Network Traffic Security Analytics

Echtzeiterkennung von Sicherheitsverletzungen. Autonome Reaktionen. Volle Transparenz

„Bitdefender Network Traffic Security Analytics liefert unserer IT-Abteilung umfassende Einsichten und macht uns auf bestimmte, unerwünschte Geschehnisse aufmerksam, die in unserem Netzwerk passieren."

Führendes Automobil- und Fertigungsunternehmen

Bitdefender Network Traffic Security Analytics (NTSA) ist eine Unternehmenssicherheitslösung, die auch komplexe Angriffe in Echtzeit zuverlässig erkennt, detaillierte Einblicke in den Bedrohungskontext liefert und automatische Reaktionen auf Vorfälle anstößt. Es ermöglicht Unternehmen eine schnelle Erkennung und Abwehr hoch entwickelter Bedrohungen, indem es die bestehende Sicherheitsarchitektur – im Netzwerk und auf den Endpunkten – um spezialisierte netzwerkbasierte Verteidigungsmechanismen ergänzt. Indem es den Netzwerkverkehr als Quelle zuverlässiger Informationen heranzieht, erkennt NTSA Bedrohungen sofort, sobald sich das Verhalten von Endpunkten aufgrund einer Infektion verändert. Dabei erkennt die Lösung herkömmliche Bedrohungen ebenso wie Advanced Persistent Threats, unabhängig davon, ob diese bereits bekannt sind oder zum ersten Mal auftreten. Vorfallswarnungen werden automatisch korreliert und priorisiert, um die Effizienz des Sicherheitsbetriebs zu steigern und eine verbesserte Untersuchung von Vorfällen zu gewährleisten. Dank der Integration mit Bitdefender GravityZone können Sicherheitsvorfälle durch automatische Reaktionen schnell behoben werden.

Bedrohungserkennung in Echtzeit für jedes Gerät im Netzwerk	**Sparen Sie Zeit durch autonome Vorfallsreaktionen**	**Lückenlose Transparenz und zielführende Erkenntnisse zu Cyberbedrohungen**
Liefert vollständige Einblicke in alle bedrohungsrelevanten Aktivitäten auf allen Endpunkten im Netzwerk, unabhängig vom Typ oder bereits vorhandenen Sicherheitslösungen (unternehmens- oder benutzerverwaltete Geräte, Netzwerkelemente, BYOD, IoT).	Automatisiert die Priorisierung von Sicherheitsvorfällen für eine wirksame Untersuchung von Vorfällen und automatisiert die Bedrohungsreaktion durch die Integration mit GravityZone, um schnellere Reaktionszeiten zu gewährleisten.	Bietet Transparenz und detaillierte Erklärungen zu den Sicherheitsvorfällen über die gesamte Umgebung hinweg. Schlägt Vorgehensweisen zur Eindämmung von Vorfällen und zur Anhebung des Sicherheitsniveaus vor.

Umfassende Aufklärung der Bedrohungslage und künstliche Intelligenz

NTSA nutzt Bitdefenders fortschrittlichste Bedrohungsaufklärung – zusammengetragen von 500 Millionen Endpunkten in aller Welt, kombiniert sie mit fortschrittlichen maschinellen Lernverfahren und Heuristiken, um die Netzwerk-Metadaten in Echtzeit zu analysieren und Bedrohungsaktivitäten und verdächtige Datenverkehrsmuster zielgerichtet zu erkennen. Automatische Sicherheitsanalysen und der Fokus auf den ausgehenden Netzwerkverkehr sorgen für einen besseren Überblick ohne Nebengeräusche und liefern konkrete und zielführende Warnmeldungen für Sicherheitsteams.

IntelliTriage – Automatisierte Triage von Sicherheitswarnungen

IntelliTriage, ein wichtiger Bestandteil von NTSA, automatisiert den Triage-Prozess für Sicherheitsvorfälle, um die Vorfallsuntersuchung zu beschleunigen und organisatorische Risiken durch hochpräzise Warnmeldungen zu reduzieren. Es umfasst zudem Anleitungen zu den empfohlenen Bereinigungsschritten, die für Sicherheitsvorfälle zu ergreifen sind. Es ermöglicht komplexes szenariobasiertes Lernen,

um auch fortschrittliche Angriffe mit hoher Genauigkeit zu erkennen und korreliert Tausende von Sicherheitswarnungen, um ein klares Bild von jedem Vorfall zu vermitteln. IntelliTriage liefert detaillierte Erläuterungen zur Schweregradbewertung von Vorfällen. Darüber hinaus empfiehlt es Bereinigungsmaßnahmen, um eine schnellere Reaktion auf Vorfälle sicherzustellen.

Integrierte autonome Bedrohungsreaktionen

Die Integration zwischen Bitdefender GravityZone und NTSA ermöglicht eine automatisierte Reaktion auf Sicherheitsvorfälle und erhöht die Widerstandsfähigkeit von Unternehmen gegen komplexe Bedrohungen.

Werden im Netzwerk kritische Vorfälle entdeckt, kann NTSA automatisch GravityZone zur Untersuchung der betroffenen Endpunkte hinzuziehen. Abhängig vom Scan-Ergebnis kann GravityZone den oder die Endpunkte automatisch bereinigen und/oder unter Quarantäne stellen, um die auftretende Bedrohung wirksam einzudämmen.

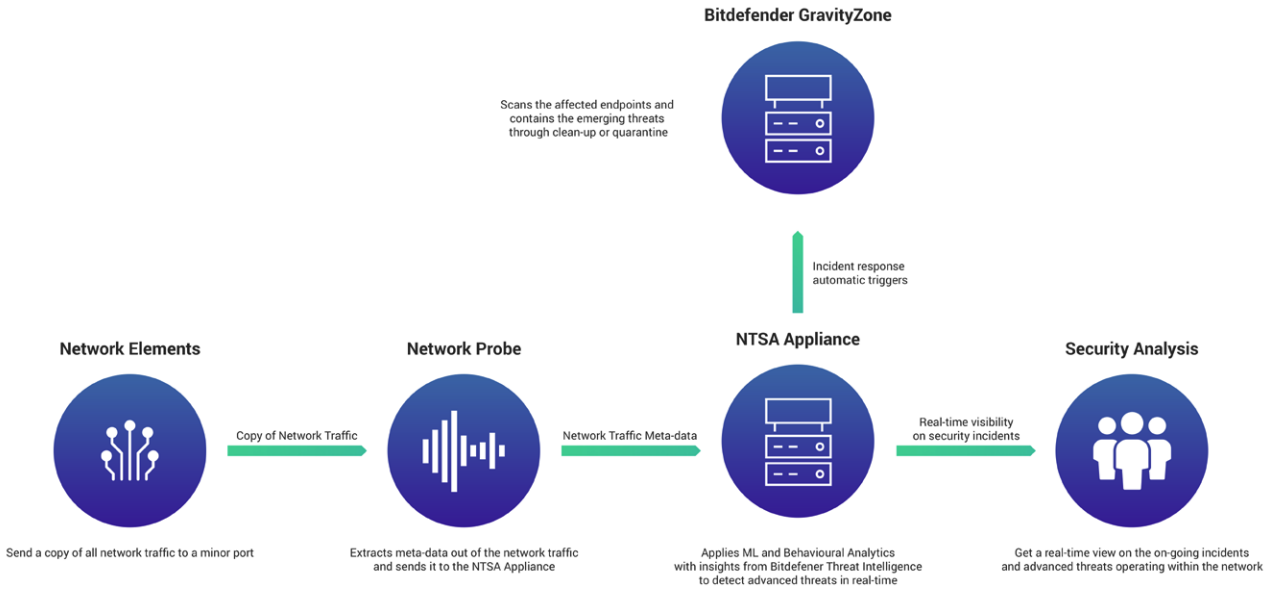
> "Bei der Ermittlung von Sicherheitsanforderungen haben wir die möglichen Bedrohungen durch Malware berücksichtigt, die ihren Weg ins Netzwerk finden könnte. Folglich haben wir ausdrücklich nach neuen Wegen gesucht, auch diese Bedrohungen zu erkennen. Die ideale Lösung für uns war also eine Sicherheitslösung, die in der Lage ist, den ausgehenden Netzwerkdatenverkehr zu erkennen."
>
> ICT-Leiter einer Gesundheitsorganisation

Bietet Schutz auch für intelligente Geräte (IoT) und BYOD

In Unternehmensumgebungen finden sich neben Geräten, die von Menschen bedient werden, zunehmend auch so genannte Smart Things. Während herkömmliche Endpunkte in der Regel gut beobachtet und geschützt werden, arbeiten diese intelligenten User-Produkte in einer Grauzone mit eingeschränktem oder nicht vorhandenem Schutz. Diese Geräte im Netzwerk geraten immer häufiger ins Visier von Angreifern und dienen ihnen als Brückenkopf. Darum erstreckt sich mit NTSA die Erkennung von Sicherheitsverletzungen auch auf die intelligenten Geräte im Unternehmensnetzwerk. Durch die Konzentration auf das Netzwerkverhalten von Endpunkten können so auch Geräte mit eingeschränkten oder ohne eigene Sicherheitsfunktionen und keinem darauf laufenden Agenten für die Endpunktsicherheit (wie bei den meisten IoT-Geräten der Fall) geschützt werden.Die Nutzung von privaten Laptops, Mobiltelefonen und anderen Geräten im geschäftlichen Umfeld führt auch immer wieder dazu, dass Angreifer Unternehmensdaten erbeuten. Sichere BYOD-Umgebungen steigern nicht nur die Produktivität von Mitarbeitern, sondern senken auch das Risiko, dass Unternehmensdaten in falsche Hände geraten. Die NTSA-Technologie hilft Unternehmen, sich gegen Datendiebstahl abzusichern, indem sie das Benutzer- und Geräteverhalten lückenlos in Echtzeit überwacht, verfolgt und überlegene Bedrohungsinformationen bereitstellt. Dabei funktioniert sie agentenlos, ist unaufdringlich und kann unabhängig vom Betriebssystem eingesetzt werden.

NTSA: Architektur und Bereitstellung

NTSA lässt sich einfach bereitstellen (Plug-and-Play), ist gegebenenfalls im Handumdrehen mit GravityZone integriert und liefert sofort Ergebnisse. Die Netzwerkleistung wird in keiner Weise beeinträchtigt, da die Lösung „Out of Band" betrieben wird und eine gespiegelte Kopie des Netzwerkverkehrs analysiert.



Compliance sicherstellen

Viele gesetzliche Bestimmungen, so auch die DSGVO, verlangen von Unternehmen, dass sie im Falle von Sicherheitsverstößen umgehend detaillierte Informationen über böswillige Aktivitäten bereitstellen. NTSA unterstützt Unternehmen bei der Erfüllung von Compliance-Anforderungen, indem es Informationen über den Netzwerkdatenverkehr bis zu 12 Monate lang bereithält. Dabei enthalten die Aufzeichnungen ausschließlich Metadaten ohne die eigentlichen Nutzdaten. Der Zugriff auf die Aufzeichnungen ist dem Datenschutzbeauftragten vorbehalten, wodurch das Risiko einer Offenlegung sensibler Daten gebannt wird.

Bestandteile

Echtzeiterkennung, lückenlose Transparenz
Erkennt Sicherheitsverstöße, indem es den Netzwerkverkehr in Echtzeit auf Anomalien in der Kommunikation untersucht. Bietet lückenlose Transparenz und Einblicke in bedrohungsrelevante Netzwerkaktivitäten und Anomalien im Endpunktdatenverkehr.

Erweiterte Abdeckung
Deckt alle Endpunkte im Netzwerk ab, unabhängig vom Typ oder bereits vorhandenen Sicherheitslösungen (unternehmens- oder benutzerverwaltete Geräte, Netzwerkelemente, BYOD, IoT).

Automatische Priorisierung, automatische Reaktionen
Automatisiert Sicherheitsanalysen und sorgt für einen besseren Überblick ohne Nebengeräusche, um Analysten eine wirksamere Vorfallsuntersuchung zu ermöglichen. Schaltet bei kritischen Warnmeldungen automatisch GravityZone zur Bedrohungsreaktion ein.

Bedrohungsaufklärung in der Cloud, KI/ML und Heuristiken
Vereint die Cloud-Bedrohungsaufklärung von Bitdefender mit Echtzeitanalysen des Netzwerkverkehrs auf Grundlage von KI/ML und Heuristiken, um überlegene Bedrohungserkennungsraten mit möglichst wenigen Fehlalarmen zu garantieren.

Schnelle Bereitstellung, vor Ort und in der Cloud
Baut auf einer einfachen und flexiblen Architektur (physische, virtuelle oder Cloud-Appliance) mit Plug-and-Play-Komponenten auf, um sofort Ergebnisse zu liefern.

Verschlüsselte Kommunikation und Datenschutz
Die Konzentration auf die Metadaten des Datenverkehrs ermöglicht die Analyse verschlüsselter Kommunikation und vermeidet Datenschutzprobleme im Zusammenhang mit unverschlüsseltem Datenverkehr.

Integration mit GravityZone
Die Integration mit GravityZone ermöglicht eine bequeme und nahtlose Verwaltung und automatisiert die Reaktion auf Sicherheitsvorfälle.

Weitere Einzelheiten zu den Systemvoraussetzungen finden Sie unter https://www.bitdefender.de/business/enterprise-products/networktraffic- security-analytics.html

Bitdefender

Bitdefender ist ein globales Sicherheits-Technologie-Unternehmen und bietet wegweisende End-to-End Cyber-Security-Lösungen sowie Advanced Threat Protection für über 500 Millionen Nutzer in über 150 Ländern. Seit 2001 ist Bitdefender ein innovativer Wegbereiter der Branche, indem es preisgekrönte Sicherheitslösungen für Privat- und Geschäftsanwender integriert und entwickelt. Zudem liefert das Unternehmen Lösungen sowohl für die Sicherheit hybrider Infrastrukturen als auch für den Endpunktschutz. Als führendes Security-Unternehmen pflegt Bitdefender eine Reihe von Allianzen sowie Partnerschaften und betreibt umfassende Forschungen und Entwicklungen. Weitere Informationen sind unter www.bitdefender.de verfügbar.

WEITERE INFORMATIONEN ERHALTEN SIE HIER: www.bitdefender.de/business