

AKAMAI-PRODUKTBECHREIBUNG

Akamai Guardicore Segmentation

Stoppen von lateraler Netzwerkbewegung mit Kontrollen für detaillierte Transparenz und Mikrosegmentierung

Die IT-Infrastruktur von Unternehmen entwickelt sich von traditionellen On-Premise-Rechenzentren hin zu Cloud- und Hybrid-Cloud-Architekturen – mit vielen verschiedenen Plattformen und Anwendungsbereitstellungsmodellen. Obwohl diese digitale Transformation viele Unternehmen dabei unterstützt, ihre Geschäftsagilität zu steigern, die Infrastrukturkosten zu senken und Remote-Arbeit zu ermöglichen, schafft sie auch eine größere und komplexere Angriffsfläche ohne genau definierten Netzwerkperimeter. Jeder einzelne Server, jede virtuelle Maschine, jede Cloudinstanz und jeder Endpoint stellt jetzt ein potenzielles Risiko dar. Und mit der Verbreitung von Bedrohungen wie Ransomware und Zero-Day-Schwachstellen werden Angreifer immer geschickter, sich hochwertigen Ziele lateral anzunähern, wenn – nicht falls – sie einen Weg hineinfinden.

Akamai Guardicore Segmentation bietet den einfachsten, schnellsten und intuitivsten Weg zur Durchsetzung von Zero-Trust-Prinzipien in Ihrem Netzwerk. Die Lösung wurde entwickelt, um laterale Netzwerkbewegungen zu unterbinden. Dazu visualisiert sie Aktivitäten in Ihren IT-Umgebungen, implementiert präzise Richtlinien zur Mikrosegmentierung und erkennt mögliche Verstöße schnell.

Wichtigste Funktionen der Lösung

Detaillierte, KI-gestützte Segmentierung

Implementieren Sie Richtlinien mit wenigen Klicks anhand von KI-Empfehlungen, Vorlagen zum Umgang mit Ransomware und anderen gängigen Anwendungsfällen sowie präzisen Workload-Attributen wie Prozessen, Nutzern und Domainnamen

Echtzeit- und Verlaufstransparenz

Ordnen Sie Anwendungsabhängigkeiten und -flows den Nutzer- und Prozessebenen in Echtzeit oder auf Basis von Verlaufsdaten zu

Umfassende Plattformunterstützung

Decken Sie moderne und ältere Betriebssysteme über Bare-Metal-Server, virtuelle Maschinen, Container, IoT und Cloudinstanzen ab

Flexible Kennzeichnung von Assets

Fügen Sie umfangreichen Kontext mit einer anpassbaren Kennzeichnungshierarchie für Transparenz und Durchsetzung hinzu und integrieren Sie Orchestrierungstools und Konfigurationsverwaltungsdatenbanken für automatisiertes Kennzeichnen

Mehrere Schutzmethoden

Sie können Threat Intelligence, Abwehrmaßnahmen und Angriffserkennung integrieren und so die Reaktionszeit bei Vorfällen reduzieren

VORTEILE FÜR IHR UNTERNEHMEN



Verhindern von Ransomware



Erreichen von Zero Trust



Schnellere Compliance



Abschirmen kritischer Anwendungen



Sichern der Cloudmigrationen



Schutz des Remotezugriffs für Mitarbeiter



Schützt Endpoints



Geht über interne Firewalls hinaus



Umfassender Schutz in großem Maßstab



Jede Umgebung

Schützen Sie Workloads in komplexen IT-Umgebungen – verfügbar für Kombinationen aus On-Premise-Workloads, virtuellen Maschinen, Legacy-Systemen, Containern und Orchestrierung, Public/Private-Cloud-Instanzen sowie IoT/OT



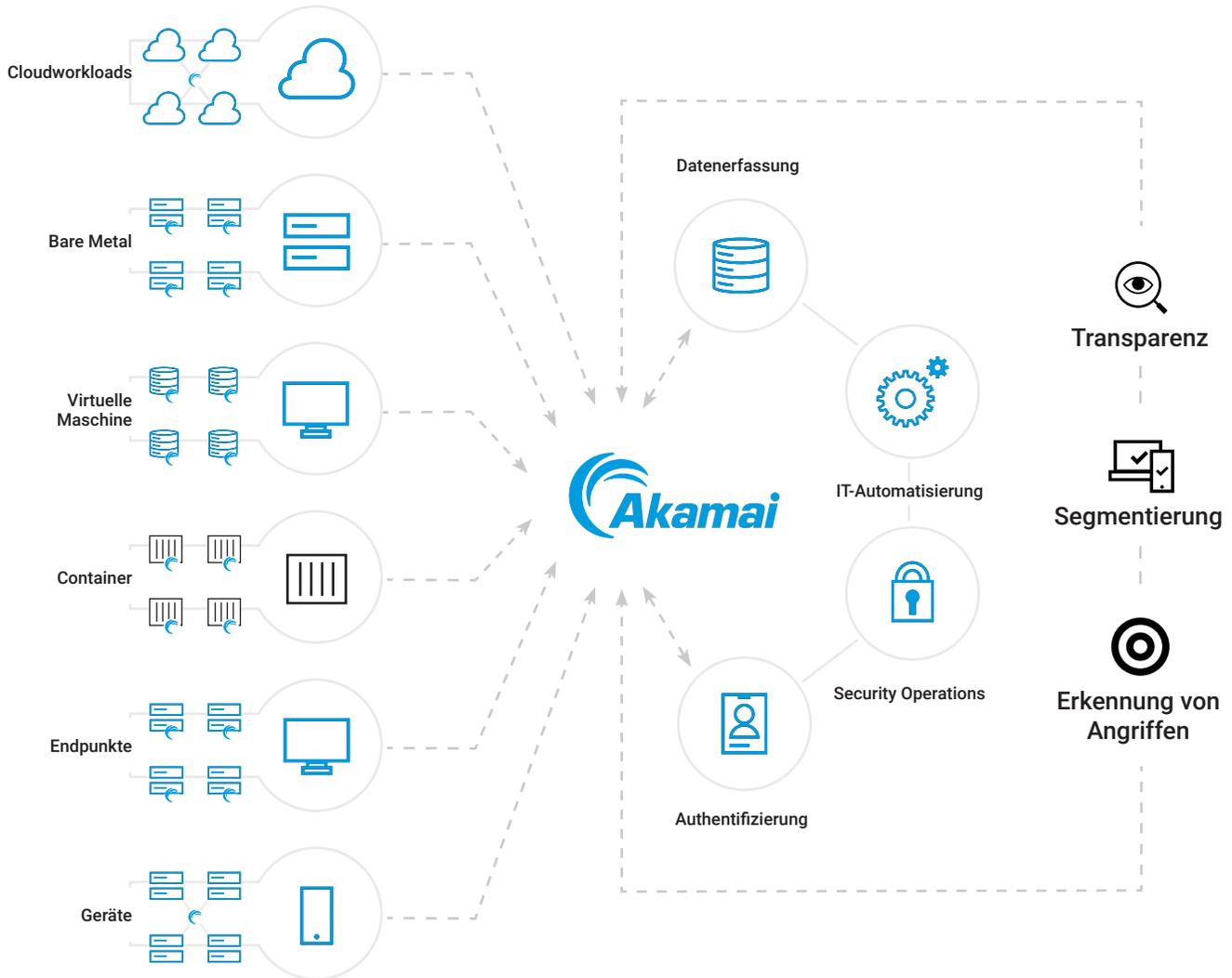
Einfachere Sicherheit

Vereinfachen Sie das Sicherheitsmanagement mit einer einzigen Plattform, die Netzwerkvisualisierung, Segmentierung, Bedrohungsabwehr, Erkennung von Sicherheitsverletzungen und geführte Richtlinien durchsetzung für Zero-Trust-Initiativen bietet



Skalierbarkeit und Performance für Unternehmen

Beginnen Sie mit dem gezielten Schutz Ihrer wichtigsten digitalen Assets – durch Skalierung können Sie Ihr gesamtes Unternehmen ohne Komplexität, Infrastrukturänderungen oder Performanceengpässe schützen



Unterstützte Plattformen und Technologien

- Akamai Guardicore Segmentation wurde für die Integration in Ihre vorhandene Infrastruktur entwickelt.
- Die unterstützten Betriebssysteme werden kontinuierlich an die Bedürfnisse unserer Kunden angepasst.
- Auf unserer [Seite für Technologiepartner](#) finden Sie die vollständige Liste unserer Integrationen.

Betriebssysteme

Linux



Apple



Microsoft



Unix



Public-Cloud-Provider



Hypervisoren



Hypervision-Orchestrierung



Sicherheits-Gateways



Container-Orchestrierung und Engines



Browser für Webkonsolen



Mindestanforderungen an Speicher und System

Management Server 32 GB RAM, 8 vCPUs, 530 GB	Aggregator 4 GB RAM, 4 vCPUs, 30 GB
Deception Server 32 GB RAM, 8 vCPUs, 100 GB	ESC Collector 2 GB RAM, 2 vCPUs, 30 GB

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

Weitere Informationen über Akamai Guardicore Segmentation oder eine personalisierte Produktdemo erhalten Sie unter akamai.com/guardicore.