Datenblatt

Arbor Networks Spectrum™ mit NETSCOUT ISNG

BREITES SPEKTRUM. SCHNELLE ERGEBNISSE.

Die Angriffslandschaft hat sich verändert. Angriffswerkzeuge wie Malware, die anfangs verwendet wurden, um die Funktionsfähigkeit eines Netzwerks zu beeinträchtigen, sind längst nicht mehr die bevorzugten Waffen. Heute verschaffen sich Angreifer Zugriff auf Benutzeraccounts und manipulieren häufig verwendete IT-Anwendungen oder Betriebssysteme, indem sie konventionelle Sicherheitsmaßnahmen am Perimeter umgehen. Die durchschnittliche Zeit bis zur Erkennung eines Angriffs (Mean Time to Detect, MTTD) beträgt in der Regel mehr als 150 Tage, während die Angreifer weniger als 10 Minuten brauchen, um eine Angriffskampagne im Netzwerk zu starten.

Befindet sich ein Angreifer bereits im Netzwerk, kann mit Arbor Networks Spectrum™ die mittlere Zeit, die ein Sicherheitsteam benötigt, um das Vorliegen eines Angriffs zu bestätigen (Mean Time to Know, MTTK) deutlich reduziert werden. Dies ermöglicht eine schnelle Reaktion, um den Angriff abzuwehren bzw. einzudämmen. Arbor Spectrum bietet nicht nur differenzierte Einblicke in alle Netzwerkaktivitäten, sondern ermöglicht auch die zeitnahe Aufdeckung von kritischen Sicherheitsvorfällen. Durch die Automatisierung und Koordinierung der Workflows für die Reaktion auf Vorfälle und der Workflows für die einzuleitenden Sicherheitsmaßnahmen werden die Sicherheitsteams gestärkt und können mit ihren Mitarbeitern und Ressourcen effizienter arbeiten.

Breites Spektrum

Arbor Spectrum bietet umfassende Netzwerktransparenz gepaart mit sehr präzisen Sicherheitsinformationen, die von ATLAS™ (Active Threat Level Analysis System) durch die Analyse eines Drittels des weltweiten Internetverkehrs ermittelt werden. Die Kombination aus ATLAS-Transparenz und ATLAS-Daten-Policies, die ständig mit den aktuellsten Sicherheitsinformationen aktualisiert werden, geben den Kunden höchst zuverlässige Einblicke in Bedrohungen, die in und um ihre Netzwerke vorhanden sind.

Schnelle Ergebnisse

Arbor Spectrum verfügt über ein High-Performance-Archiv mit Echtzeitinformationen zum Datenverkehr, sodass wichtige Erkenntnisse schneller gewonnen werden können. Durch die Integration von ISNG mit der ASI-Technologie, einer industrieweit führenden Technologie zum Sammeln und Analysieren von Netzwerk- und Applikationsmetadaten, sind differenzierte Einblicke in und Analysen von Protokoll-, Anwendungs- und Netzwerkdaten möglich. Mit integrierten Workflows für die Analyse, einer schnellen Suchfunktion und einfachen Pivot-Darstellungen vergangener Netzwerk- und Benutzeraktivitäten über mehrere Monate lassen sich zeitintensive Arbeiten in wenigen Sekunden erledigen.

—

„Es gibt keine Wunderwaffe für die IT-Sicherheit, doch Arbor Spectrum liefert uns echte Ende-zu-Ende-Transparenz, die wir bisher nie hatten und die andere Lösungen nicht bieten."

„Wir sind sehr zufrieden mit dem Funktionsumfang von Arbor Spectrum. Mit dieser Lösung konnten wir unsere MTTD beträchtlich reduzieren."

LEITENDER SICHERHEITSINGENIEUR BEI EINEM GROSSEN FINANZDIENSTLEISTER

ARBOR® NETWORKS

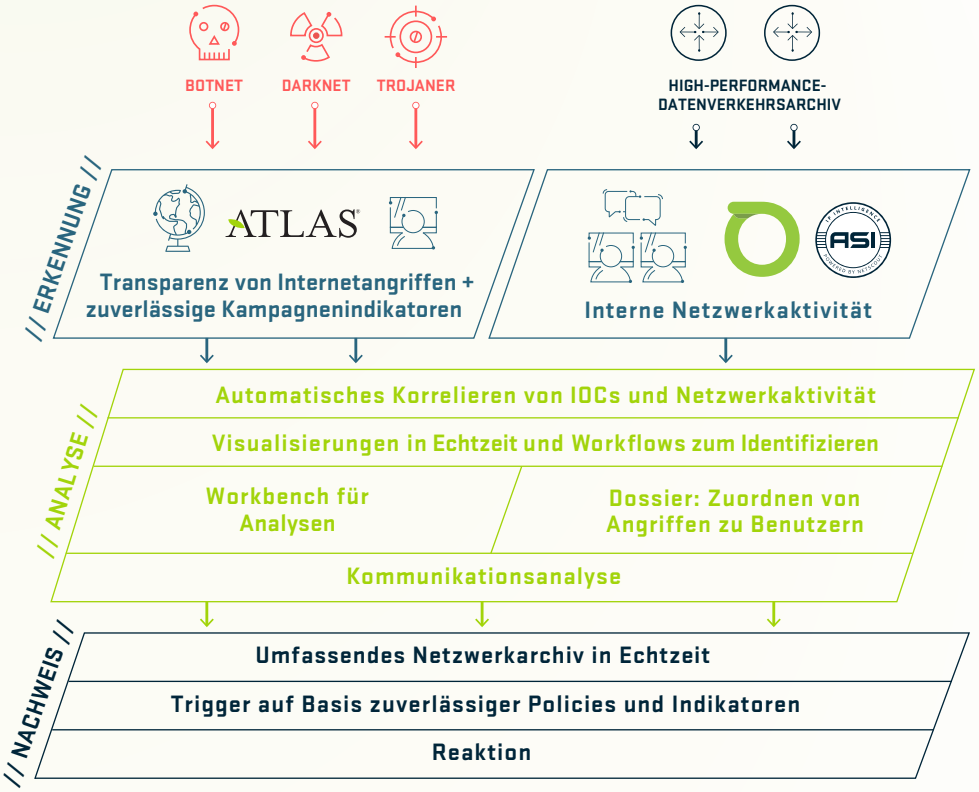
The Security Division of NETSCOUT

Funktionsweise von Arbor Spectrum

Arbor Spectrum nutzt die von ATLAS weltweit erhobenen Sicherheitsinformationen in Verbindung mit kundeneigenen Erkenntnissen über Angriffe und Datenverkehrsmuster, um schwerwiegende Bedrohungen zu erkennen, zu analysieren und nachzuweisen. In Kombination mit NETSCOUT ISNG mit der ASI-Technologie und/oder Arbor Spectrum Flow Collection mit Active Directory kann Arbor Spectrum interne Netzwerkaktivitäten aufdecken.

Abbildung 1:

Funktionsweise von Arbor Spectrum



ERKENNUNG

- Relevante Indikatoren zum Starten der Analyse
- Neue Bedrohungen durch Indikatoren von ATLAS Intelligence
- Importieren von STIX-Feeds zum Anwenden der bereitgestellten Informationen zu Bedrohungen
- Retrospektive Analyse, um das Archiv nach neu identifizierten Indikatoren zu durchsuchen

Indikatoren von ATLAS Intelligence

ATLAS ist die weltweit größte Datensammlung, die Live-Einblicke in die Telemetriedaten des Internetverkehrs ermöglicht (es wird etwa ein Drittel des gesamten Datenverkehrs erfasst). Mithilfe von ATLAS kann Arbor die Stärke von Angriffsaktivitäten im Internet beobachten, die Angriffsmuster analysieren und als zuverlässige Indikatoren für Sicherheitsrisiken stündlich an Arbor Spectrum übermitteln.

ANALYSE

Priorisierung von Indikatoren

Trends bei neuen Netzwerkaktivitäten und Indikatoren werden in Echtzeit visualisiert und können Gruppen zugeordnet werden (u. a. Benutzer, Geschäftsfunktion und Standort).

Modul „Investigations“

Verwandte Indikatoren, Host-Profile und Netzwerkverbindungen können aggregiert und als Gesamtansicht einer komplexen Bedrohung dargestellt werden.

Host-Dossier mit Benutzer-ID/ Activity-Directory-Integration

- Individuelle Workflows identifizieren und verfolgen verdächtige Aktivitäten im Netzwerk
- Detaillierte Ansicht der Netzwerkkommunikation zwischen Hosts und relevanten Verbindungspunkten

NACHWEIS

Automatische PCAP-Funktionalität für alle IoCs (Indicators of Compromise)

Innovative, automatisierte Forensik durch Speichern der PCAPs aller identifizierten Indikatoren. Dadurch wird die Forensik skalierbar und kosteneffizient.

Manuelle PCAP-Funktionalität für alle Hosts bzw. Kommunikationen

Upload oder Auslösen eines PCAP für alle Hosts bzw. Kommunikationen, die beim Aufspüren bzw. bei der Analyse entdeckt werden.

Integration mit führenden SIEM-Plattformen

Die aufgezeichneten Daten werden an SIEM-Plattformen wie HP Arcsight, IBM QRadar oder Splunk Enterprise Security gesendet.

Arbor Spectrum mit NETSCOUT ISNG-Implementierung

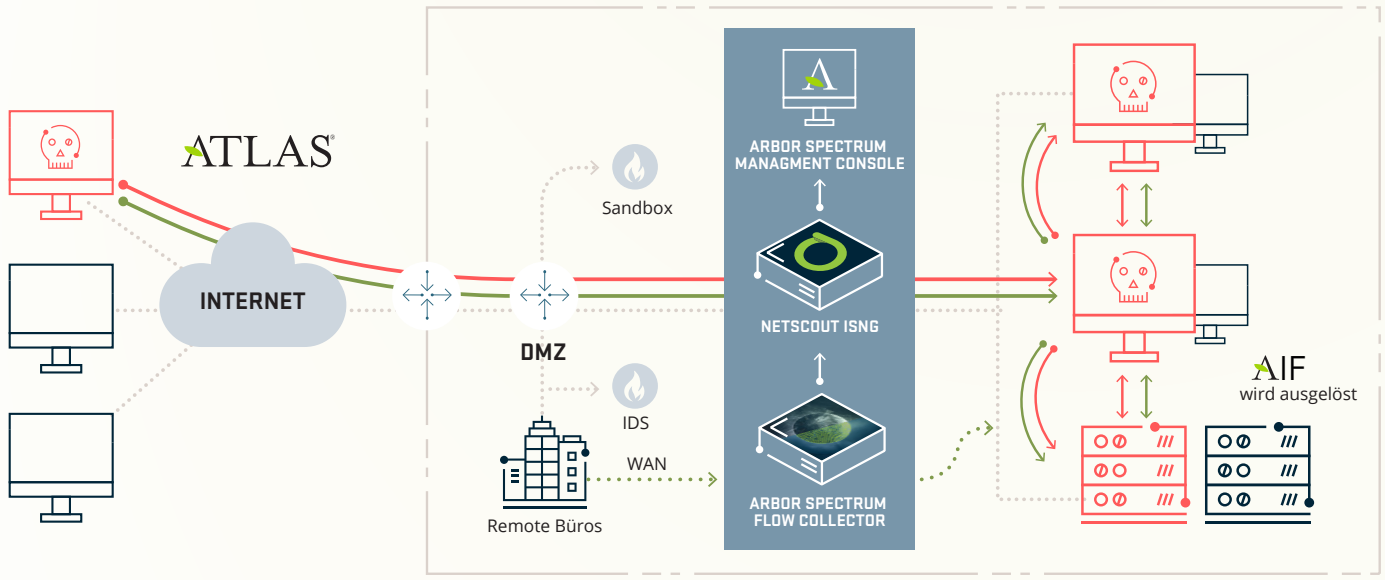


Abbildung 2 *Arbor Spectrum mit NETSCOUT ISNG*

Leistungs-merkmale

Zuverlässige Indikatoren für Sicherheitsvorfälle

durch ATLAS Intelligence

Innovative Workflows

Schnelle Aufdeckung von Vorfällen und Zuordnung von Angriffsindikatoren zu verdächtigen Aktivitäten

Leistungsstarkes Archiv mit Daten zum Netzwerkverkehr

Jetzt mit sofortigem Zugriff auf die Netzwerkdaten vergangener Monate dank NETSCOUT ISNG

Suchfunktion und Pivot-Darstellung

Anzeige der Netzwerkdaten vergangener Monate in Sekunden

Implementierung in weniger als einem Tag

Als Appliance und virtuelle Lösung

Primäre NETSCOUT ISNG-Modelle

ISNG-Modell	# Interfaces	Interface-Typ	Datenspeicher	Cores	RAM
ISNG 9895	4	4-Port 10G/1G	96 TB	36	256 GB
ISNG 9795	4	4-Port 10G/1G	64 TB	24	128 GB
ISNG 4895	4	4-Port 10G/1G	32 TB	36	256 GB
ISNG 4795	4	4-Port 10G/1G	24 TB	24	128 GB

Arbor Spectrum Management Konsole und Flow Collector Modelle

	2200	2300
Implementierungsoptionen	Platform Console, Packet Collector oder Flow Collector	Packet Collector oder Flow Collector
Speicher	64 GB	64 GB
Festplatten	8 x 2 TB SATA 7200 RPM	16 x 4 TB SATA 7200 RPM
Speicherkapazität	15 TB	64 TB
Archiv für Datenverkehr	9,1 TB	44 TB
Max. Flows pro Sekunde (als Flow Collector)	25.000	100.000
Max. Paketprüfung (als Packet Collector)	1,5 Gbps	5 Gbps
Optionen für Capture-Interface	SFP (4 Port) oder SFP+ (2 Port)	
Management Interface	2 x 10/100/1000 Kupfer	
Prozessor	2 x XEON ES-2658; 2,1 GHz/20 MB; 8-Core-Prozessoren	
Abmessungen	2 RU	3 RU
Spannungsversorgung	Doppelnetzteil (Gleich- oder Wechselstrom) **Wechselstrom:** 100–240 V, 47–63 Hz, 10-5A **Gleichstrom:** -40 bis -72 V / 20–12A	Doppelnetzteil (Gleich- oder Wechselstrom) **Wechselstrom:** 100–240 / 200–240 V, 50/60 Hz, 10/5 A; **Gleichstrom:** -36 bis -72 V / 31–15A
Relative Luftfeuchtigkeit	8 bis 90 % (nichtkondensierend)	8 bis 90 % (nichtkondensierend)
Wärmeabgabe	bei 400 Watt, 1365 BTU/h	bei 525 Watt, 1791 BTU/h

Hardware-Empfehlungen für Arbor Spectrum VM

Arbor gibt folgende Hardware-Empfehlungen:

VM-Implementierungen	Konsole	Packet Collector	Flow Collector
Unterstützte VMware-Version	vSphere Hypervisor (früher: ESXi), Softwareversion 5.5		
Core-Zuweisung	8 bis 32	8 bis 32	8
Speicherzuweisung	16 bis 64 GB	16 GB	16 GB
Festplattenzuweisung	**OS:** 150 GB / **Daten:** 1 bis 4 TB	**OS:** 150 GB / **Daten:** 1 bis 40 TB (getestetes Maximum; ausgelegt für Skalierung über 40 TB)	
Netzwerk-Interfaces	1 bis 2	3 bis 15	1 bis 15
Max. Flows pro Sekunde			250.000 FPS
Max. Paketprüfung		Bis zu 2 Gbps	

Die angegebenen Anforderungen und Leistungsdaten gelten für den Einsatz in Produktionsumgebungen. Arbor Spectrum unterstützt weitere Optionen für den Einsatz in kleineren Umgebungen.

ARBOR NETWORKS
The Security Division of NETSCOUT

Unternehmenszentrale
76 Blanchard Road
Burlington, MA 01803, USA
T: +1 866 212 7267 (gebührenfrei in USA)
T: +1 781 362 4300

Vertrieb Nordamerika
T: +1 855 773 9200 (gebührenfrei in USA)

Europa
T: +44 207 127 8147

Asiatisch-Pazifischer Raum
T: +65 6664 3140

Latein- und Mittelamerika
T: +52 55 4624 4842

www.arbornetworks.com

DS/SPECTRUM/DE/0717-A4