TD SYNNEX

paloalto NETWORKS

Palo Alto Networks - CORTEX XDR

Extended Detection & Response

Carsten Zarnetta
Business Development Manager

Date	Author	Version
24.05.2024	Carsten Zarnetta	1.0

Wir brauchen bessere Endpoint Security

Ransomware Attacken steigen an

100%+

Anstieg in 2021

Milliarden Endpunkte sind gefährdet

3Mrd.+

Devices anfällig ggü. Log4Shell in Dez ’21 mit wenig bis keinem Schutz vor Exploits

Anzahl & Kosten von Breaches steigen

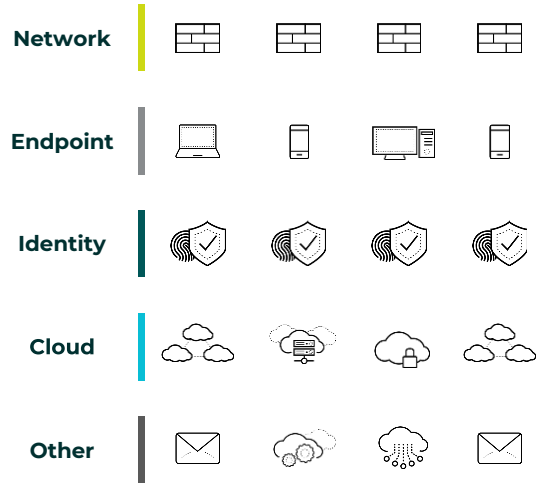
$4.2M

Durchschnittliche Kosten eines Breaches

Quelle: 2021 Verizon Data Breach Investigation Report (ransomware attacks as a percentage of all breaches have increased 100%), Ponemon Cost of a Data Breach Report, 2021

Wir müssen Kosten und Komplexität eines SOCs reduzieren

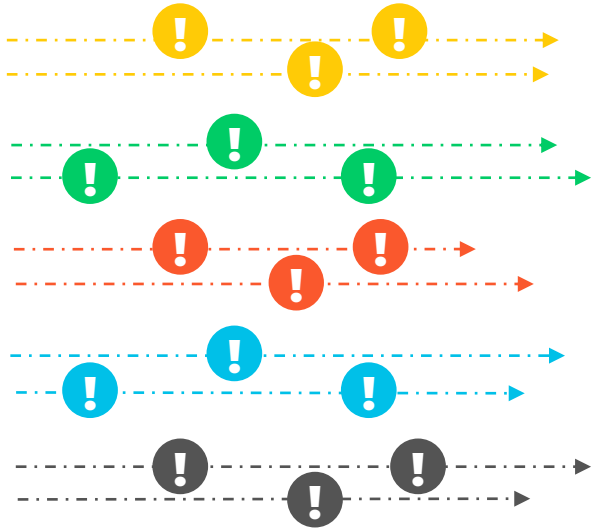
Isolierte Tools



45+

Security Tools im Schnitt

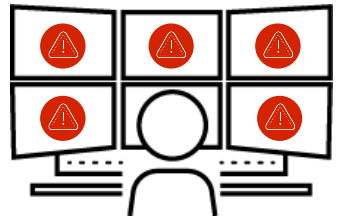
Zu viele Alarme



11,047

Alarme / Tag

Langsame Recherche



Isolierte Tools und manuelle Prozesse verlangsamen die Reaktionszeit

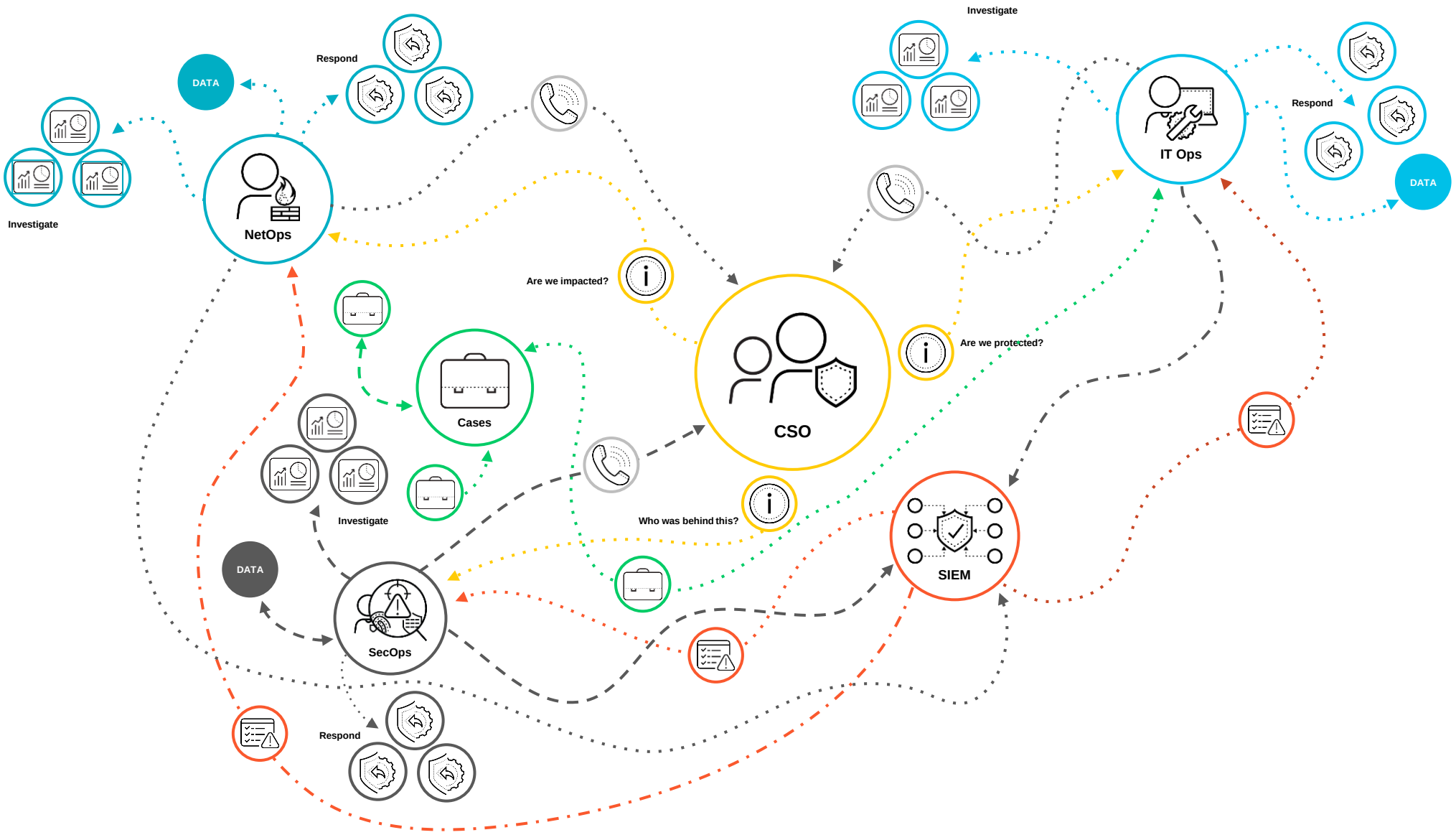
4+

Tage zur Untersuchung

Quelle: Ponemon Cyber Resilient Organization Report, Forrester, The 2021 State of Security Operations, The State of SOAR Report

Die Realität (und Komplexität) von SecOps

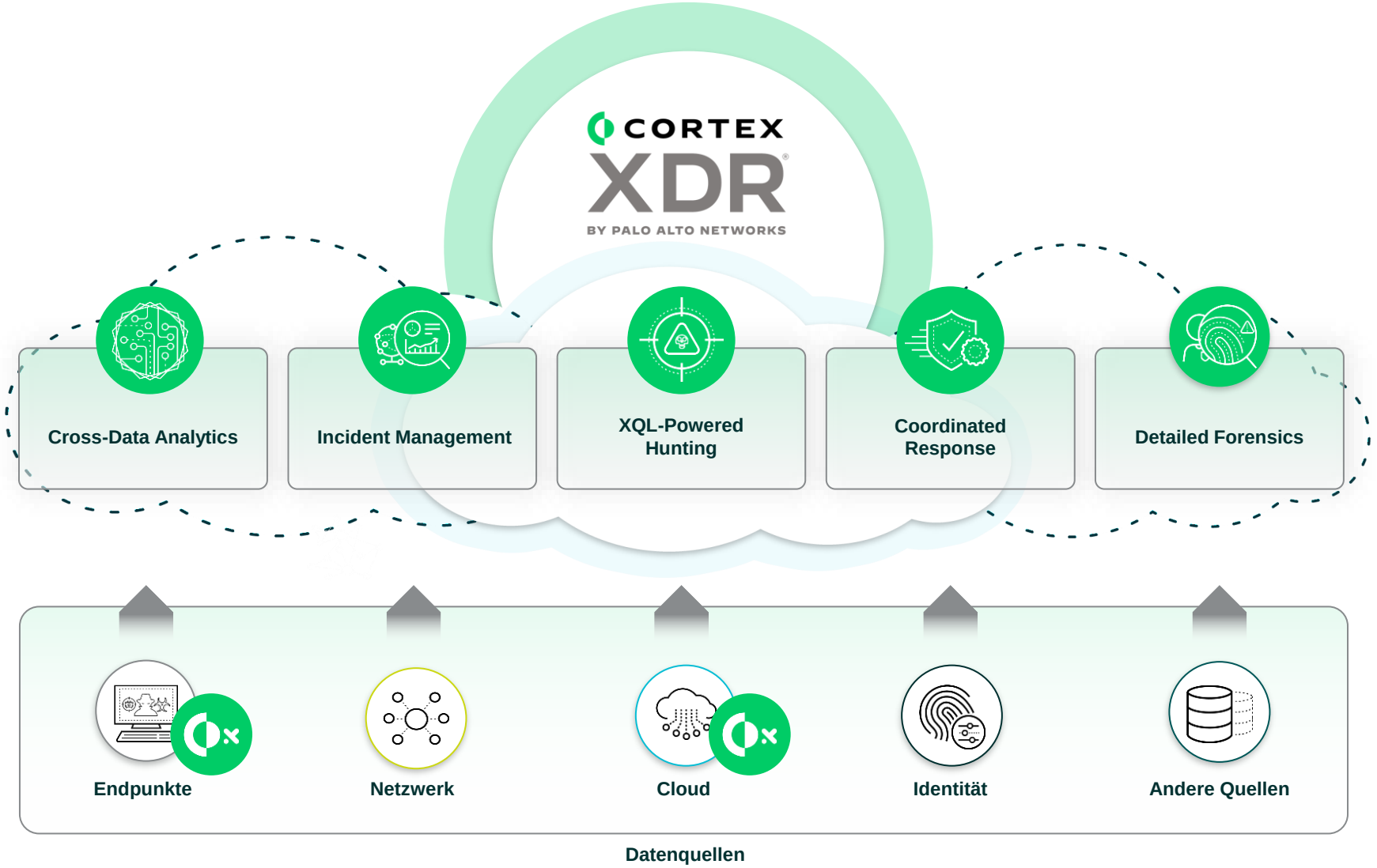
TD SYNNEX



CORTEX XDR®

Cortex XDR: Advanced Threat Prevention, Detection & Response

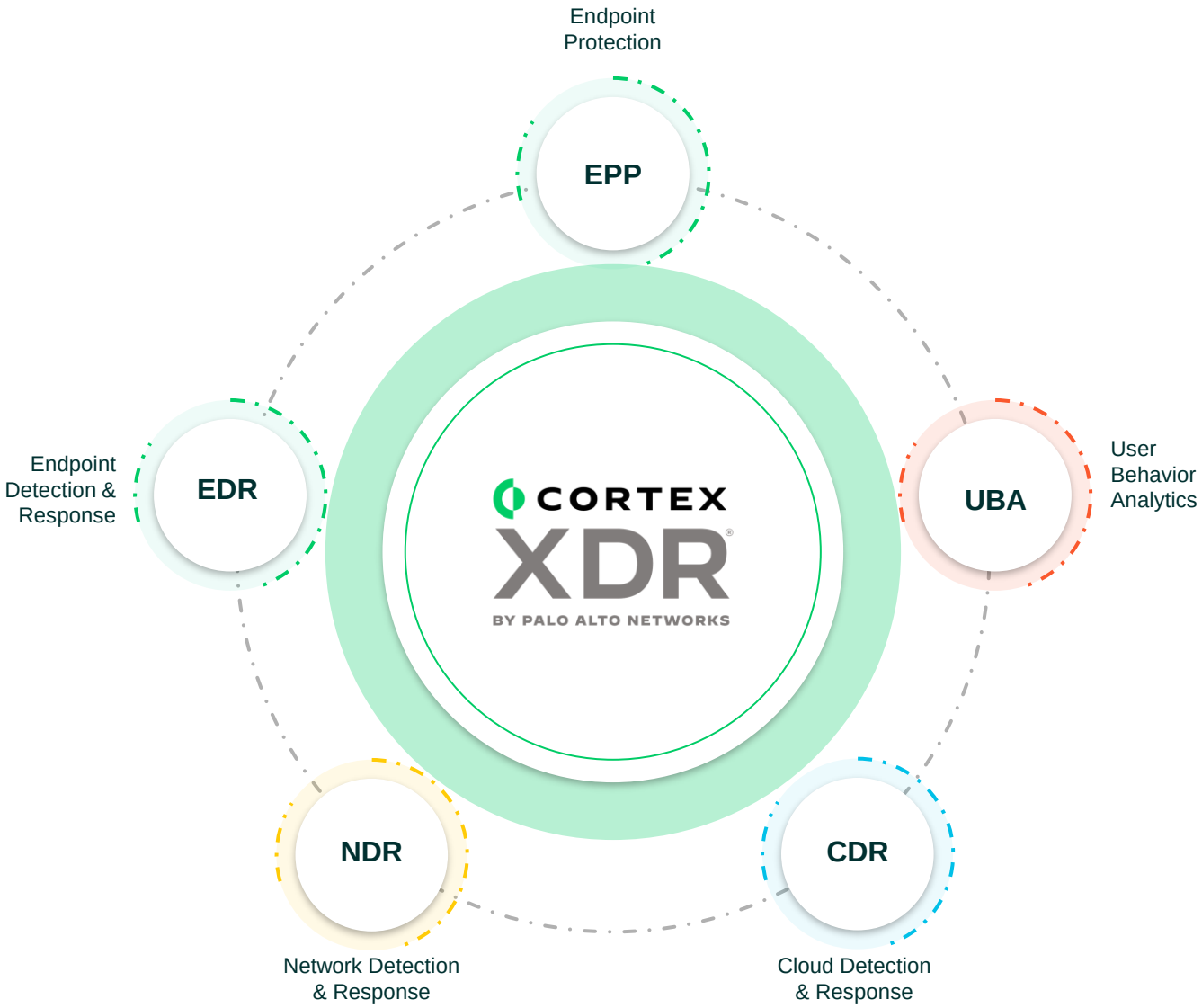
TD SYNNEX



Complete Endpoint Protection

Enterprise Threat Detection

Rapid Investigation & Response



Cortex XDR
bricht Daten- und Produktsilos auf

Prävention, Erkennung und Abwehr anhand aller Daten

Cortex XDR liefert ganzheitliche Threat Prevention, Detection & Response

TD SYNNEX

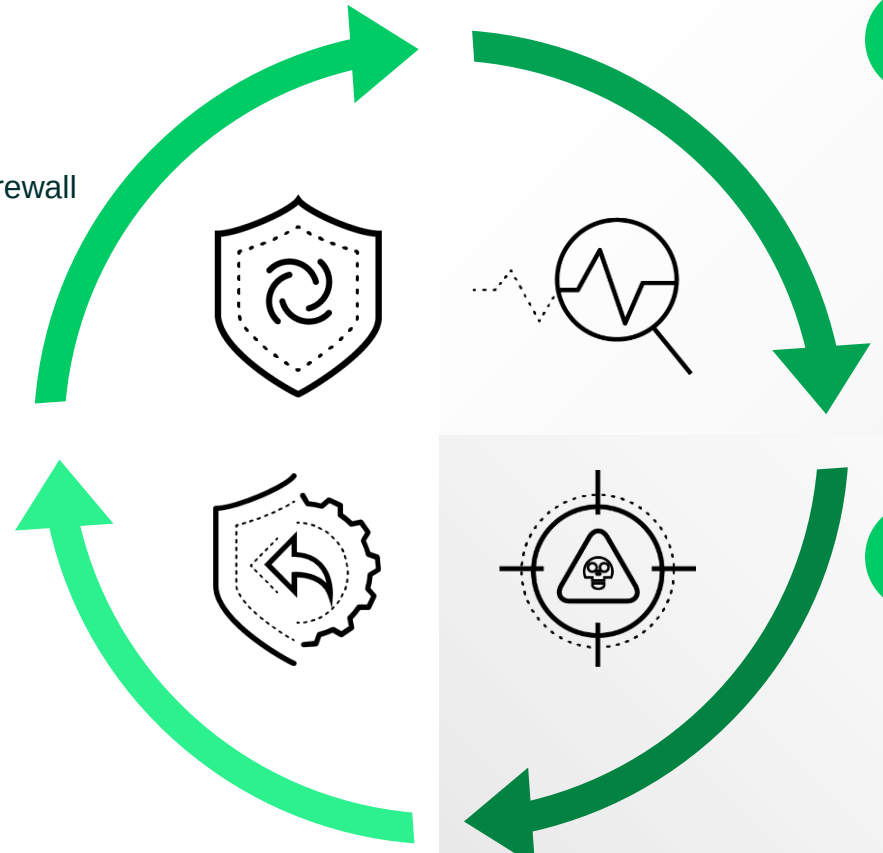
1 Blockt Attacken

Marktführende Endpoint Security

- Next-generation AV
- Device Control, Disk Encryption, Host Firewall

2 Präzise Erkennen

- Behavioral Analytics mit Machine Learning
- Anpassbare Erkennung
- Vulnerability Assessment



3 Schnelles Untersuchen

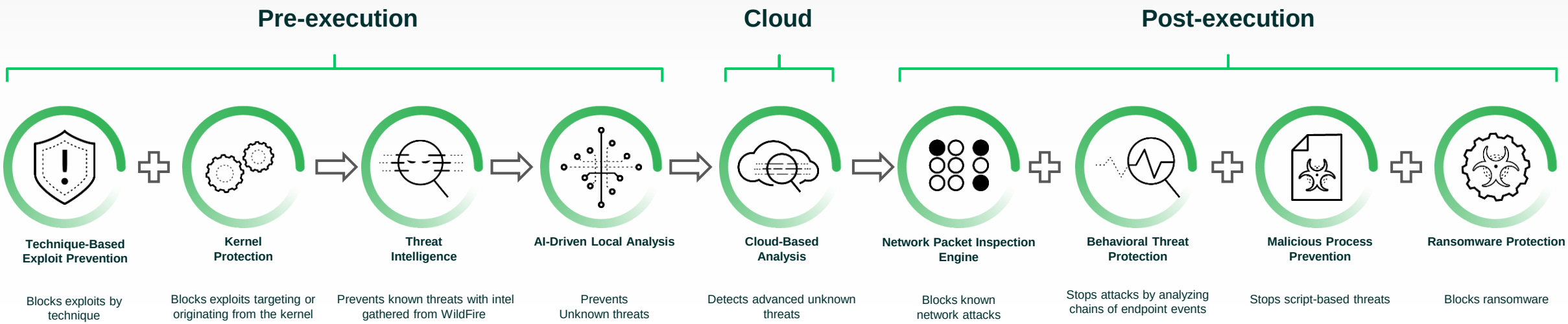
- Root Cause & Timeline Analysis
- Threat Hunting
- Integrated Threat Intel

4 Reagieren & Anpassen

- Integrated Enforcement
- Live Terminal
- Search and Destroy

Blockieren von Angriffen mit umfassenden Endpunktschutz

TD SYNNEX



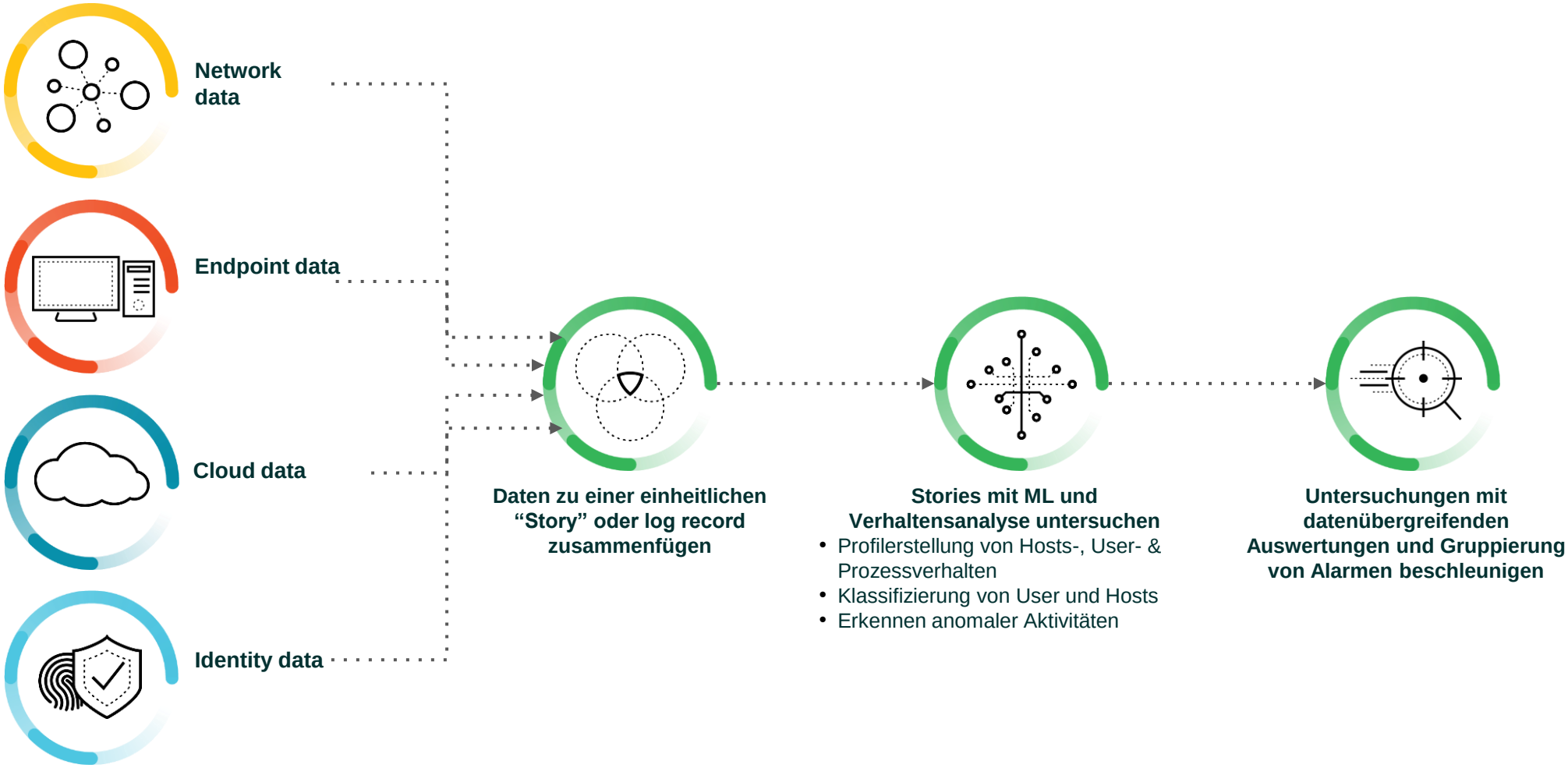
Device Control, Disk Encryption und Firewall reduzieren die Angriffsfläche

Blockieren Sie Malware mit Hilfe von KI-gestützter lokaler Analyse und Verhaltensanalyse

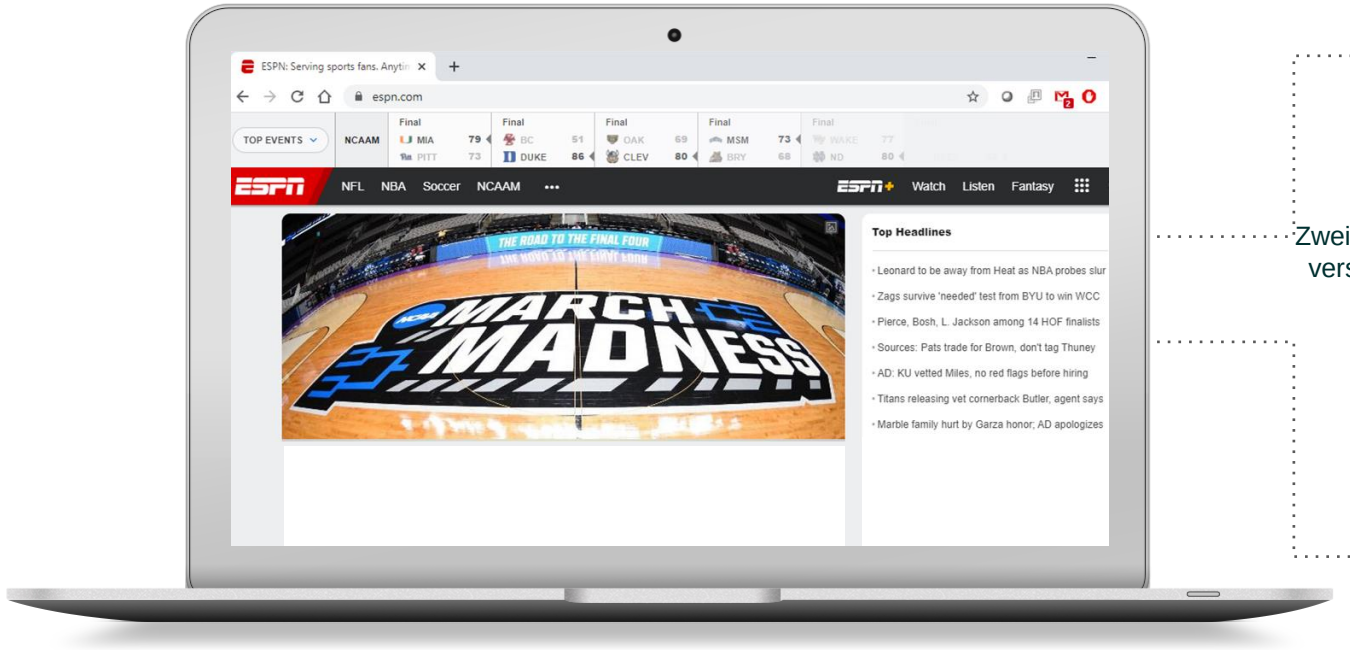
Umfassende Datenerfassung zur Erkennung von Bedrohungen

Erkennen und Untersuchen von Bedrohungen mit datenübergreifenden Analysen & Auswertungen

TD SYNNEX



Was bedeutet es, Daten zu einer “Story” zusammenzufügen?



Der User hat **eines** getan: eine Website besucht.

Netzwerk-Daten

Zwei (oder mehr) Logs wurden aus zwei verschiedenen Blickwinkeln generiert.

Endpoint-Daten

Eine einheitliche und klare “Story” in XDR

Bedrohungen mit den besten Daten, Analysen und Informationen erkennen

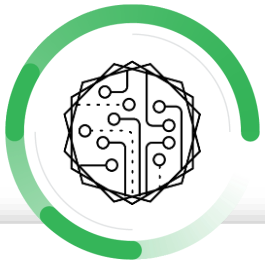
TD SYNNEX

Reichhaltige Telemetrie

- 30+ Tage, kontinuierliche Endpunkt-Erfassung
- Erfassung und Zusammenfügen von 3rd-Party-Daten

Unit 42 Threat Intel + WildFire Analysis

- 200+ Threat Researchers, 500 Mrd. Events pro Tag
- Informationen aus WildFire



ML-Powered Analytics

700+ Analysen über verknüpfte Daten hinweg

Cloud-, Netzwerk-, Endpunkt-,
und User Analytics (UEBA)

Globale Analysen über alle Kunden hinweg

Detection Rules

350+ Erkennungsregeln out-of-the-box

Möglichkeit eigene Correlation Regeln zu erstellen

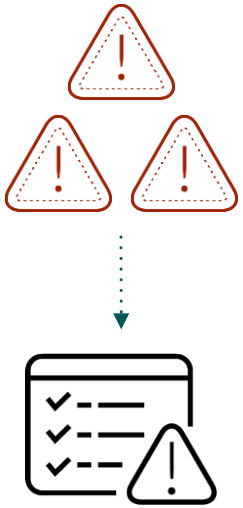
Top MITRE ATT&CK Ergebnisse

Beschleunigte Untersuchungen mit ML und datenübergreifenden Auswertungen

TD SYNNEX

Incident Management

Alarme intelligent zu Incidents gruppieren



SmartScore Incident Scoring

Incident-Attribute analysieren

ML-Vorhersage treffen

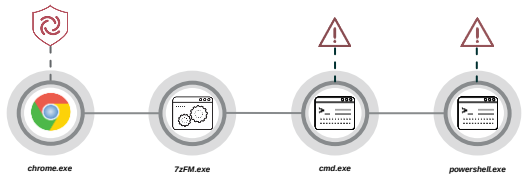
Score: 92

High-risk Incident

Score: 21

Low-risk Incident

Root Cause Analysis



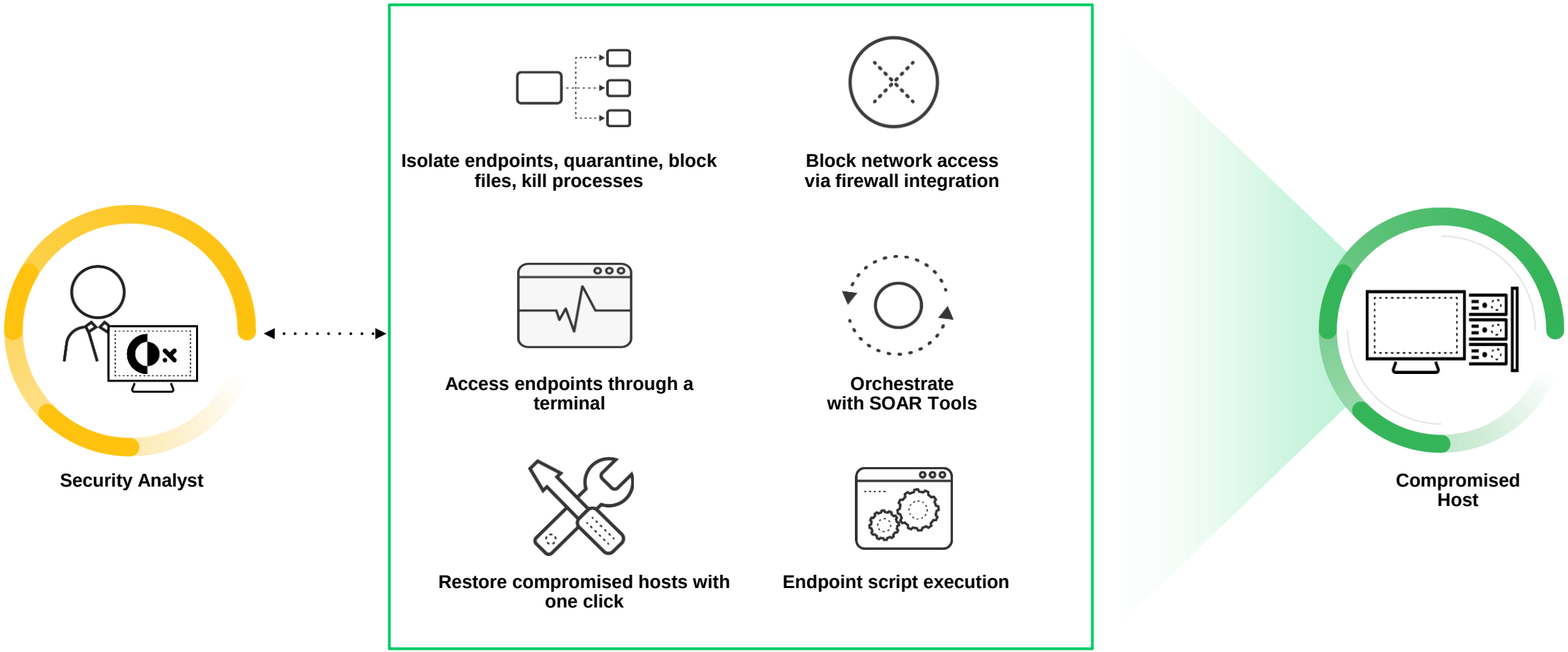
Schnelles Untersuchen durch Anzeigen von:

- Prozesskette und Root Cause, sogar von Netzwerk-Alerts
- Key Alert Artifacts
- Threat Intelligence
- CLI Kommandos

Reduzierung der zu überprüfenden Warnungen um 98%

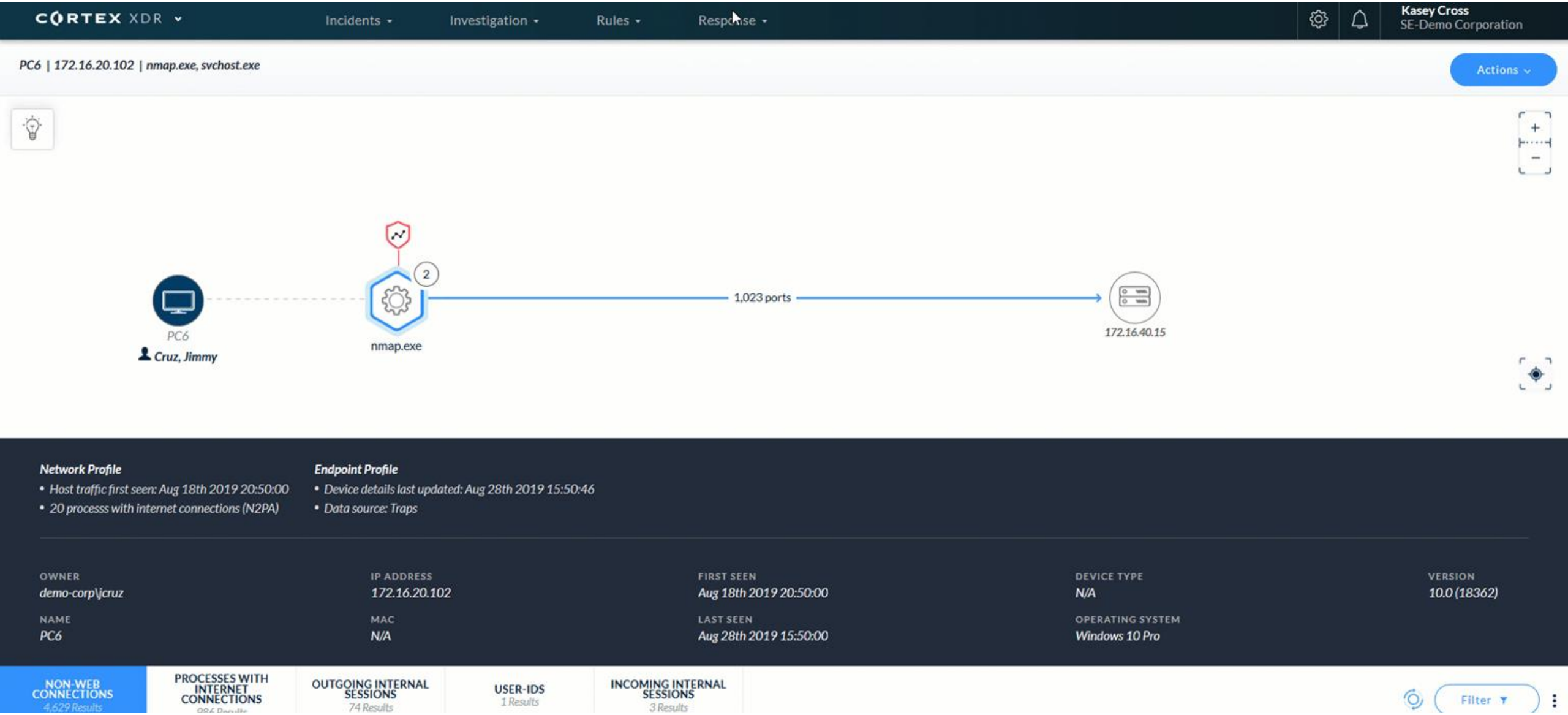
Konzentration auf die wirklich wichtigen Bedrohungen

Schnelles Eindämmen und Wiederherstellen von Angriffen mit flexibler Reaktion



Live Terminal ermöglicht flexible Reaktionen

TD SYNNEX



Zusätzliche Services

TD SYNNEX

Managed Threat Hunting

Lassen Sie Ihre Endpunkt-, Netzwerk-, und Cloud-Daten kontinuierlich von weltweit anerkannten Threat Huntern überwachen

Managed Detection & Response

Reduzieren Sie Ihre MTTR und erhalten Sie 24/7 Monitoring und Analyse von Unit 42 MDR oder XMDR Partner

Premium Success

Erhalten Sie 24x7 Kundensupport, Beratung und Unterstützung beim Onboarding durch Experten

Unit 42 MDR für Cortex XDR

TD SYNNEX

Proactive Threat Hunting

Erstklassige Threat Hunter überwachen Ihre Umgebung auf komplexe Attacken
Tiefgreifendes Verständis von XDR-Datenquellen und Palo Alto Networks Threat Intelligence
Frühzeitiger Erhalt von Informationen aus der Cortex XDR-Forschung

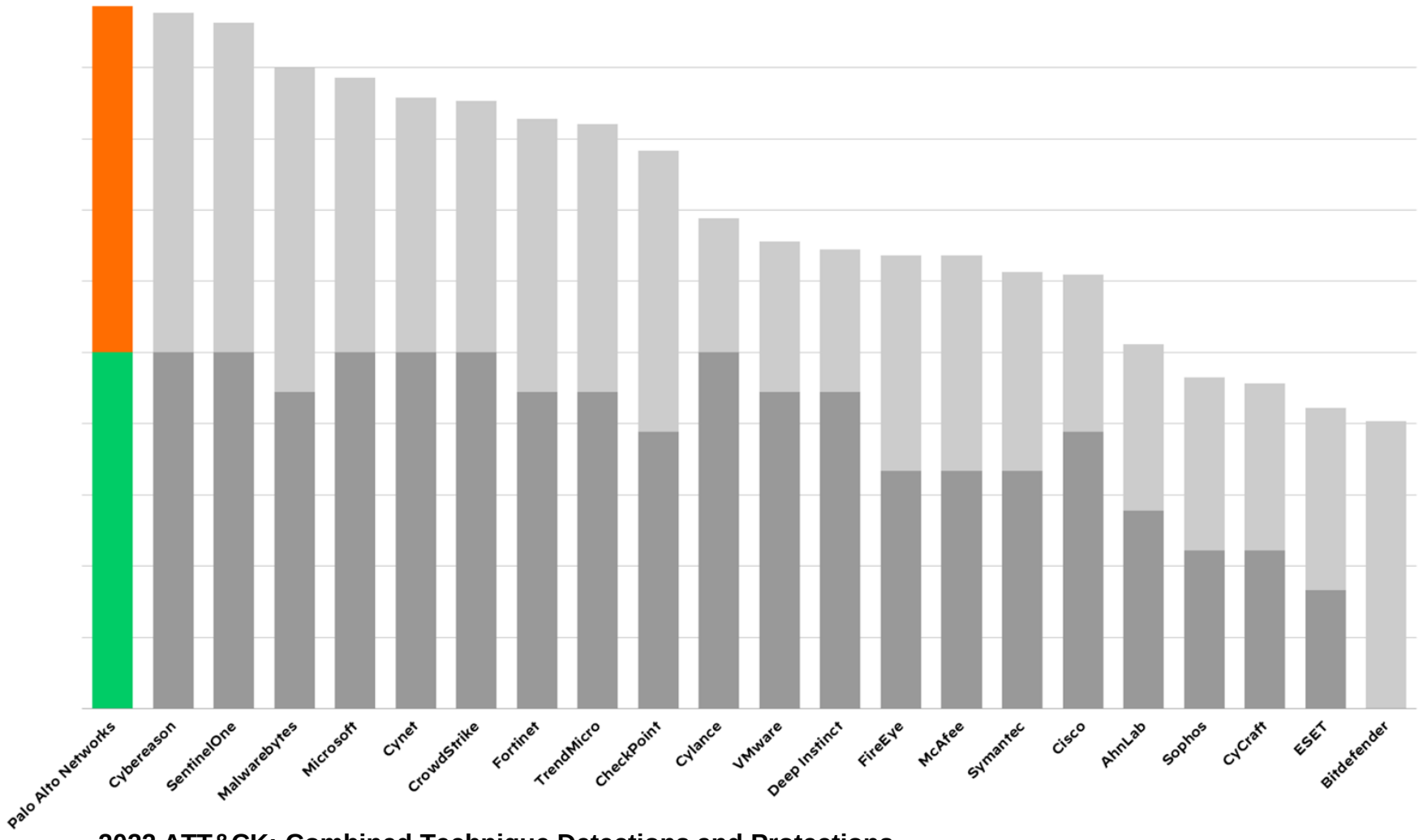
Continuous Monitoring and Response

Überwachung auf Alerts, Events, und Indikatoren 24x7x365 durch hochqualifizierte Analysten
Integrierte Threat Intelligence und umsetzbare Berichte zu Bedrohungen und Auswirkungen
Elite Incident Response, Eindämmung von Bedrohungen und Wiederherstellung

Cortex XDR

Vollständige Sicht auf Endpunkte, Netzwerk & Cloud
Analyse und Threat Detection über alle Datenquellen hinweg generieren Ansatzpunkte für das Hunting
100% Prävention & 100% Erkennung im MITRE ATT&CK Testing

MITRE ATT&CK Testing 2022



2022 ATT&CK: Combined Technique Detections and Protections

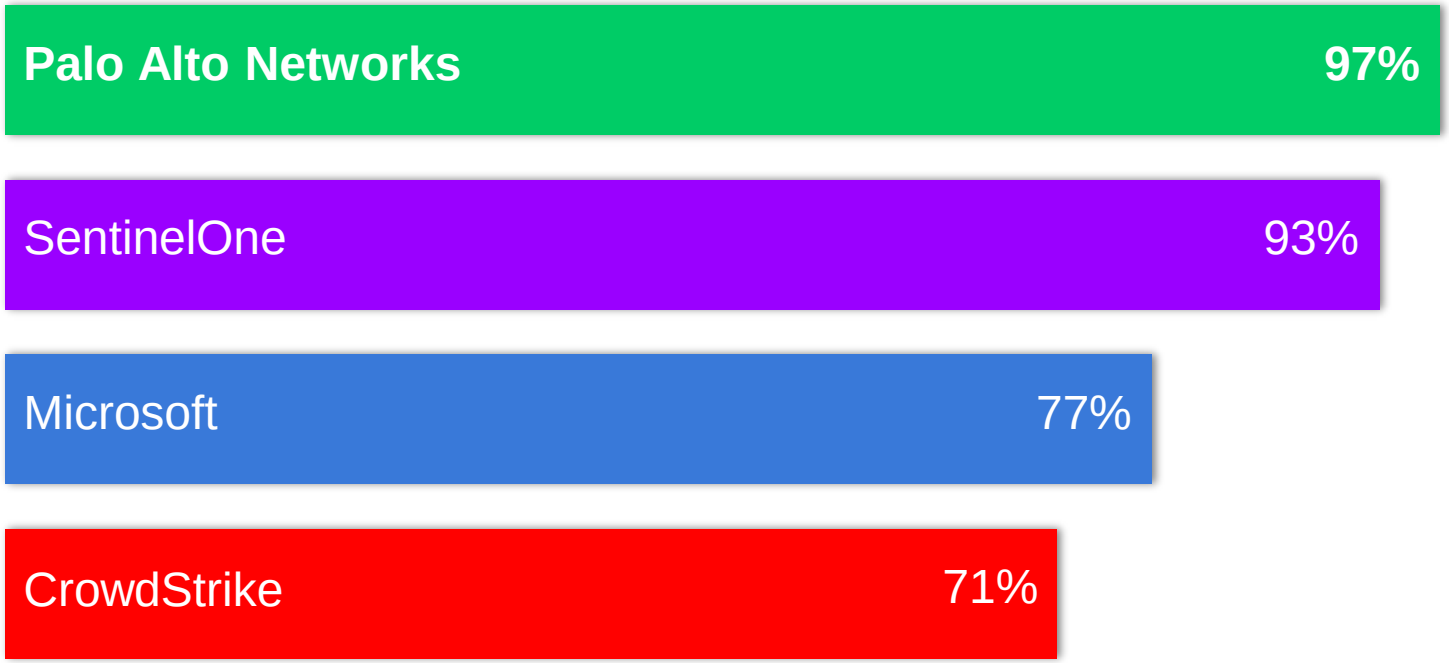
Technique Detections Protections

- **100% Schutz**
  inklusive Linux und Windows
- **100% Erkennung**
  aller 19 Angriffsschritte
- **107 of 109 Technique Detections**,
  höchster Wert aller Hersteller

Note that Technique Detections exclude configuration changes. Not all vendors participated in the Protections or the Detections for Linux evaluations.

Details zu Technique Detections

Technique Detections



(Configuration Changes excluded)

Technique Detections sind der “Gold Standard”, da sie das *Was, Warum und Wie* eines Angriffs beantworten.

SecOps-Effizienz erhöhen

TD SYNNEX

Kosten von Angriffen senken

65%

Anstieg der entschärften Vorfälle

Operative Kosten senken

86.16%

Verringerung der MTTR

Ausgaben für Tools reduzieren

87%

Verringerung der laufenden Ausgaben für Tools

Source: Outcomes reported by XDR customers and the Palo Alto Networks SOC

Cortex XDR Lizenzen

TD SYNNEX

	Cortex XDR Prevent	Cortex XDR Pro
Next-Generation Antivirus Stop malware, exploits, and fileless attacks	✓	✓
Endpoint Protection Secure your endpoints with device control, host firewall, and disk encryption	✓	✓
Detection and Response Pinpoint attacks with AI-driven analytics and coordinated response	—	✓
Host Insights Identify and eliminate risks with vulnerability assessment and Search & Destroy	—	Optional
Managed detection and response Let Unit 42 experts uncover the most complex threats across data sources	—	Optional
Forensics Investigate incidents swiftly with comprehensive forensics data	—	Optional
XDR for Cloud Extend threat prevention, detection and response for Kubernetes cloud hosts	—	Optional
Threat intelligence feed Enrich investigations with rich context from a global community of customers	Optional; WildFire analysis included	Optional; WildFire analysis included
Data sources Get extended visibility across data sources	Endpoint	Endpoint, network, cloud and all third-party data

Vielen Dank

Carsten Zarnetta
Business Development Manager
carsten.zarnetta@tdsynnex.com
+49 175 7270250