

Zero Trust: Der ultimative Schutz vor Ransomware-Angriffen

Neue Ransomware-Angriffe umgehen herkömmliche Netzwerksicherheit

User, Anwendungen und Daten haben sich in den vergangenen zwei Jahren vom Perimeter gelöst, weshalb der Umfang und die Auswirkungen von Ransomware-Angriffen zugenommen haben. Einzelne Angreifer wurden durch Gruppen verdrängt, die mit ihren spezialisierten Fähigkeiten und Toolkits miteinander Handel treiben. Angriffe waren einst breit angelegt und eindimensional. Heute werden bei ihnen jedoch gezielte, mehrstufige Taktiken eingesetzt, die sich mit veralteter Castle-and-Moat-Sicherheitsarchitektur kaum noch aufhalten lassen.



20 Mrd. USD

geschätzter durch Ransomware
verursachter Schaden 2020



Alle 14 Sekunden

kommt es weltweit
zu einem Ransomware-Angriff



500 %

mehr Ransomware in SSL-verschlüs-
seltem Traffic zur Umgehung her-
kömmlicher Abwehrmechanismen

Ransomware-Angriffe sind die größte Bedrohung für die digitale Wirtschaft.

Anfängliche
Gefährdung

Laterale
Bewegung

Ausschleusen
von Daten
für doppelte
Erpressung

Installation von
Ransomware und
Verschlüsselung
von Computern

Forderung
von Lösegeld



80%

der Angriffe beginnen
mit Phishing-E-Mails

94 %

der Infektionen
breiten sich
in unter
4 Stunden aus

50%

aller Ransomware-
Angriffe sind
Datenschutzverlet-
zungen

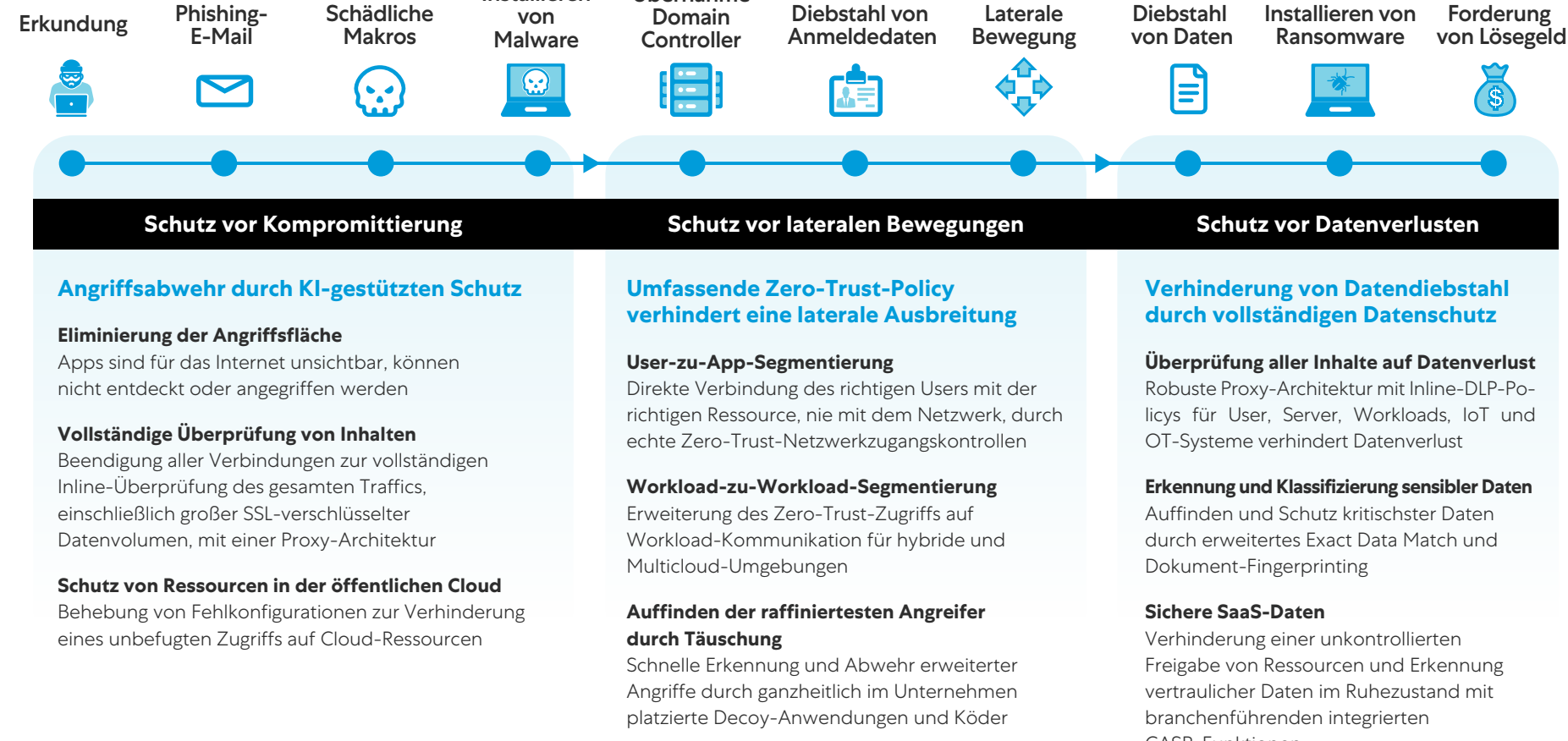
200 %

mehr Ausfallzeit
durch
Ransomware

**234.000
USD**

durchschnittliche
Ransomware-
Lösegeldsumme

Zero-Trust-Architektur



Zero Trust: Die effektivste Strategie zum Schutz vor Ransomware

Erstklassige Ransomware-Abwehr:

Inline-Überprüfung des gesamten Traffics für moderne mobile Cloud-First-Unternehmen minimiert die Angriffsfläche und eliminiert eine laterale Ausbreitung.

Vorteile gegenüber herkömmlichen Lösungen:

Zero Trust bietet einen vollkommen alternativen Ansatz zu herkömmlichen Castle-and-Moat-Sicherheitsarchitekturen und verbindet User und Applikationen stets direkt miteinander, nie mit dem Netzwerk.

Sicherheit für agile Unternehmen:

Ein vollkommen Cloud-basiertes Sicherheitsmodell ohne herkömmliche Infrastruktur reduziert Komplexität und Kosten und sorgt für eine herausragende Geschäftsagilität und User Experience.

Vorteile für Unternehmen und Sicherheit durch Zero Trust

Unübertroffene Risikominderung

Eliminiert die Angriffsfläche und eine laterale Ausbreitung durch erstklassigen Schutz vor Cyberbedrohungen und Datenschutz

35x
Reduktion
infizierter Computer

NOV

Schnellere Zeit zur Umsetzung

Als echte Cloud-Services ohne Infrastruktur bereitgestellt, in weniger als 24 Stunden einsatzbereit

Für über
10.000 User
in unter 48 Stunden
bereitgestellt

NORDSTROM

Besseres Preis- Leistungs-Verhältnis

Keine Einzelprodukte mehr für die Sicherheit und Vereinfachung des Betriebs

70%
Kostensenkung

SIEMENS

Sie möchten mehr darüber erfahren, wie der Ransomware-Schutz mit dem branchenweit größten Funktionsumfang auch Ihr Unternehmen absichern kann? [Laden Sie das E-Book herunter.](#)

E-Book lesen →