Bitdefender®

Q4
2020

Network Attack Defense

REPORT BY

ASHISH CHAKRABORTTY, TECHNICAL MARKETING ENGINEER

Table of Contents

Network Attack Defense

Overview

Network Traffic Analysis (NTA) uses a combination of machine learning, advanced analytics and rule-based detection to detect suspicious activities on enterprise networks [1]. NTA tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior.

Bitdefender provides Network Attack Defense (NAD) which is a powerful technology focused on preventing an array of attacks from Lateral Movement (Brute Force; Port Scanners), web-service attacks (SQL injections), Traffic-Level attacks (botnets; malicious URLs or remote IOT attacks) to privacy breaches performed via phishing attacks to exfiltrate passwords, credit card or email addresses [2]. Detailed information of the attack, like: Attacker's IP, Victim's IP, type of attack and many other pieces of information which are relevant to the attack are logged. GravityZone Network Attack Defense technology is extended with threat insights from Network Traffic Security Analytics (NTSA), further expanding visibility and control of network based threats.

Technical Diagram

Network elements such as Firewalls, Secure Web Gateways, Intrusion Detection/Prevention Systems, Sandboxes protect internal network and block outside threats at the perimeter level. Bitdefender probes use analytics which are specialized tools that are built to detect advanced threats by analyzing network traffic. It uses machine learning and heuristics to analyze the network metadata (like IP addresses) in real-time and accurately reveals threat activity and suspicious traffic patterns. This telemetry information is sent to Bitdefender's Endpoint Detection and Response (EDR) feeds for visibility.

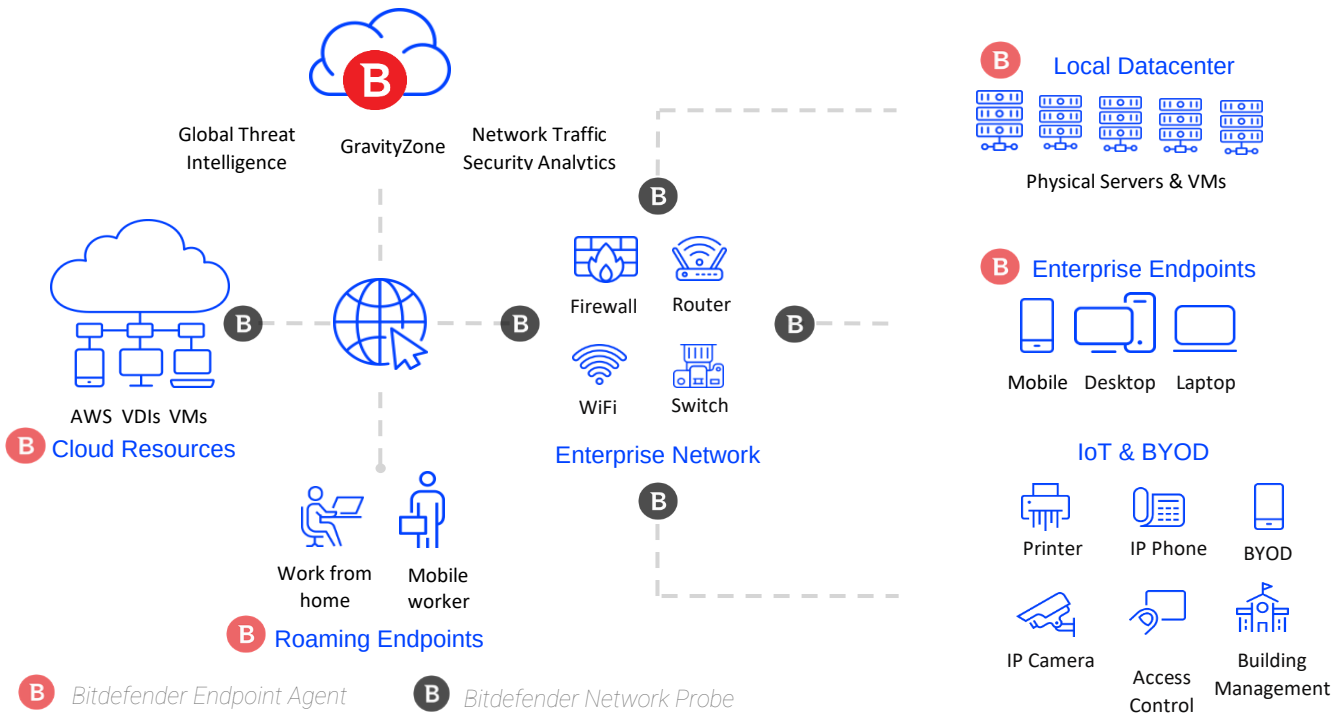

Fig. 3 End-to-End breach avoidance platform

Use Case

Detect Initial Access Techniques

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network [3]. Techniques include targeted spearphishing and exploiting weaknesses on public facing web servers. Network

Attack Defense (NAD) hardens network protocols like HTTP, SMB, RPC and analyzes network traffic to block attacks like SQL Injection, Brute Force and Drive-By Downloads.

Prevent Credential Access

Credential Access consists of techniques like keylogging or credential dumping for stealing account names and passwords [4]. NAD analyzes network traffic to prevent exfiltration of personal information.

Disallow Asset Discovery

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network [5]. Adversaries can observe the environment and orient themselves before deciding which assets to compromise. Native OS tools are often used toward this post-compromise information-gathering technique. Using behavior analytics, NAD quickly spots suspicious processes and takes actions against it.

Beneficial Outcomes and Consequences

Lateral movement of malware is blocked

Lateral movement consists of techniques that adversaries use to enter and control remote systems on a network [6]. Post asset discovery, attacker uses lateral movement to discover other valuable network resources to either spread the infection or gain elevated privileges. They can then pivot through multiple systems and accounts. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier. NAD, using Bitdefender's patented machine learning, can harden defenses by providing an additional layer of security and prevents adversaries from moving laterally.

Increased protection against Crimeware

Crimeware is not a purely technical threat but more of a socio-technical affair [7]. Malware is now built and pushed by technologically sophisticated organizations, aided-by phishing-like deceit tactics and spread via advertisements, social networks and other IT electronic devices for financial gains. 2019 has seen 1,272 data breaches to date (read here), exposing more than 163M records [8]. Attackers have latched onto transactional data — social security numbers, phone numbers, personal addresses, medical records, etc. Host-based NAD along with network-based NTSA detect breaches and advanced threats that eluded prevention mechanisms at endpoint in the network. It provides complete visibility and insights into threat related network activity and endpoint's traffic anomalies.

FAQs

Can Network Attack Defense protect my personal information from leaving the network?
Bitdefender provides unparalleled visibility of applications and process using an extensive library of machine learning technologies. NAD uses behavioral heuristics to analyze host network activity in real-time and harden controls against exploit techniques that can exfiltrate personal information from your network.

How can my data be protected against attacks like BlueKeep?
BlueKeep enables attackers to remotely drop malware or gain persistence on the system. The Network Attack Defense uses machine learning to block the exploit and protect our customers. Bitdefender's multiple pre-execution and on-execution layers will also halt ransomware, cryptojacking or other threats delivered through BlueKeep, well before they can execute or affect business operations.

How is the traffic analyzed with Network Attack Defense? What happens after NAD detects an exploit?
Bitdefender combines cloud threat intelligence with real-time network traffic analytics based on AI, ML and heuristics to achieve superior threat detection rates with low false positives. By default, network attack defense is enabled in the policy with all techniques set in Block mode. The machine learning quickly blocks the exploit and extracts meta-data information about attack origin, IP, URL and the technique used by the attacker for investigation and security audit reports.

References:

[1] Gartner, Market Guide for Network Traffic Analysis, February 2019 – *Published 28 February 2019 – ID G00381265*
[2] GravityZone Elite Security
[3] https://attack.mitre.org/tactics/TA0001/
[4] https://attack.mitre.org/tactics/TA0006/
[5] https://attack.mitre.org/tactics/TA0007/
[6] https://attack.mitre.org/tactics/TA0008/
[7]https://commons.erau.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1125&context=adfsl
[8] https://medium.com/@chroniclesec/chronicle-cybersecurity-predictions-crimeware-cloud-and-beyond-6c93ca8de80c