und Erkennungseffizienz kontinuierlich verbessern, wodurch die betriebliche Gesamteffizienz erhöht wird.

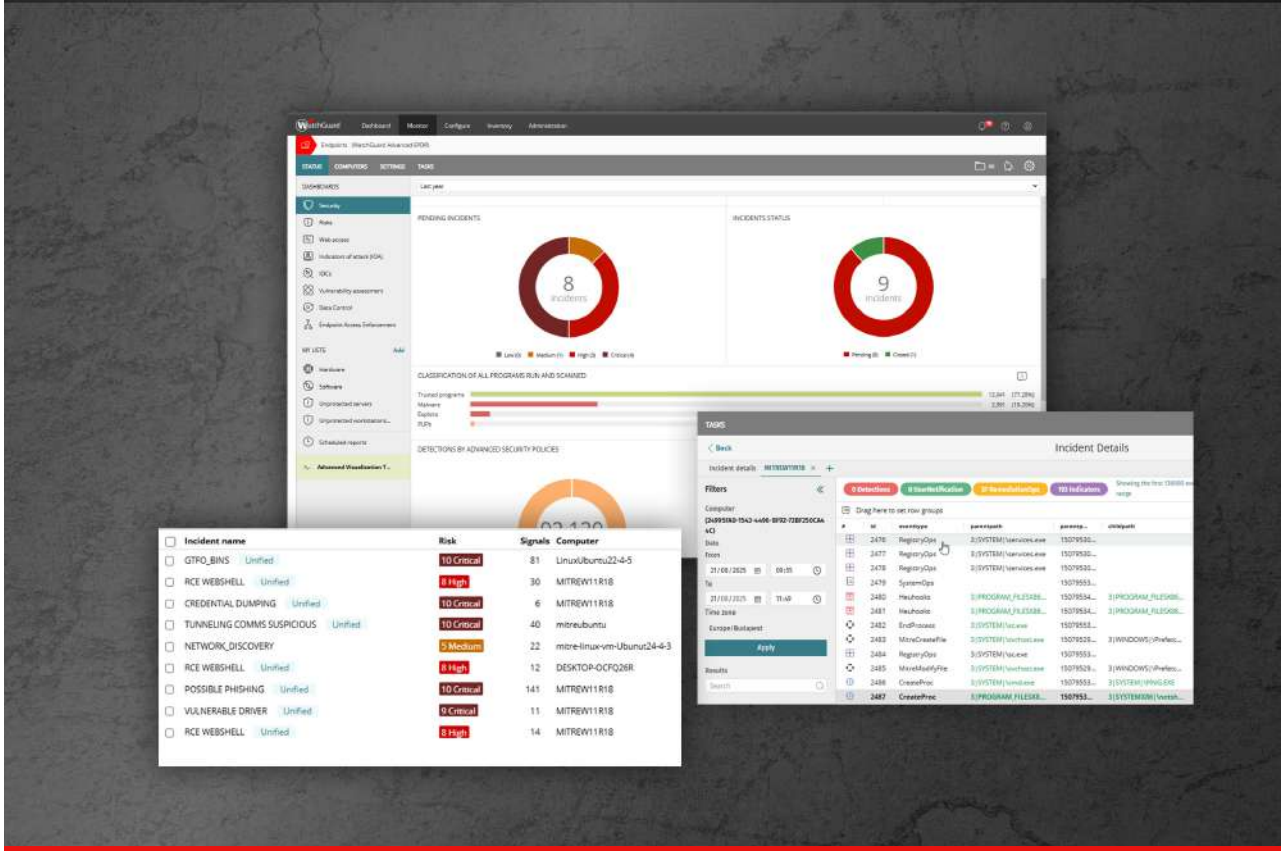
07 Fazit

WatchGuard Endpoint Security ist nicht nur eine weitere EDR-Lösung. Sie setzt einen neuen Standard für betriebliche Effizienz:

1. **Blockieren, was blockiert werden kann.**
2. **Korrelieren, was korreliert werden muss.**
3. **Erstellen eines einzigen Vorfalls, einer einzigen Warnung nur dann, wenn das Vertrauen hoch ist.**
4. **Vereinfachen, was andere verkomplizieren.**

Seit Jahren gilt die Anzahl erkannter Bedrohungen in der Branche als Erfolgskriterium. Es ist an der Zeit, das zu messen, wodurch Teams Zeit sparen und was das Unternehmen schützt: **Signale müssen effizient in Vorfälle umgewandelt werden, um das zu blockieren, was blockiert werden kann, unnötige Benachrichtigungen zu minimieren und menschliches Talent dort einzusetzen, wo nur Menschen einen Mehrwert schaffen können.** Es geht nicht darum, mehr Warnmeldungen zu sehen; es geht darum, das Gesamtbild mit weniger Aufwand zu sehen und schneller zu handeln.

Effizienz ist Schutz, der skalierbar ist. Dadurch wird WatchGuard Endpoint Security zur intelligenteren Wahl für MSPs, MSSPs und alle Unternehmen, für die Zeit genauso wichtig wie Sicherheit ist.



Möchten Sie die Lösung in Aktion erleben?

Erfahren Sie mehr über WatchGuard Endpoint Security Elite oder kontaktieren Sie uns, um eine Testversion zu nutzen und Effizienz in Aktion zu erleben.

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit des Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von über 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49-206-596-1001 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB www.watchguard.com