

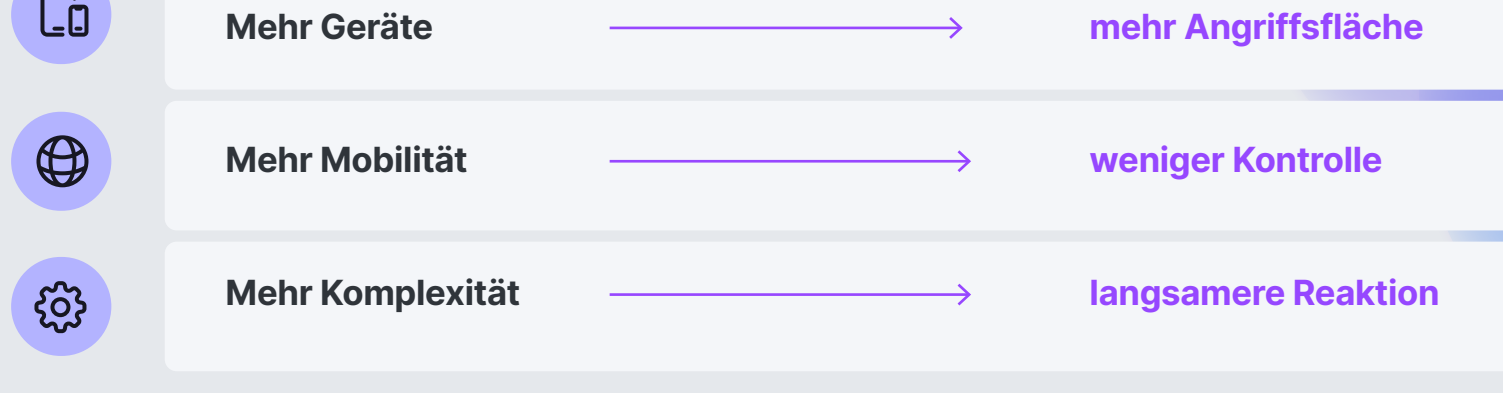
Die Sicherheitslücken werden immer größer. Wir zeigen Ihnen, wie Sie diese schließen können.



Hybrides Arbeiten, mobile Geräte und hochentwickelte Bedrohungen haben die klassische Perimetersicherheit ausgehebelt. Ein mehrstufiger Ansatz ist der richtige Weg.

WARUM ALTSYSTEME SCHEITERN

Die **Netzwerk**grenzen sind weg. Das **Risiko** ist noch da.



Cloud-Dienste, Remote-Arbeit, BYOD und nicht vertrauenswürdige Netzwerke haben die Grenzen aufgeweicht, für deren Schutz herkömmliche Tools konzipiert wurden.

BEDROHUNGSLANDSCHAFT

Die **Bedrohungen** von heute sind ausgeklügelt, konvergiert und unerbittlich.

| | | | |
|--|--|--|--|
| <p>Über 100 Mio. Kundendaten durch jüngste Sicherheitsverletzungen kompromittiert</p> | <p>2,1 Bio. Downloads mit bekannten Schwachstellen im Jahr 2023</p> | <p>25 Mio. USD Durch Deepfake-Kampagnen verloren, die auf den CFO abzielten</p> | <p>90 % der Angriffe exfiltrieren nun Daten, anstatt sie zu verschlüsseln</p> |
|--|--|--|--|

WICHTIGE BEDROHUNGSKATEGORIEN

| | | |
|---|---|---|
| <p>Social Engineering & Phishing E-Mail-, Spear-, Whaling-, Smishing-, Vishing- und QR-Code-Phishing sowie neuartige Techniken wie der vorgetäuschte Flugmodus und der vorgetäuschte Blockierungsmodus</p> | <p>Nationalstaatliche / APT-Angriffe 90 % der Warnungen stammen aus Bereichen außerhalb der kritischen Infrastrukturen Primäre Angriffsziele: Bildungssektor, Regierung und Think Tanks Durchschnittliche Kosten: 1,6 Mio. USD pro Vorfall</p> | <p>Angriffe auf die Lieferkette Verdreifacht 2023, wobei Partner und Lieferanten als indirekte Einstiegspunkte kompromittiert wurden</p> |
| <p>Mobile Bedrohungen 43 % der kompromittierten Geräte werden vollständig ausgenutzt (Anstieg um 187 % ggü. dem Vorjahr), 80 % der Phishing-Seiten zielen auf Mobiltelefone ab Malware für Mobilgeräte um 51 % gestiegen</p> | <p>KI-gestützte Bedrohungen 5 APT-Gruppen, die KI als Waffe einsetzen, um ihre Angriffsmöglichkeiten zu verbessern</p> | <p>5</p> |

NATIONALSTAATLICHE BEDROHUNGEN

Gezielte Angriffe nach Zahlen

| | |
|--|--|
| <p>Hauptangriffsziele nach Sektoren</p> <ul style="list-style-type: none"> Bildung 100 % Regierung 75 % Think Tanks/NGOs 69 % IT 69 % | <p>9 von 10 Unternehmen glauben, dass sie von staatlich unterstützten Akteuren angegriffen wurden</p> <p>1,6 Mio. USD durchschnittliche Kosten pro Vorfall</p> |
|--|--|

WARUM EINE EINHEITSLÖSUNG NICHT FÜR ALLE PASST

Die **Gerätelandschaft** hat sich verändert.

| | | | |
|--|---|---|---|
| <p>25% macOS-Marktanteil in den USA</p> | <p>96% der CIOs erwarten eine wachsende Mac-Flotte in den nächsten 12-24 Monaten</p> | <p>3,6 durchschnittliche Geräte pro Benutzer weltweit (2023)</p> | <p>96% der Mobilgeräte in Unternehmensnetzwerken befinden sich in Privatbesitz</p> |
|--|---|---|---|

MOBILGERÄTE: UNKONTROLLIERTES RISIKO

Mobilgeräte sind die **Eingangstüren**, die niemand bewacht.

Der durchschnittliche Benutzer hat 3,6 Geräte. Das sind 4 x mehr Angriffsvektoren pro Person, oft ohne speziellen Endpunktschutz.

| | | | |
|---|---|--|---|
| <p>43% der kompromittierten Geräte werden vollständig ausgenutzt (Anstieg um 187 % ggü. dem Vorjahr)</p> | <p>80% der Phishing-Seiten zielen auf mobile Geräte ab</p> | <p>51% Anstieg von spezifischer Mobile-Malware (mehr als 920.000 Varianten)</p> | <p>96% der Mobilgeräte in Unternehmensnetzwerken befinden sich in Privatbesitz</p> |
|---|---|--|---|

STRATEGISCHER RAHMEN

Die vier **K's** zum Schließen von Sicherheitslücken

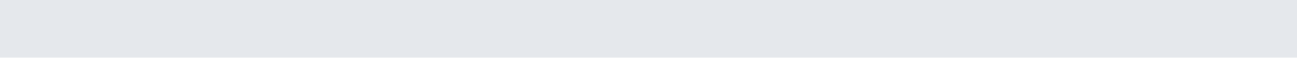
| | | | |
|---|---|--|--|
| <p>1. Consistency (Konsistenz) Behandeln Sie alle Endgeräte gleich, unabhängig von Gerätetyp, Umfaktor, Betriebssystem oder Eigentumsmodell.</p> | <p>2. Konformität Definieren Sie Baselines, überwachen Sie Abweichungen und führen Sie einen prüffähigen Nachweis mittels Telemetriedaten.</p> | <p>3. Consolidation (Konsolidierung) Vereinigen Sie IT und Sicherheit zu einem Team, um Silos aufzubrechen, Informationen auszutauschen und Arbeitsabläufe zu vereinheitlichen.</p> | <p>4. Cost Savings (Kosteneinsparungen) Steigern Sie Ihren ROI durch native Tools, Automatisierung, optimierte Prozesse und BYOD-Programme.</p> |
|---|---|--|--|

MEHRSCHICHTIGES SICHERHEITSMODELL

Defense-in-Depth = **Schichten**, die **auffangen**, was andere übersehen

Wenn eine Bedrohung eine Kontrolle umgeht, ist die nächste Schicht dazu da, sie zu stoppen. Die Integration dieser drei Säulen schafft durchgängige Sicherheitsbarrieren über Ihre gesamte Infrastruktur hinweg.

| | | |
|--|---|---|
| <p>Geräteverwaltung Bereitstellung von Konfigurationen, Durchsetzung von Richtlinien und Aufrechterhaltung der Kontrolle in großem Umfang</p> | <p>Identität & Zugriff Verifizierung der Benutzer und Geräte, bevor Zugriff auf geschützte Ressourcen gewährt wird</p> | <p>Endpunktsicherheit Erkennung von und Reaktion auf Bedrohungen auf jedem Gerät in Echtzeit</p> |
|--|---|---|



SCHLÜSSELTECHNOLOGIEN

Wie die **Schichten** in der Praxis funktionieren

| | | | |
|--|--|--|---|
| <p>Zero-Touch-Bereitstellung Geräte sind vom ersten Einschalten an gesichert. Konfigurationen, Apps und Richtlinien werden bei der Einrichtung von Unternehmens- und BYOD-Geräten automatisch bereitgestellt.</p> | <p>Bedrohungssuche Proaktive Erkennung unbekannter Bedrohungen durch Baselines, Telemetrie und automatisierte Workflows zur Behebung von Problemen.</p> | <p>ZTNA Niemals vertrauen, immer überprüfen. Verschlüsselte Mikrotunnel, Zugriff nach dem Prinzip der geringsten Berechtigungen und kontinuierliche Zustandsüberprüfungen ersetzen herkömmliche VPNs.</p> | <p>Erweiterte Reaktion auf Bedrohungen IoC/IoA-Analyse, Erstellung von Zeitplänen und Beseitigung von APTs. Die Zeiten für Untersuchungen wurden von mehreren Wochen auf wenige Minuten reduziert.</p> |
|--|--|--|---|

ERGEBNISSE

Warum dies wichtig ist

| | | | |
|--|---|---|--|
| <p>Stärkerer Schutz für alle Geräte</p> | <p>Schnellere Erkennung von und Reaktion auf Bedrohungen</p> | <p>Geringerer operativer Aufwand</p> | <p>Konsistente Sicherheit in verschiedenen Umgebungen</p> |
|--|---|---|--|

Entdecken Sie das komplette Framework für den Aufbau integrierter, mehrschichtiger Sicherheit in Ihrem Unternehmen.