

Network Traffic Security Analytics

Rilevamento delle violazioni in tempo reale e visibilità completa sulle minacce

Bitdefender Network Traffic Security Analytics è una soluzione di sicurezza di livello enterprise che rileva in modo accurato le violazioni e fornisce informazioni approfondite sugli attacchi avanzati tramite l'analisi del traffico di rete. Permette alle organizzazioni di rilevare e contrastare rapidamente le minacce più sofisticate, agendo in modo complementare all'architettura di sicurezza preesistente, sia sulla rete che sugli endpoint, con una difesa specializzata basata sulla rete.

Sfruttando il traffico di rete come fonte di dati attendibili, NTSA rileva le violazioni immediatamente, non appena il comportamento degli endpoint varia in seguito all'infezione. Il rilevamento è efficace sia contro le minacce generiche che contro quelle avanzate e persistenti, note o del tutto sconosciute. NTSA genera degli avvisi per segnalare al reparto preposto alla sicurezza le variazioni del comportamento sugli endpoint che indicano la presenza di un attacco avanzato in corso o di endpoint compromessi.

"Bitdefender Network Traffic Security Analytics offre al reparto IT una visibilità completa e ci permette di venire a conoscenza di diversi eventi poco desiderabili che avvengono nella rete"

Azienda leader nel settore dell'automotive e della produzione

Leader nel campo dell'intelligence sulle minacce informatiche e dell'IA

NTSA sfrutta l'intelligence avanzata di Bitdefender sulle minacce informatiche, con dati provenienti da 500 milioni di endpoint a livello globale, in combinazione con tecnologie euristiche e di apprendimento automatico avanzato per analizzare i metadati di rete in tempo reale e individuare in modo accurato l'attività delle minacce e schemi di traffico sospetti. Grazie a un'analytics di sicurezza automatizzata e concentrandosi sul traffico di rete in uscita, riduce il "rumore di fondo" e fornisce avvisi immediatamente utilizzabili da parte del reparto IT.

Protezione per dispositivi IoT e BYOD nel tuo ambiente

I laptop, gli smartphone e gli altri dispositivi personali utilizzati dai dipendenti nell'ambiente di lavoro vengono sfruttati dai criminali per esfiltrare i dati aziendali. Proteggere i dispositivi BYOD (Bring Your Own Device) aumenta la produttività dei dipendenti e riduce il rischio di divulgazione di informazioni societarie. Proteggere i dispositivi BYOD (Bring Your Own Device) aumenta la produttività dei dipendenti e riduce il rischio di divulgazione di informazioni societarie. La tecnologia NTSA aiuta le organizzazioni a difendersi dal furto di dati, monitorando e tracciando costantemente e in tempo reale il comportamento di tutti gli utenti e dispositivi e sfruttando una potente intelligence sulle minacce. Non richiede l'utilizzo di agenti e non è intrusivo, indipendentemente dal sistema operativo.

Gli ambienti aziendali sono sempre più condivisi su dispositivi gestiti dagli utenti e oggetti smart. Mentre gli endpoint tradizionali sono solitamente ben protetti e sorvegliati, i dispositivi smart operano in un'area grigia, con una sicurezza limitata o del tutto assente. I dispositivi connessi alla rete vengono sempre di più presi di mira e usati come testa di ponte per attacchi avanzati. Le capacità di rilevamento delle violazioni offerte da NTSA si estendono anche agli oggetti smart presenti sulla rete aziendale. Concentrandosi sul comportamento degli endpoint della rete, è in grado di proteggere dispositivi con funzionalità di sicurezza ridotte o assenti e privi di qualsiasi agente di sicurezza (come la maggior parte dei dispositivi IoT).

Architettura e implementazione di NTSA

NTSA è facile da implementare (plug-and-play) e garantisce risultati immediati. Non influisce in alcun modo sulle prestazioni della rete, poiché l'appliance è situata out-of-band e poiché analizza una copia del traffico generata tramite mirroring.

BITDEFENDER

Minaccia
Intelligence
Labs

HEURISTICS

Static & Dynamic

DESTINATIONS

Our labs

IP Reputation Feed + Malicious URLs + Geofence + Bad Hoods

External:

Commercial threat intelligence

YOUR COMPANY NETWORK

With Network Security Analytics Tools

DASHBOARD



CORPORATE ASSETS

PC's, Laptops, Printers, Wifi, Servers, BYOD

Threat intelligence

STIX & TAXII
Threat intelligence
from organisations

FORENSIC DATA STORAGE

Data Retention

DATI PROTEZIONE OFFICER

Bitdefender®
Network Traffic Security Analytics

Destination + Behavior
= Egress Monitoring

IPFIX Data

Mirrored
Traffic

SWITCH

PROBE

MNGT & Flow
Data / IPFIX

INTERNET

Popular websites
Malicious e-mail

VPN'S, Proxies
& TOR

Criminal Controlled
Reti



ATTACKER

Infects

Hides Identity

Hires

Conformità alla normativa

Molte normative, incluso il GDPR, impongono alle organizzazioni di fornire in tempi molto brevi informazioni dettagliate su attività dannose, in caso di violazione. NTSA le aiuta soddisfare questi requisiti, registrando informazioni sul traffico di dati sulla rete per un periodo fino a 12 mesi. Le registrazioni contengono solo metadati, senza alcun effettivo payload, e l'accesso ad esse è riservato al ruolo del responsabile della protezione, per eliminare il rischio di divulgazione di dati sensibili.

Benefici Chiave

Previene interruzioni dell'attività

- Rileva le violazioni e le minacce avanzate che hanno eluso i meccanismi di protezione a livello di endpoint o di rete
- Fornisce una visibilità completa sulle attività di rete legate alle minacce e su anomalie nel traffico sugli endpoint
- Sfrutta un'intelligence sulle minacce basata su cloud, l'apprendimento automatico e analytics comportamentali per rilevare le minacce più sofisticate

Soddisfa i requisiti normativi

- Identifica i comportamenti anomali da parte degli utenti o minacce interne che possono portare a violazioni delle policy aziendali
- Agevola l'individuazione delle minacce e l'indagine, grazie all'accesso a dati archiviati a lungo termine
- Offre un facile e rapido accesso alle informazioni richieste dalle autorità entro il periodo di 72 ore successive alla scoperta della violazione (GDPR)

Facile da usare, ROI rapido

- Una soluzione integrativa, facile da implementare e da mantenere, che garantisce risultati immediati, per un rapido ritorno dell'investimento
- Integrazione con altri sistemi di monitoraggio, per offrire una sicurezza automatizzata e una risposta rapida
- Copre tutti gli endpoint presenti sulla rete, indipendentemente dal loro tipo o dalla presenza di soluzioni di sicurezza preesistenti (dispositivi gestiti a livello aziendale o dagli utenti, elementi di rete, BYOD, IoT)

Caratteristiche

Rilevamento in tempo reale e retroattivo

Rileva le violazioni controllando in modo passivo e in tempo reale il traffico di rete in uscita, per individuare qualsiasi comunicazione dannosa. Applica elementi di intelligence sulle minacce ai metadati registrati, per rilevare retroattivamente le violazioni

Intelligence sulle minacce basata su cloud, IA, apprendimento automatico e tecnologie euristiche

Unisce l'intelligence sulle minacce informatiche di Bitdefender ad analytics in tempo reale del traffico di rete basate su IA, apprendimento automatico e tecnologie euristiche, garantendo un maggiore rilevamento delle minacce e meno falsi positivi

Copertura estesa, visibilità completa

Copre tutti gli endpoint presenti sulla rete, indipendentemente dal loro tipo o dalla presenza di soluzioni di sicurezza preesistenti (dispositivi gestiti a livello aziendale o dagli utenti, elementi di rete, BYOD, IoT). Fornisce una visibilità completa sulle attività di rete legate alle minacce e su anomalie nel traffico sugli endpoint

Rumore ridotto, individuazione efficace delle minacce

Automatizza l'analisi delle minacce e riduce il rumore per aumentare l'efficienza delle attività degli analisti. Genera avvisi immediatamente utilizzabili, per agevolare la risposta agli incidenti

Comunicazioni criptate e privacy

Concentrandosi solo sui metadati del traffico, permette l'analisi di comunicazioni criptate ed elimina i problemi legati alla privacy del traffico non criptato

Implementazione rapida, risultati immediati

Basato su un'infrastruttura semplice e flessibile (implementazione fisica o virtualizzata) con componenti plug-and-play, per garantire risultati immediati

Per informazioni dettagliate sui requisiti di sistema, fare riferimento a <https://www.bitdefender.com/business/enterprise-products/network-traffic-security-analytics.html>



Bitdefender è una società leader mondiale nelle tecnologie di sicurezza che fornisce soluzioni di sicurezza informatica end-to-end innovative e una protezione avanzata da ogni minaccia a oltre 500 milioni di utenti in più di 150 paesi. Sin dal 2001, Bitdefender ha sviluppato ininterrottamente tecnologie di sicurezza rivolte ad aziende e clienti, vincitrici di numerosi riconoscimenti, ed è il fornitore di riferimento nel settore della sicurezza delle infrastrutture ibride e della protezione degli endpoint. Grazie alla R&S, alle sue alleanze e alle sue partnership, Bitdefender garantisce sempre soluzioni di protezione innovative, solide e affidabili. Maggiori informazioni sono disponibili sul sito <http://www.bitdefender.it/>

Tutti i diritti riservati. © 2018 Bitdefender. Tutti i marchi, nomi commerciali e prodotti a cui si fa riferimento nel presente documento sono di proprietà dei rispettivi titolari.
PER MAGGIORI INFORMAZIONI VISITATE: bitdefender.it/business

