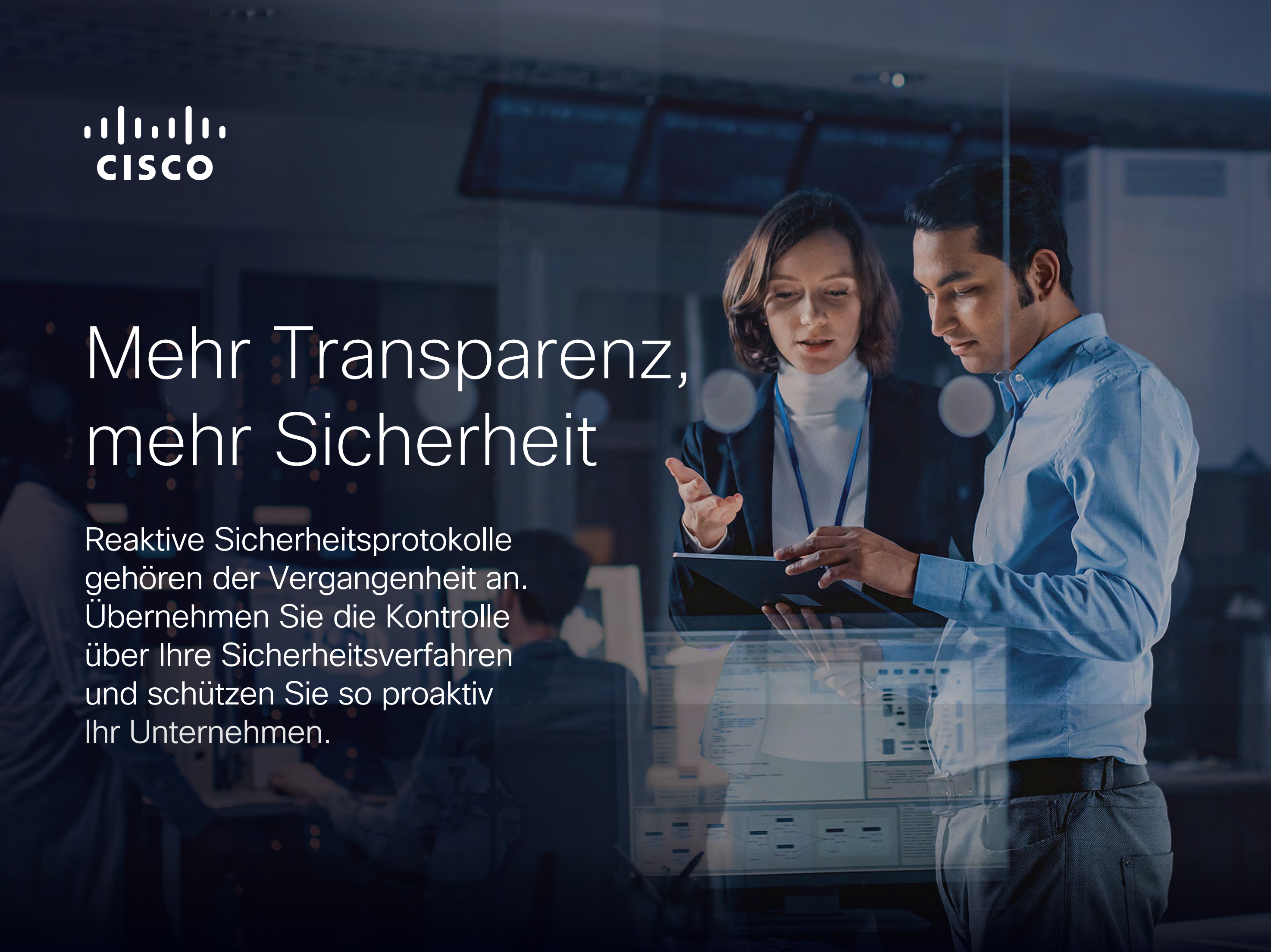


Mehr Transparenz, mehr Sicherheit

Reaktive Sicherheitsprotokolle gehören der Vergangenheit an. Übernehmen Sie die Kontrolle über Ihre Sicherheitsverfahren und schützen Sie so proaktiv Ihr Unternehmen.

Mit welchen Herausforderungen sehen sich Sicherheitsverantwortliche konfrontiert?

Angriffe gehen mit immer höheren Kosten einher

4,45 Mio. USD sind die durchschnittlichen Kosten eines Ransomware-Angriffs – die Kosten für die Freigabe der Daten nicht inbegriffen[1]

Die effektive Erkennung von und Reaktion auf Bedrohungen ist entscheidend, um das Geschäft wie gewohnt am Laufen zu halten und sich auf weiteres Unternehmenswachstum zu konzentrieren.

Jeder kann Opfer eines Angriffs werden

83 % aller Unternehmen hatten bereits mehr als eine Datensicherheitsverletzung zu beklagen[1]

Die Anzahl, die Häufigkeit sowie die Komplexität von Angriffen nimmt stetig zu. Dies führt zu einem immer größeren Aufwand für Ihre SOC-Teams.

Die Überlastung durch zu viele Warnungen nimmt zu

37 % aller IT- und Sicherheitsfachkräfte geben an, dass es aufgrund der Häufigkeit und Komplexität von Warnungen immer schwerer wird, ihre Sicherheitsumgebung zu verwalten[2]

Unterschiedliche Warnungen bei der Erkennung von Bedrohungen sowie komplexe Untersuchungen fördern die Überlastung durch zu viele Warnungen sowie eine hohe Fluktuation von AnalystInnen.

Aktuelle Security-Tools haben jedoch oft Probleme damit, ausgeklügelte Angriffe durch Hackergruppen wie BlackTech, Volt Typhoon oder Wizard Spyder zu erkennen und zu analysieren.

Mehr Unternehmenssicherheit durch ein besseres SOC-Erlebnis

Sicherheitsverantwortliche und ihre Teams wünschen sich eine höhere Effizienz, hochwertigere Erlebnisse und einen höheren ROI.

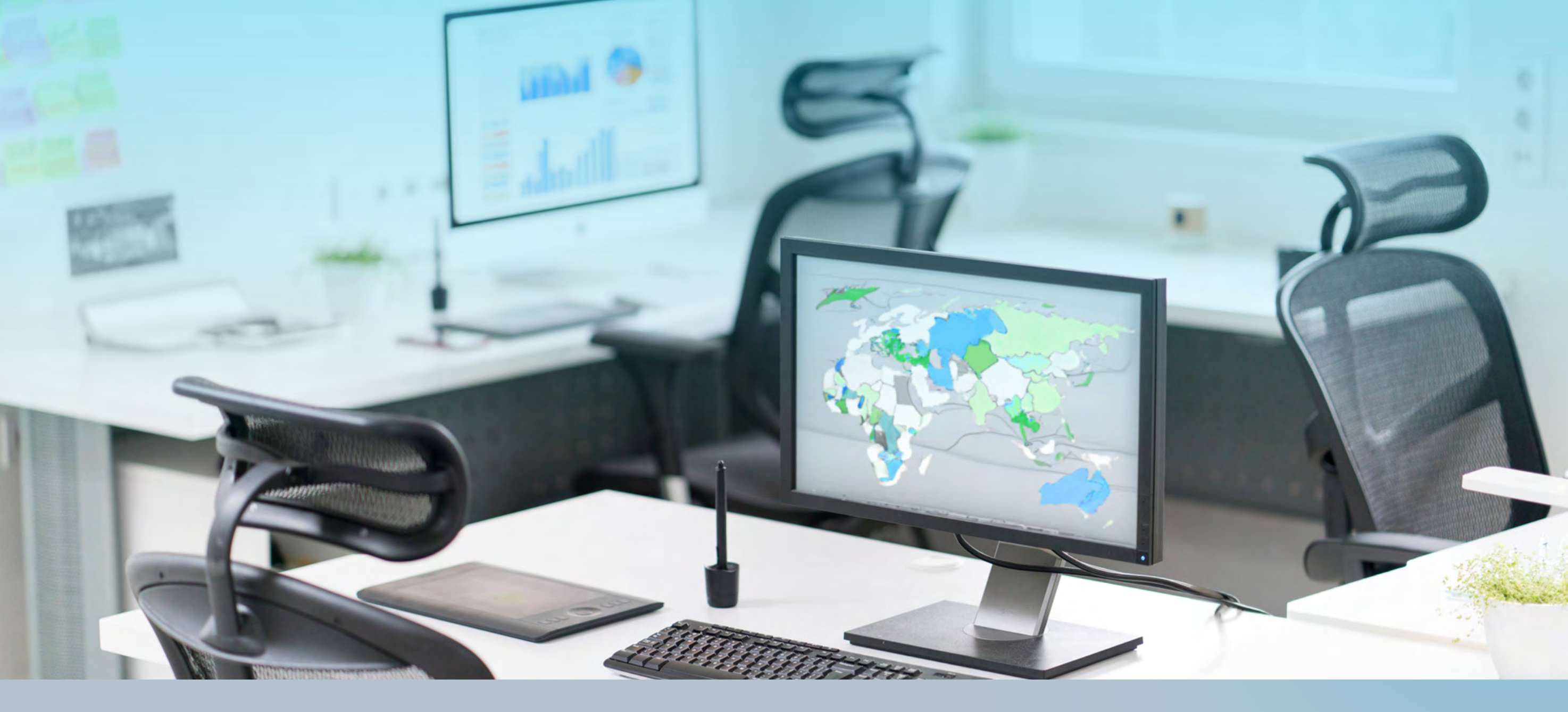
Höhere Effizienz: Erkennung von und Reaktion auf ausgeklügelte Bedrohungen wie Ransomware durch korrelierte Telemetrie und die Kombination von menschlicher Intuition und KI

Hochwertigere Erlebnisse: mehr Transparenz, kürzere Reaktionszeiten und Entlastung von AnalystInnen durch eine einheitliche Plattform und höhere Automatisierung

Höherer ROI: umfassende Nutzung von Sicherheitsressourcen durch automatisierte Reaktionen und geführte Untersuchungen für noch höhere SOC-Produktivität

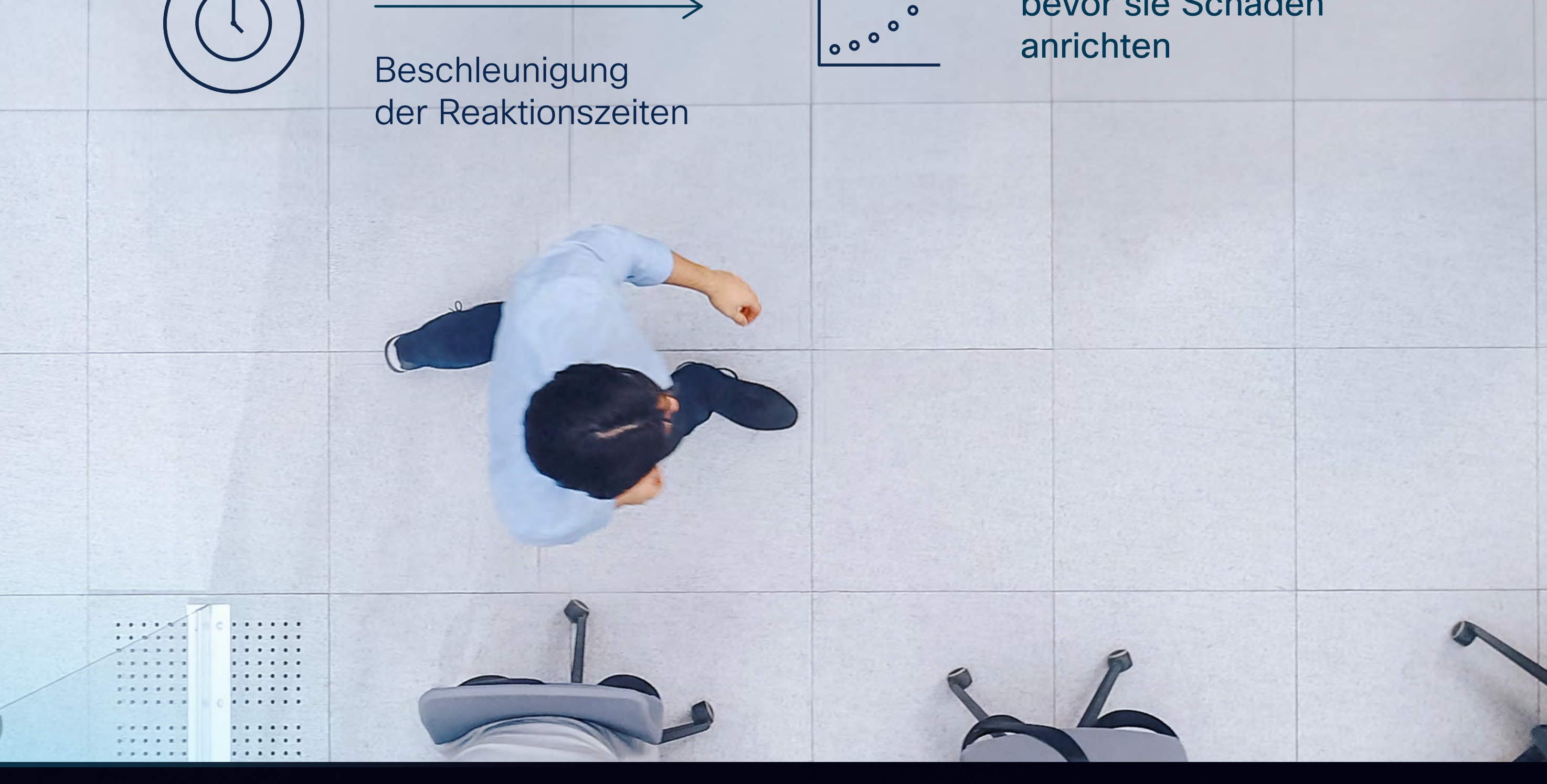
Mit der Cisco Breach Protection-Suite können Sicherheitsteams Bedrohungen wie Ransomware, Phishing, Malware und Insider-Bedrohungen auf sämtlichen Umgebungen effizient abwehren – ganz gleich ob auf Endpunkten, in E-Mails, im Netzwerk oder in Cloud-Umgebungen.

- Extended Detection and Response (XDR)
- Endpunktsicherheit
- Network Detection and Response (NDR)
- E-Mail-Sicherheit
- Cloud-Security



Breach Protection unterstützt Sie durch Folgendes:

- Schnellere Erkennung von Bedrohungen → Verkleinerung der Angriffsfläche
- Priorisierung von Vorfällen nach potenziellen Auswirkungen → Minderung von Geschäftsrisiken
- Schnelle Untersuchung von Vorfällen → Erstellung eines vollständigen Bildes über den Angriff
- Beschleunigung der Reaktionszeiten → Abwehr von Angriffen, bevor sie Schaden anrichten

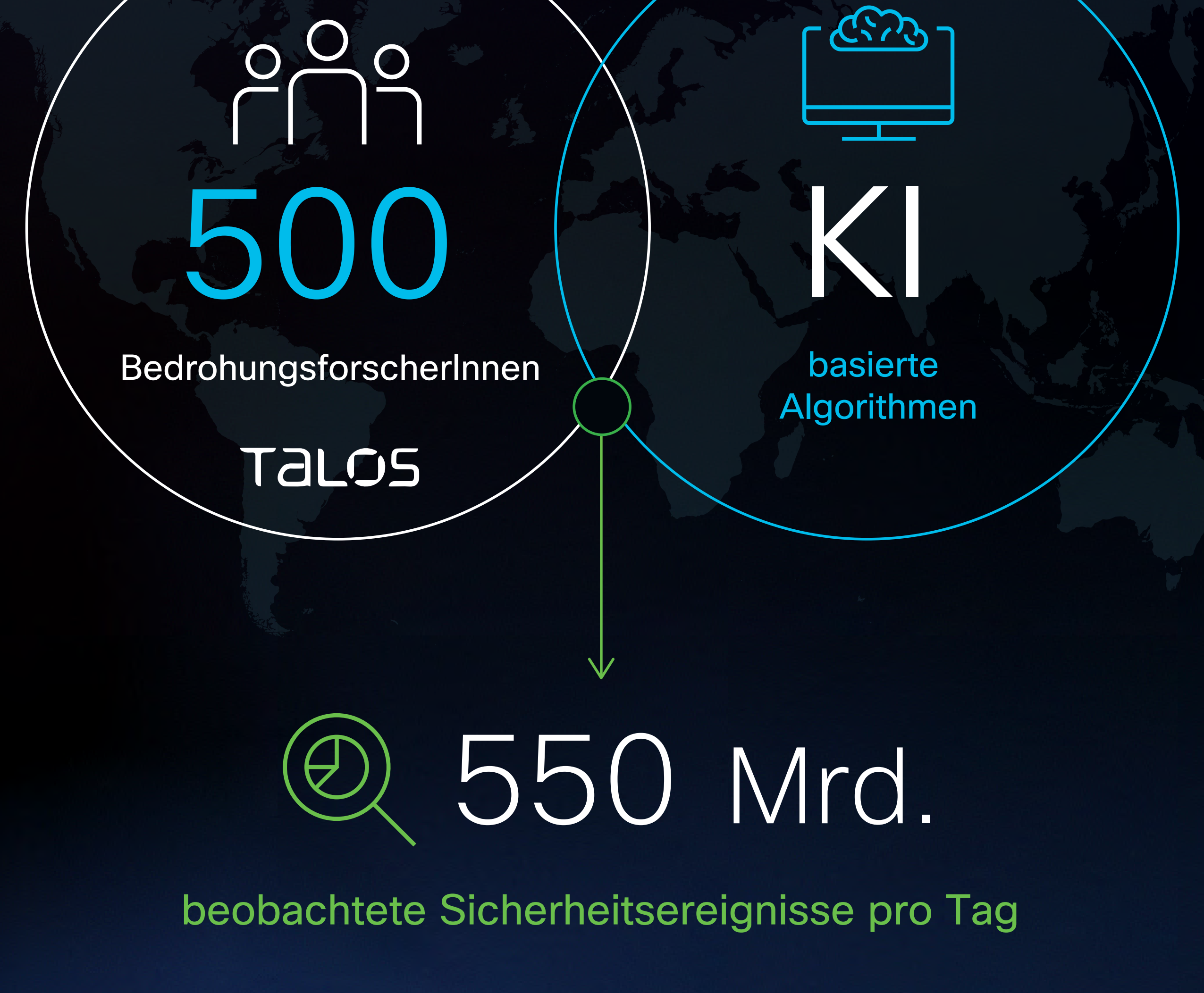


Mehr Transparenz, mehr Sicherheit

Unsere Lösung überwacht jeden Tag Milliarden an Authentifizierungsanfragen, unzählige Phishing-Angriffe und nicht vertrauenswürdige Webseiten. Gleichzeitig verfolgen wir jede einzelne Verbindung nach, die von einem Endpunkt aus aufgebaut wird. Ihr SecOps-Team weiß also jederzeit ganz genau, was gerade passiert, und kann so Bedrohungen wie Ransomware im Keim ersticken.

In Kombination mit der Cisco Security Cloud erhalten Ihre Teams eine Plattform mit End-to-End-Einblicken und profitieren so von umfassender Transparenz und der Möglichkeit, ausgefeilte Angriffe noch effizienter abzuwehren.

Breach Protection wird gestützt durch:



550 Mrd.

beobachtete Sicherheitsereignisse pro Tag

Wehren Sie Bedrohungen noch effizienter ab als Ihre Mitbewerber, indem Sie menschliche Intuition mit KI und Automatisierung kombinieren.

Entdecken Sie Bedrohungserkennung und -reaktion, die ihresgleichen sucht.

Breach Protection entdecken