Calico-Cloud: Aktive Plug-and-Play-Containersicherheit

In Containern und Kubernetes laufende cloudnative Anwendungen kommen über ihren gesamten Lebenszyklus mit einer großen Angriffsfläche daher, von der Entwicklung über die Bereitstellung bis hin zum produktiven Einsatz. Diese große Angriffsfläche, kombiniert mit der hochdynamischen und kurzlebigen Natur cloudnativer Auslastung, erfordert eine neue Einstellung gegenüber der Sicherheit.

Die Calico-Cloud ist eine Containersicherheitsplattform der nächsten Generation, die ein Gleichgewicht zwischen Prävention und Risikominimierung mit Bedrohungserkennung bietet, um die Angriffsfläche zu verkleinern und aktiv Bedrohungen zu erkennen sowie abmildernde Sicherheitskontrollen tätigt, um die Risiken einer Gefährdung zu begrenzen. Die Calico-Cloud ist die einzige aktive Sicherheitsplattform der Branche mit vollständiger Beobachtbarkeit des Systems. Sie erlaubt es Organisationen, durch Zero-Trust Angriffe zu vermeiden sowie Risiken aus Sicherheitslücken über Multi-Cloud- und Hybrid-Umgebungen hinweg zu erkennen, Fehler zu korrigieren und die Gefahr automatisch zu beheben. Die Calico-Cloud basiert auf Calico-Opensource, der verbreitetsten Container-Networking- und Sicherheitslösung.

Sicherheitstechnische Herausforderungen

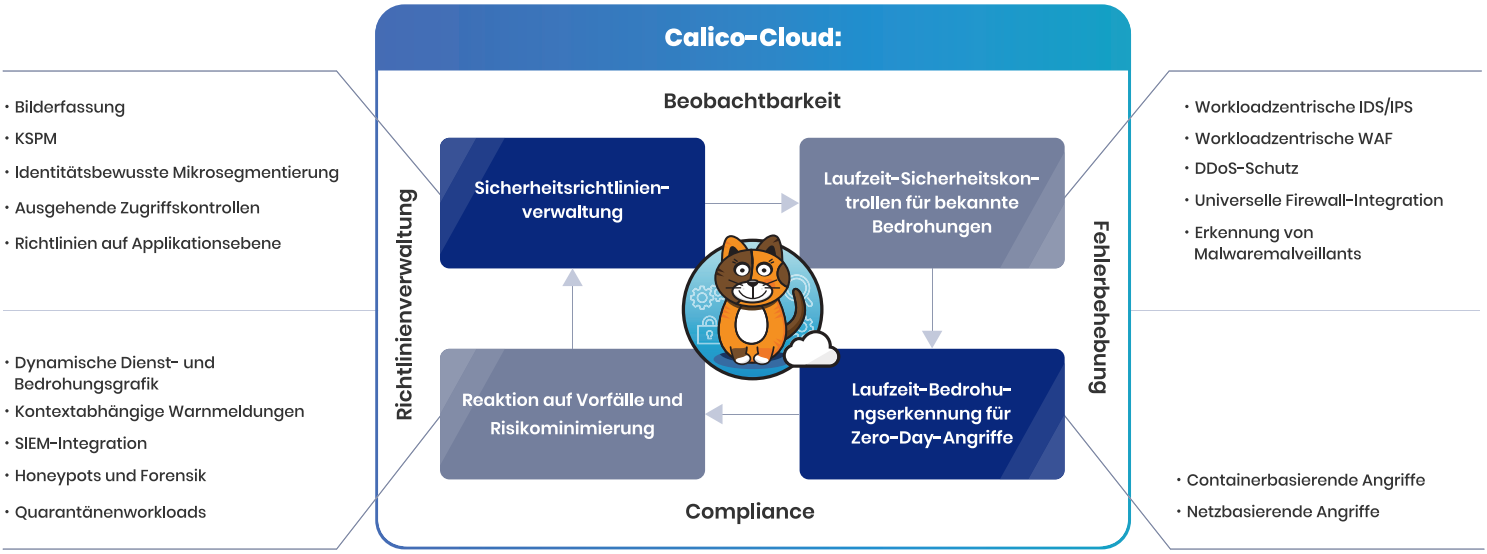
- Große Angriffsfläche über den gesamten Applikationslebenszyklus hinweg
- Fehlende Sichtbarkeit führt zu blinden Flecken hinsichtlich Sicherheit
- Entdeckungsorientierte Sicherheit erzeugt False Positives, die zu Desensibilisierung führen und Sicherheitsteams überfordern
- Die Umsetzung der Vorgaben von as SOC 2, PCI DSS und HIPAA ist arbeitsintensiv
- Angesichts des Kubernetes-Netzes ist die traditionelle Perimetersicherheit unzureichend

Wie Calico Abhilfe schaffen kann

Calico ist branchenweit die einzige aktive Plug-and-Play-Sicherheitsplattform mit Full-Stack-Beobachtungsfähigkeit, um Sicherheitslücken in Applikationscontainern zu vermeiden, erkennen und beheben.

Angriffsfläche reduzieren	Angriffe erkennen und aufhalten	Risiken aktiv minimiere
Zugriffe und Kommunikation innerhalb und außerhalb des Clusters absichern, um Angriffe abzuwehren	Zugriffe vor bekannten und Zero-Day-Bedrohungen in Containern und dem Netz zur Laufzeit abschirmen	Empfohlene Sicherheitskontrollen in Kraft setzen, um Risiken zu minimieren

Wie Calico Containersicherheit umwandelt



Robuste Sicherheitslage für Containerzugriffe

Automatisiertes Schwachstellenmanagement

Images kontinuierlich nach bekannten CVEs absuchen und anfällige Zugriffe mittels einer automatisierten, vollintegrierten CI/CD-Pipeline unterbinden. Verwendung der Laufzeitansicht anfälliger Zugriffe zur Risikobewertung und Bereitstellung abmildernder Sicherheitskontrollen zur Schadensminimierung.

Kubernetes-Sicherheitslagenmanagement (KSPM)

Härten Sie Ihre Kubernetes-Umgebung gegen branchenübliche CIS-Benchmarks, um Fehlkonfigurationen über Ihre dynamischen Kubernetes-Umgebungen hinweg zu erkennen und zu beheben.

Zero-Trust-Zugriffskontrollen

Richten Sie fein abgestimmte Zero-Trust-Zugriffskontrollen zwischen einzelnen Abschnitten in Kubernetes-Clustern auf externe Ressourcen ein, wie z.B. Datenbanken, interne Applikationen, 3rd-Party-Cloud-APIs und SaaS-Applikationen. Sichern Sie Abschnitte mittels fein abstimmbarer Richtlinien für ausgehende DNS-Abfragen und NetworkSets.

Identitätsbewusste Mikrosegmentierung

Sichern Sie Lateralkommunikation zwischen Abschnitten, Namensräumen und Diensten ab. Erreichen Sie Zugriffsisolierung basierend auf Umgebungen, Applikationsebenen, Complianceanforderungen, Nutzerzugriffen sowie individuellen Anforderungen.

Richtlinien auf Applikationsebene

Setzen Sie Richtlinien auf Applikationsebene zur Mikrosegmentierung und Zugriffskontrolle mit L7-spezifischen Attributen wie z.B. HTTP-Methoden und URL-Pfaden um.

Schutz vor bekannten Bedrohungen zur Laufzeit

Workloadzentrische IDS/IPS

Unterbinden Sie die Kommunikation mit bekannten bösartigen IPs und erhalten Sie Alarme über verdächtige Domains durch Integration globaler Bedrohungsintelligenz.

Workloadzentrische WAF

Schützen Sie Ihre Zugriffe vor HTTP-basierten Angriffen wie z.B. OWASP Top Ten und anderen abnormalen HTTP-Headern, insbesondere bei Lateralkommunikation.

Erkennung von Malware

Malware erkennen und gewarnt werden - Mit einem signaturbasierten Ansatz. Entdecken Sie Ransomware und Cryptominer mit Hilfe kuratierter Erkennungsfähigkeiten und Warnungen.

DDoS-Schutz

Verhindern Sie DDoS-Angriffe und mildern Sie deren Folgen ab - Mit Hilfe von Sicherheitsrichtlinien auf Host- und Applikationsebene.

Universelle Firewall-Integration

Erweitern Sie zonenbasierende Architekturen (trusted/untrusted/DMZ) auf Kubernetes. Schützen Sie cloudnative Kubernetes-Zugriffe mittels vertrauter Tools, Prozesse und Sicherheitsworkflows, die Sie aus der kubernetesfremden Welt kennen.

Schutz vor Zero-Day-Bedrohungen zur Laufzeit

Netzbasierende Erkennung von Anomalien und Zero-Day-Angriffen

Halten Sie Zero-Day-Angriffe mit Hilfe heuristikbasierenden Lernens anomaler Netzaktivitäten auf. Erkennen Sie in Datenfluss-, DNS- und HTTP-Zugriffsprotokollen Anzeichen von Angriffen (IoA).

Containerbasierende Erkennung von Anomalien und Zero-Day-Angriffen

Erkennen Sie Zero-Day-Angriffe heuristisch und out-of-the-box durch Analyse von Containeraktivitäten mittels Prozess-, Dateisystem- und Systemaufrufen, die durch eBPF-Sonden gesammelt werden.

Reaktion auf Vorfälle und Risikominimierung

Überwachbarkeit und Fehlerbehebung

Verschaffen Sie sich einen umfassenden Überblick durch eine grafikbasierte Veranschaulichung Ihrer Kubernetes-Instanzen, Bilder, Abschnitten, Namensräumen und Diensten mit Calicos dynamischer Dienste- und Bedrohungsgrafik. Speziell angefertigt mit Fehlerbehebungsfunktionen zur Erkennung und Behebung von Sicherheits- und Compliancelücken, Performanceproblemen, Konnektivitätsverlusten, anomalem Verhalten und Verletzungen von Sicherheitsrichtlinien.

Warnungen und Quarantäne

Betrachten und verwalten Sie sämtliche sicherheits-, netzwerk- und performancebezogenen verwertbaren Warnungen von einer einzigen Stelle aus: Ihrem Dashboard mit anpassbaren Filtern. Setzen Sie Quarantänerichtlinien ein, um verwundbare Zugriffe zu isolieren und so Schritte zur Fehlerbehebung zu ermöglichen.

Verwaltung und Compliance

Datenflussverschlüsselung mit Hilfe von WireGuard

Bekämpfen Sie die Betriebskomplexität von Standard-Verschlüsselungslösungen durch die Integration von Calicos WireGuard. Erfüllen Sie gesetzliche Vorgaben hinsichtlich Verschlüsselung, wie z.B. SOX, HIPAA, GDPR und PCI DSS.

Compliance (PCI DSS, SOC 2, GDPR, HIPAA, benutzerdefinierte Frameworks und vieles mehr)

Erreichen Sie Compliance und behalten Sie diese bei durch kontinuierliche Echtzeitüberwachung zur Erkennung von Störungen und erzeugen Sie auditfertige Berichte. Unterstützt PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA und benutzerdefinierte Frameworks.

Sicherheitsrichtlinienverwaltung

Erstellen, Bereitstellen, Voransehen, Erzwingen und Verwalten von Sicherheitsrichtlinien mit Hilfe unseres einheitlichen Richtlinienframeworks. Calico empfiehlt die Verwendung von Richtlinien und bietet hierfür auf Rollen und Berechtigungen basierende Hierarchieebenen. Das Verwaltungs-UI verfügt über ein Richtlinienboard, damit Teams alle aktiven und inaktiven Sicherheitsrichtlinien des Kubernetes-Clusters ganz einfach ansehen und verwalten können.

Kunden

Sammeln Sie praktische Erfahrungen auf unseren bald stattfindenden Webinaren und Live-Online-Workshops.

Los geht's

TIGERA

Tigera, Inc.

58 Maiden Lane, Fl 5
San Francisco, CA 94108
+1 (415) 612-9546 / www.tigera.io