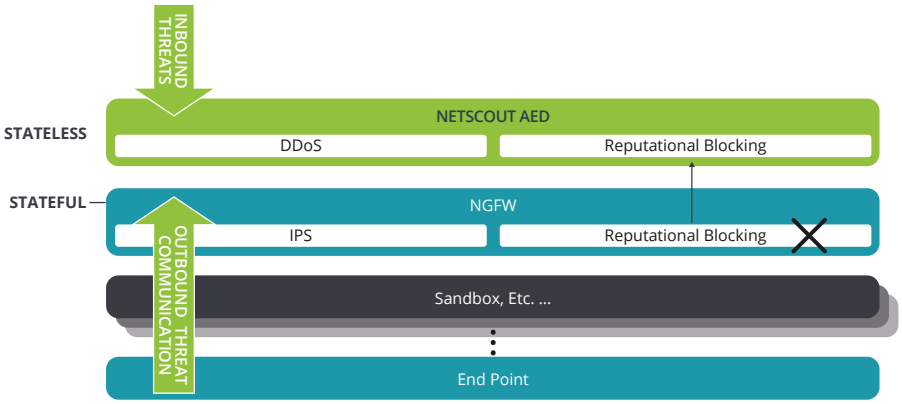
NETSCOUT AED

First and Last Line of Smart, Automated Perimeter Defense

Redefining the Network Perimeter Security Stack

As cyberthreats have evolved, so too has the cybersecurity 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 from threats using reputation-based IoCs. Once again, the time has come for a redefinition of the modern-day, network perimeter security stack; NETSCOUT® AED will play a critical role.



First Line of Defense

In an appliance or virtual form factor, 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 and is based upon Arbor Networks' 20+ year heritage, proven technology and global threat intelligence from NETSCOUT ATLAS®.

KEY FEATURES AND BENEFITS

First Line of Defense

Deployed at the network perimeter, using stateless technology and armed with millions of reputation-based 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

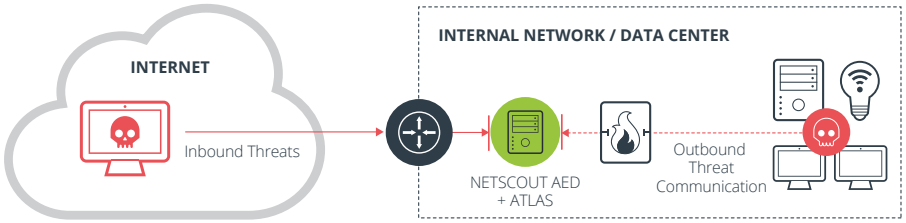
Enhancing the existing security stack, AED can detect and block outbound communication to hacker command and control (C2), domains and URLs; thus helping stop the further proliferation of malware with an organization and avoid a data breach.

Best of Breed DDoS Protection

AED can automatically detect and stop inbound application layer, TCP-state exhaustion and DDoS attacks as large as 200 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

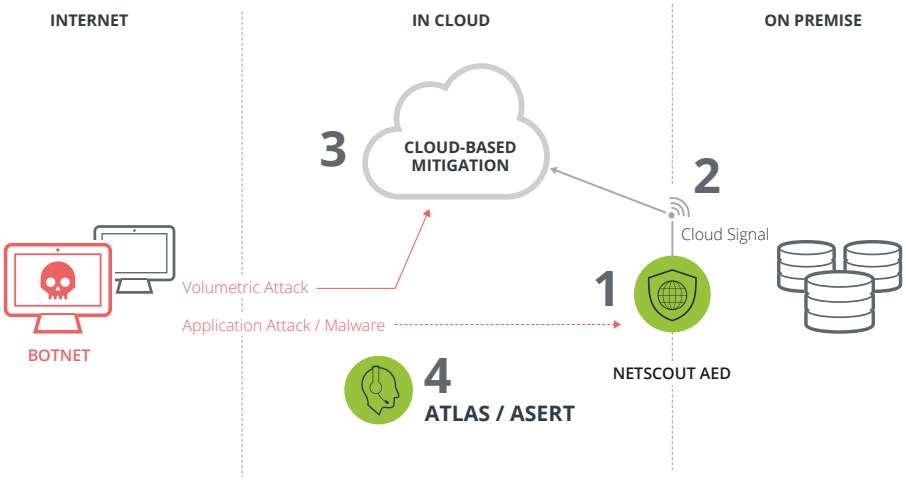
AED's robust REST API, support for Syslog, Common Event Format (CEF), Log Event Extended Format (LEEF) and STIX/TAXII enables AED to integrate with existing security technologies and processes.



AED delivers best of breed and adaptive DDoS attack protection.

To stop the modern-day, multi-vector adaptive DDoS attack, you must deploy a adaptive DDoS attack protection solution consisting of both cloud-based and on premises-based mitigation. Deployed on-premises, AED can:

1. Automatically stop inbound volumetric DDoS attacks as large as 200 Gbps. In the event of larger DDoS attack, AED's Cloud Signaling will automatically alert and/or reroute traffic to a cloud-based mitigation service (e.g. from your ISP, CDN provider, or NETSCOUT's Arbor Cloud).
2. Stop application layer attacks by combining traffic profiling, IP reputation, and intelligent challenging techniques to track and block abnormal application-layer activity.
3. Inspect encrypted traffic on premises, securely with locally stored authentication certificates and ensure traffic authenticity without slowing, disrupting or compromising legitimate traffic.
4. Using its stateless design, can stop TCP-state exhaustion attacks that target your network's stateful devices (e.g. firewalls, VPN concentrators and load balancers).
5. Stay 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 while being 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 analysis 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.

Summary

NETSCOUT AED is 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 also protects the availability and performance of not only an organization's networks and services, but also their security stack.

LEARN MORE

For more information about NETSCOUT AED visit:

www.netscout.com/product/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)

bako tech®

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers. BAKOTECH is the official distributor of Netscout in Ukraine, Georgia & CIS, Central Asia countries.

netscout@bakotech.com

+380 44 273 3333

www.netscout.bakotech.com

SECSB_001_EN-2201 02/2022