AKAMAI-CHECKLISTE

Funktionen von Zero-Trust-Plattformen

Eine effektive Zero-Trust-Plattform kombiniert Lösungen in einer integrierten Plattform mit einziger Konsole, die vorher immer Einzellösungen waren. Diese Lösungen umfassen Zero Trust Network Access, Mikrosegmentierung, DNS-Firewall und Threat Hunting. Durch die schnelle und effektive Implementierung von Zero Trust können Sie Ransomware stoppen, anspruchsvolle Compliance-Anforderungen erfüllen und Remotemitarbeiter sowie Ihre Hybrid-Cloud-Infrastruktur schützen. Diese Checkliste kann zur Bewertung der Anbieterfunktionen oder als Anforderungsliste zur Implementierung von Zero Trust auf einer einzigen Plattform verwendet werden.

Kategorie 1: Anforderungen an die Plattform

Ihre Zero-Trust-Plattform sollte flexibel, skalierbar und einfach zu verwalten sein.

- [ ] Skalierbarkeit, um den Anforderungen des Traffics gerecht zu werden und kontinuierlichen Schutz ohne Performance-Einbußen zu bieten
- [ ] Möglichkeit zur Integration in vorhandene Sicherheitstools, die Kunden derzeit nutzen, wie z. B. SIEM, SOAR, EDR, CMDB und vieles mehr
- [ ] Abdeckung für heterogene Rechenzentren – hybride und Multicloud-Umgebungen, Legacy-Systeme, Endnutzergeräte, Kubernetes-Cluster, virtuelle Maschinen, IoT/OT-Umgebungen und vieles mehr
- [ ] Flexible Bereitstellungsmodelle, die verschiedene hybride Architekturen unterstützen – Cloud, virtuell, On-Premise
- [ ] Fähigkeit, sowohl agentbasierte als auch agentlose Bereitstellungen (IoT/OT, PaaS) zu unterstützen
- [ ] Unterstützung für Windows, Linux und macOS sowie ältere Betriebssysteme
- [ ] Auditprotokollfunktionen, die die Aufzeichnung aller Aktionen sicherstellen

Kategorie 2: Transparenzanforderungen

Eine umfassende Transparenz ist entscheidend für das Verständnis der Umgebung, die Erkennung von verdächtigen Verbindungen und eine schnelle und präzise Bedrohungsreaktion.

- [ ] Mapping-ähnliche Visualisierung aller Anwendungen und Workload-Flüsse sowie des Nutzerzugriffs zur Anwendung in jeder Umgebung – Container, serverlos, IaaS oder PaaS – und über eine einzige Konsole
- [ ] Verlaufs- und Echtzeitflüsse für Untersuchungen und Forensik
- [ ] Interoperabilität mit Firewalls und Hardware von Drittanbietern, wie z. B. Switches
- [ ] Möglichkeit zur Datenerhebung aus verschiedenen Drittanbieterquellen wie CMDB, EDR und Cloud-APIs für kontextbezogene Bezeichnungen und Regeln
- [ ] Unterstützung bei der Kennzeichnung, vorzugsweise mithilfe von KI für Geschwindigkeit und Genauigkeit

Kategorie 3: Richtlinienanforderungen

Sowohl East-West-Richtlinien (Mikrosegmentierung) als auch North-South-Richtlinien (Zero Trust Network Access) werden von einem Ort aus angewendet. Sie basieren auf Attributen, die in verschiedenen Anwendungsfällen genutzt werden können, wie z. B. Ransomware-Schutz, Schutz der Remotemitarbeiter, Reaktion auf Zero-Day-Schwachstellen und Compliance.

- [ ] Eine softwaredefinierte Richtlinie, die im gesamten Unternehmen verteilt ist, ohne dass interne physische Firewalls erforderlich sind, die für Flaschenhälse sorgen
- [ ] Regeln, die nach verschiedenen Workloadattributen statt nur anhand von IPs und Ports erstellt werden
- [ ] Detaillierte, anwendungsorientierte Richtlinien werden durchgesetzt, sodass Workloads auf Port-, Prozess- und sogar Service-Ebene geschützt sind
- [ ] Eine Engine für Richtlinienempfehlungen mit vorkonfigurierten und nutzerdefinierten Vorlagen, die vorzugsweise auf KI setzen, um die Richtlinienerstellung zu beschleunigen
- [ ] Richtlinien, die mit oder ohne Agent durchgesetzt werden
- [ ] Richtlinienkontrollen basierend auf einer umfassenden Flussübersicht
- [ ] Vorkonfigurierte Richtlinien für die globale Risikominderung basierend auf branchenbewährten Best Practices
- [ ] Richtlinie für Hybrid Cloud in virtualisierten, IaaS- und PaaS-Umgebungen
- [ ] Richtlinien, die an die Workload gebunden sind und bei Verschiebungen, Migrationen oder Änderungen befolgt werden können
- [ ] Zugriffsrichtlinie für Nutzer im Büro und Remotemitarbeiter

Kategorie 4: Zero-Trust-Komponentenanforderungen

Von den verschiedenen Funktionen, die in eine einheitliche Zero-Trust-Plattform integriert sind, heben sich Zero Trust Network Access und Mikrosegmentierung als Grundpfeiler hervor. Diese Technologien ermöglichen es Unternehmen, Zero-Trust-Kontrollen zu implementieren, ohne die Mitarbeiter oder die Geschäftskontinuität zu beeinträchtigen.

- [ ] Einheitliche Zugriffs- und Netzwerkrichtlinien-Engine (kombinierte East-West- und North-South-Kontrollen)
- [ ] Starke Identitätsdurchsetzung mit FIDO2-Multifaktor-Authentifizierung (MFA)
- [ ] Fähigkeit zum Schutz von IT-Umgebungen und Nutzern vor einer Vielzahl von Bedrohungen durch Überwachung und Filterung des DNS-Traffics
- [ ] Fortlaufende Erkennung gut getarnter Bedrohungen und Überwachung der Sicherheitslage
- [ ] Die Signalverteilung über die Plattformtools hinweg stellt sicher, dass ein Angreifer gestoppt wird, selbst wenn er den Zugriffsmechanismus umgehen kann
- [ ] Einführung dynamischer Täuschungssysteme, die Angreifer verfolgen und in Quarantäne verschieben können
- [ ] Möglichkeit, Endpunkte oder Server auf Sicherheitslücken abzufragen, um eine schnelle Ransomware-Erkennung und -Abwehr zu ermöglichen

Kategorie 5: Integrierte KI-Anforderungen

Viele Aspekte der effektiven Implementierung von Zero Trust können mit KI optimiert werden. Dies beschleunigt und vereinfacht die Richtlinienerstellung, die Compliance, die Vorfallsreaktion und die Schwachstellenbewertung.

- [ ] Kommunikation mit Netzwerkprotokollen in natürlicher Sprache, um die Zeit bis zur Vorfallsreaktion, für Compliance-Umfangsbestimmungen und vieles mehr zu reduzieren
- [ ] Optimierung des gesamten Richtlinienprozesses mit KI, die Kennzeichnungen und Richtlinien basierend auf Ihren individuellen Trafficmustern vorschlägt
- [ ] Übersetzung natürlicher Sprache in Syntax, um schnell nach Schwachstellen in Ihrem Netzwerk zu suchen, ohne IOCs durchsuchen oder nutzerdefinierte Abfragen schreiben zu müssen
- [ ] KI-Mechanismen zur Bedrohungssuche für erweiterte Erkennungsmethoden, um Anomalien und schädliche Aktivitäten zu finden, die herkömmliche Tools übersehen

Weitere Informationen finden Sie unter Zero-Trust-Sicherheit von Akamai.