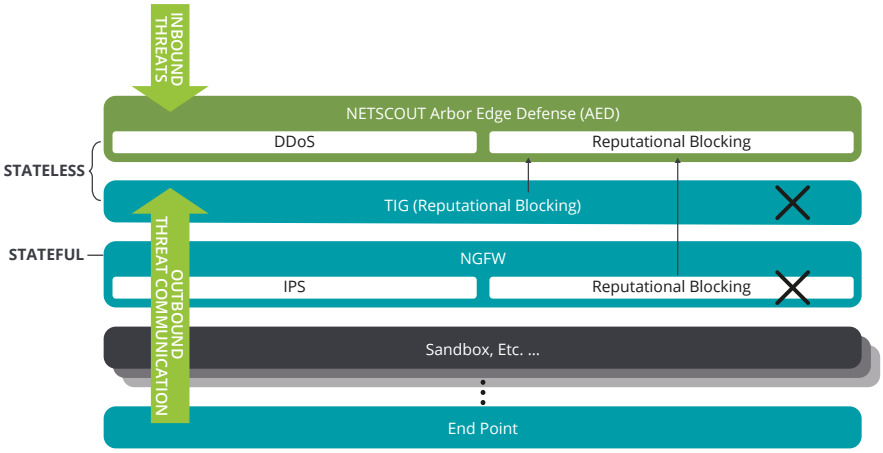
NETSCOUT Arbor Edge Defense

First and Last Line of Smart, Automated Perimeter Defense

Redefining the Network Perimeter Security Stack

As cyber threats have evolved, so too has the cyber security stack. The Next Generation Firewalls (NGFW), necessary components of the stack, have expanded outside of their core use cases. For example, IDS/IPS and Sandboxing technologies, once standalone devices are now consumed by many NGFWs. More recently the NGFW, a stateful device, has become overwhelmed stopping threats using reputation-based IoCs. To offload this functionality, letting NGFWs focus on their core functionality, enterprises have looked for new devices that can operationalize the volume of high-quality threat intel they have access to. An emerging product, the Threat Intelligence Gateway (TIG), is starting to gain the interest of forward-leaning security teams. Using stateless technology and armed with millions of reputation-based IOCs, the TIG is deployed in front of the firewall adding yet another standalone device to the security stack and making it more complex. Once again, the time has come for a redefinition of the modern-day, network perimeter security stack; NETSCOUT® Arbor Edge Defense (AED) will play a critical role.



NETSCOUT Arbor Edge Defense (AED) is a deployed at the network perimeter (i.e. between the Internet router and firewall). Using a stateless packet processing engine and armed with continuous highly curated, reputation-based threat intelligence it receives from NETSCOUT ATLAS® Threat Intelligence or 3rd parties via STIX/TAXII, AED is a network perimeter enforcement point that can automatically detect and stop both inbound threats (e.g. DDoS attacks and other threats in bulk) and outbound communication from internal compromised hosts that have been missed by other components in the security stack – essentially acting as the first and last line of defense for organizations. AED simplifies the security stack by consolidating DDoS protection and TIG-like functionality in a single device. AED also protects the availability and performance of not only an organization's networks and services, but also their security stack (e.g. the struggling NGFW), enabling it and their teams to perform more efficiently.

KEY FEATURES AND BENEFITS

First Line of Defense

Deployed at the network perimeter, using stateless technology and armed with millions of IoCs, AED detects and blocks inbound cyber threats at internet scale, thus taking pressure off of stateful devices such as Next Gen Firewalls.

Last Line of Defense

Enhancing the existing security stack, AED can detect and blocking outbound communication to hacker command and control (C2), domains and URLs; thus helping stop the further proliferation of malware with an organization and avoid a data breach.

Contextual Threat Intelligence

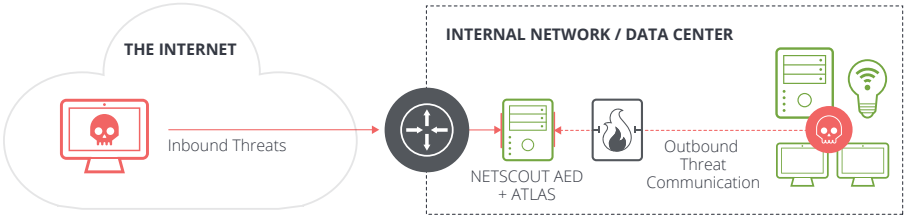
When an IOC is blocked, AED leverages the global threat intelligence of NETSCOUT ATLAS to provide more context related to the indicator thus helping security teams determine risk and/or give them more information to proactively hunt for the source of the infections.

Best of Breed DDoS Protection

AED can automatically detect and stop inbound application layer, TCP-state exhaustion and DDoS attacks as large as 40 Gbps. In the event of even larger DDoS attacks, Cloud Signaling automatically reroutes traffic to Arbor Cloud or a MSSP's cloud-based mitigation center.

Integration with Security Stack

AED's robust REST API, support for Syslog, Common Event Format (CEF), Log Event Extended Format (LEEF) and STIX/TAXII enables AED to integrate with existing security technologies and processes.

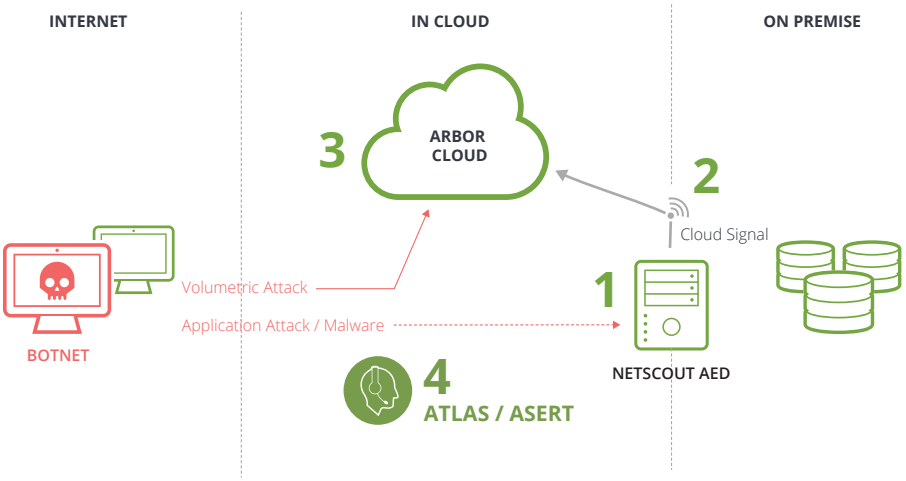


First Line of Defense

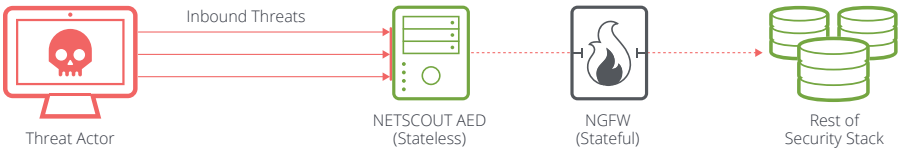
In an appliance or virtual form factor, NETSCOUT Arbor Edge Defense (AED) is deployed at the network perimeter (i.e. between the Internet router and firewall) where it provides first line of defense from DDoS attacks and inbound threat connection attempts. AED Provides Best of Breed DDoS Attack Protection: Based upon Arbor Networks' 20-year heritage, proven technology and global threat intelligence from NETSCOUT ATLAS.

AED delivers best of breed and comprehensive DDoS attack protection.

1. AED can automatically detect and stop inbound application layer, TCP-state exhaustion (which can bring down firewalls) and DDoS attacks as large as 40 Gbps.
2. In the event of larger DDoS attack, AED's Cloud Signaling will automatically reroute traffic to Arbor Cloud or a MSSP's cloud-based DDoS attack mitigation center.
3. Arbor Cloud provides protection from the largest DDoS attacks via 14 worldwide scrubbing centers providing over 9 Tbps of mitigation capacity.
4. AED stays abreast of the latest DDoS threats via the ATLAS Threat Intelligence Feed.

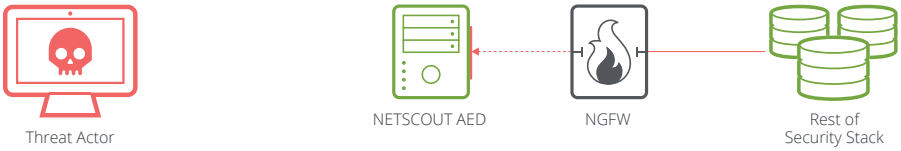


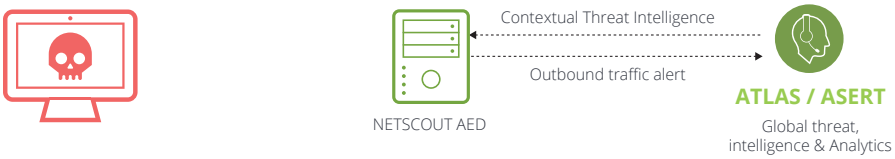
AED Blocks Inbound Threat Connection Attempts Using Stateless Technology:
Inspecting each packet to make a go/no-go decision, continuously armed with millions of Indicators of Compromise (IoCs) it receives from NETSCOUT ATLAS Threat Intelligence and/or 3rd parties via STIX/TAXII, AED is a network perimeter enforcement point that can automatically detect and stop inbound threats in bulk. Essentially AED acts as a first line filter that stops internet-scale threats so other devices in security stack; for example the NGFW, which was designed for session-oriented monitoring and security analysts to work more efficiently.



Last Line of Defense

In a world where security stacks are still missing Indicators of Compromise (IoCs), AED can act as the last line of defense. Armed with highly curated Indicators of Compromise (IoCs) it receives from NETSCOUT ATLAS Threat Intelligence and/or 3rd parties via STIX/TAXII, AED can act as an outbound network enforcement point by detecting and automatically blocking outbound communication to known attacker C2 infrastructures (i.e. IP addresses, domains, URLs, C2C infrastructure). By acting as this last line of defense, AED can help organizations stop the proliferation of stage 2 malware within their networks and ultimately avoid the data breach.





Contextual Threat Intelligence

Today's point security solutions produce individual alerts of discrete activities, tied to the malicious tools used, often at different points in an attacker's operation. Enterprises expect correlation capabilities like SIEM and big data to link disparate events, but the effectiveness of these tools is hamstrung by the overwhelming amount of false positive and nuisance data that they process. AED can help by providing more context to IoCs that it has blocked. For example, when AED blocks an outbound IoC, it sends an alert NETSCOUT ATLAS Security Engineering Research Team (ASERT). Using Machine learning and other technology, ASERT automatically analyzes its vast database of threat intelligence to provide more context related to the IoC. This additional context is then automatically delivered to the security analyst via the AED UI who then can answer important questions such as:

Is this something I should be worried about?...What's the real risk to our organization?...Who is the associated threat actor, and what other TTPs do they use during various phase of kill chain?...What other recommendations can you give to go hunting using other tools I have in my security stack?

Linking IoCs to known attackers, flips the risk conversation from one about the volume of threats (number of blocks made) to one about the potential severity of persistent attackers targeting specific intellectual property, customer records, or destruction-based hacktivism. The additional Contextual Threat Intelligence AED provides (e.g. malware samples, hashes, and endpoint IOCs) enable cybersecurity hunting teams to use their arsenal of other security tools such as Endpoint Detection and Response (EDR) tools to proactively hunt for other signs of compromise, eradicate and ultimately avoid the data breach. It's this additional Contextual Threat Intelligence (CTI) that allows AED to be much more than just a network perimeter enforcement point. AED's CTI allow AED to become an integral part of the overall security stack and process.

LEARN MORE

For more information about NETSCOUT AED visit:

https://www.netscout.com/products/netscout-aed

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECSB_014_EN-1901 03/2019