DATENBLATT

Infoblox für Telekom-Sicherheitsgruppen

Verbessern Sie die Effektivität und Ausfallsicherheit Ihrer Sicherheit und steigern Sie die Effizienz Ihrer SecOps

DIE HERAUSFORDERUNG

Die Netzwerke der heutigen Kommunikationsdienstanbieter (CSP) entwickeln sich zu Telco-Clouds, die private, öffentliche und hybride Netzwerke umfassen und die Betriebsdomänen über das RAN, Kabel- und Kernnetze, private und öffentliche Clouds sowie Multi-Access-Edge-Standorte erweitern. Da Rechenleistung und Speicher an den Rand verlagert werden, um neue Arten der Dienstverarbeitung und -bereitstellung an Tausenden neuer Standorte zu ermöglichen, steigt das Potenzial für Sicherheitsbedrohungen sowohl durch Anwendungen von Drittanbietern als auch durch externe Angreifer erheblich. Betreiber speichern große Mengen personenbezogener Daten und sind für die Stabilität ihrer Kommunikationsdienste verantwortlich. Der weit verbreitete Einsatz von Geräten außerhalb des Rechenzentrums legt auch eine zunehmende Anzahl von Zugriffspunkten offen und schafft eine massive Angriffsfläche, die von Angreifern ausgenutzt werden kann. Eine Datenverletzung oder ein Dienstausfall infolge eines Cyberangriffs kann zu erheblichen finanziellen Einbußen und Reputationsschäden führen oder Auswirkungen auf Kunden haben – ein schwerer Schlag für jedes Unternehmen, um in einem wettbewerbsintensiven Markt zu bestehen.

Da immer mehr Ressourcen am äußersten Rand bereitgestellt werden, müssen die IT- und Sicherheitsteams der Betreiber deutlich mehr Pods, virtuelle Maschinen – manchmal Hunderte gleichzeitig und möglicherweise Tausende von Containern – in physischen, virtuellen und Cloud-Umgebungen verwalten. Ungepatchte Geräte können zu Kompromittierungspunkten werden. Und während Endpunktschutz mit Erkennungs- und Reaktionsfunktionen unverzichtbar ist, müssen bereits stark beanspruchte Sicherheitsteams die Anzeichen eines Angriffs in einem sich ständig weiterentwickelnden und wachsenden Netzwerk unbedingt erkennen. CSPs benötigen ausgereifte Cybersicherheitslösungen, die ihre Sichtbarkeit erweitern, um moderne Bedrohungen zu erkennen, Untersuchungen zu verkürzen und eine effiziente Reaktion auf Vorfälle zu beschleunigen.

DIE LÖSUNG

Die Lösungen von Infoblox für Service-Provider unterstützen die entscheidenden IP-Verbindungen zwischen Ihren Abonnenten und deren digitaler Welt. Wir vereinen DNS, DHCP und IP-Adressverwaltung (DDI), um die Sichtbarkeit, Skalierbarkeit und Verwaltung von Netzwerken zu automatisieren. Unsere Lösungen helfen dabei, die Reaktionszeiten bei Vorfällen um zwei Drittel zu verkürzen, indem sie es allen wichtigen Komponenten Ihres Sicherheits-Stacks, einschließlich der Systeme für Sicherheit, Orchestrierung, Automatisierung und Reaktion (SOAR), ermöglichen, schneller auf Sicherheitsereignisse zu reagieren, bevor diese Schaden anrichten. Wir helfen Anbietern auch dabei, Geschäftsunterbrechungen durch DDoS und andere DNS-basierte Risiken und Angriffe zu minimieren.

WICHTIGE FÄHIGKEITEN

Verstärkter Sicherheitsschutz
Erkennen und blockieren Sie Exploits, Phishing, Ransomware und andere moderne Malware, die andere Lösungen übersehen.

Erhöhen Sie die Transparenz
Verschaffen Sie sich präzise Transparenz und einen umfassenden Netzwerkkontext, indem Sie die Asset-Metadaten der IP-Adressverwaltung integrieren, um ein optimales Ereignisverständnis und eine optimale Korrelation zu erzielen.

Beschleunigen Sie die Reaktion auf Vorfälle
Reduzieren Sie die Zeit bis zur Remediation, indem Sie Ereignis-, Netzwerk- und Bedrohungsinformationen aus Dutzenden von Quellen automatisch korrelieren und so die Untersuchungen um bis zu zwei Drittel beschleunigen.

Verbessern Sie den Sicherheits-ROI
Erkennen Sie mit minimalem Aufwand den maximalen Wert durch stärkere Abwehrmaßnahmen und größere Effizienz in Sicherheitsoperationen – und nutzen Sie Ihre SIEM- und SOAR-Plattformen sowie andere Sicherheitswerkzeuge optimal aus.

Infoblox senkt die Gesamtkosten für Ihre Bedrohungsabwehr, da die Beanspruchung der überlasteten Perimeter-Verteidigung reduziert wird. Unsere Lösungen ermöglichen es Sicherheitsteams, den Wert bestehender Sicherheitslösungen von Drittanbietern durch den wechselseitigen Echtzeit-Austausch von Informationen zu Sicherheitsereignissen und durch Automatisierung zu steigern, wodurch die Kosten für manuelle Arbeit und menschliche Fehler gesenkt werden. Sicherheitsanalysten können sich einen einheitlichen Überblick über die mit einem Ereignis verbundenen Bedrohungsinformationen verschaffen und die Zeit für die Bedrohungsuntersuchung um bis zu zwei Drittel verkürzen.

WICHTIGE VORTEILE

Stoppen Sie Bedrohungen, die andere Abwehrmaßnahmen übersehen

Bessere Bedrohungsinformationen sorgen dafür, dass jedes Sicherheitstool effektiver ist. BloxOne® Threat Defense erfasst, kuratiert und aggregiert Bedrohungsinformationen von Infoblox, Ihren anderen kommerziellen Tools sowie von Drittanbietern und staatlichen Quellen. Die Vorabauswahl durch die Infoblox Cyber Intelligence Unit (CIU) erhöht die Genauigkeit und minimiert Fehlalarme, sodass Sie die Zusammenstellung auf Ihre Bedürfnisse abstimmen können. Ein normalisierter „Super-Feed“ kann dann im gesamten Sicherheitsstack genutzt werden, um die Effektivität jeder Verteidigungsmaßnahme zu erhöhen.

Blockieren von Malware und Datenexfiltration

BloxOne Threat Defense arbeitet auf der DNS-Ebene, um Bedrohungen zu erkennen, die andere Lösungen nicht sehen, und stoppt Angriffe früher im Bedrohungslebenszyklus. Blockieren Sie den Zugriff auf bösartige Websites, Command-and-Control-Kommunikation (C&C), DNS-basierten Datendiebstahl und andere bösartige Aktivitäten, indem Sie Threat Intelligence aus verschiedenen Quellen und leistungsstarke KI/ML nutzen.

Geschäftsunterbrechungen minimieren

Das DNS ist für jedes Unternehmen von grundlegender Bedeutung, da es die geschäftskritische Netzwerkkonnektivität sicherstellt. Wenn Ihr DNS ausfällt, funktioniert in Ihrem Unternehmen nichts mehr. Erfolgreiche DDoS-Angriffe können ein Unternehmen Hunderttausende von Dollar an entgangenen monatlichen Einnahmen kosten. Infoblox Advanced DNS Protection (ADP) schützt Sie effektiv vor einer breiten Palette an DNS-DDoS-Angriffen und sorgt so dafür, dass die Dienstleistungen Ihres Unternehmens jederzeit verfügbar bleiben.

Schnelle Untersuchung und Behebung

Analysten benötigen Zugriff auf vertrauenswürdige Bedrohungsinformationen und andere kontextbezogene Daten zu einem Ereignis, um schneller reagieren zu können. Mit Dossier™ als Teil von BloxOne Threat Defense erhalten Analysten einen zentralen Überblick über die mit einem Ereignis verbundenen Bedrohungsdaten. Der schnelle Zugriff auf ereignisspezifische Informationen kann Bedrohungsuntersuchungen um bis zu zwei Drittel beschleunigen.

Optimierung von SIEM, SOAR und mehr

Ausgestattet mit einer Vielzahl von Defense-in-Depth-Tools können Cybersicherheitsteams mit der Notwendigkeit überfordert sein, Dutzende von Sicherheitstools manuell zu verwalten und täglich auf Hunderte oder Tausende von Warnungen zu reagieren. Die Ecosystem Exchange von Infoblox bietet eine Reihe von hochgradig vernetzten Integrationen, die es Sicherheitsteams ermöglichen, Silos zu beseitigen, ihre SIEM- und SOAR-Lösungen zu optimieren und den ROI ihres gesamten Cybersecurity-Ecosystems zu verbessern.

Reduzieren Sie den Sicherheitsaufwand
Nutzen Sie umfassende Ereignis-, Bedrohungs- und KI/ML-basierte Analysen im DNS für einen skalierbaren Schutz gegen moderne Malware und DNS-Bedrohungen.

Minimieren Sie Netzwerkunterbrechungen
Bewahren Sie die DNS-Integrität und stoppen Sie externe und interne DNS-DDoS-Angriffe, die Ihr Netzwerk lahmlegen können.

Entlastung der SecOps durch Automatisierung

BloxOne Threat Defense umfasst viele Funktionen, die es Ihnen ermöglichen, Bedrohungsinformationen, Ereignisinformationen und andere Daten intelligenter zu nutzen. Die Automatisierung eliminiert den Verwaltungsaufwand, macht aber auch die SecOps-Untersuchungs- und Reaktionsaufgaben effizienter. Reduzieren Sie die Belastung überlasteter Perimeter-Sicherheitsgeräte wie Firewalls, IPSs und Web-Proxys, indem Sie Ihre bereits verfügbaren DNS-Server als erste Verteidigungslinie nutzen.

Vereinfachen und optimieren Sie das Netzwerkänderungs- und Konfigurationsmanagement

Die Ursachen vieler Netzwerkprobleme lassen sich auf Änderungen zurückführen – Fehler, die beim manuellen Wechseln von Geräten gemacht werden, die Einstellung schlechter Konfigurationen, die später zu Problemen führen, und die Untergrabung wichtiger Sicherheitsrichtlinien und des Netzwerkschutzes. Infoblox NetMRI ist eine Lösung für die Verwaltung von Netzwerkänderungen und -konfigurationen, die Routineabläufe wie die Gerätebereitstellung und Sicherheitsvorgänge automatisiert und so eine strengere Compliance und schnellere Reaktion auf Vorfälle ermöglicht.

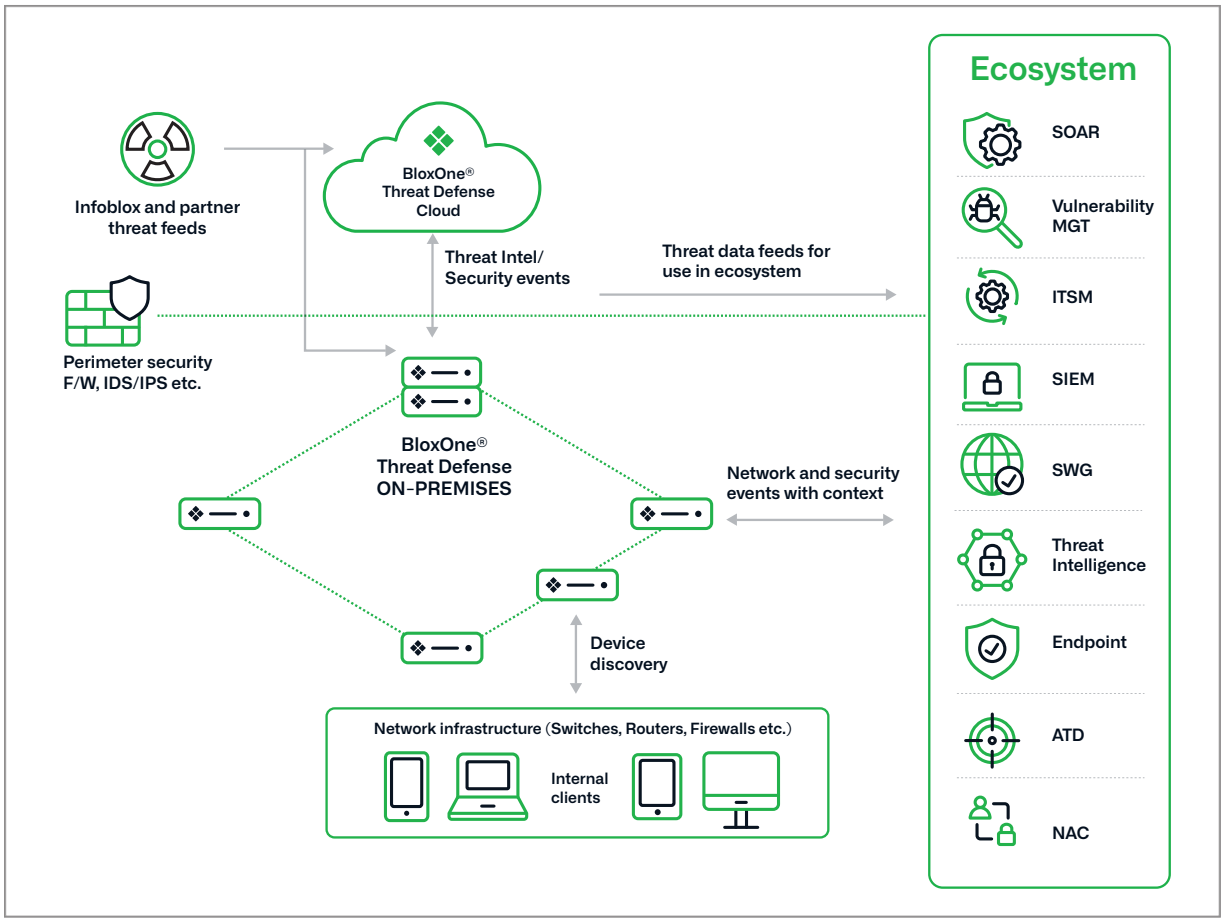

Abbildung 1: Infoblox stärkt und optimiert die Netzwerke von Kommunikationsdienstanbietern

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1 408 986 4000
www.infoblox.com/de

Version: 20240521v1