

Healthcare Organizations are Increasingly Becoming Targets of Dynamic DDoS Attacks

Healthcare Organization Uses NETSCOUT Solution To Solve Cybersecurity Challenges by Stopping DDoS Attacks Impacting Availability of Services

IT Manager uses Arbor Edge Defense to:

- Effectively stop complex DDoS attacks as efficiently as possible before they impact network, business-critical applications, or services.
- Effectively stop state-exhaustion DDoS attacks before they impact stateful network devices such as firewalls, VPN gateways, or load balancers.
- Enhance end-user and customer productivity with improved network availability, reliability, and responsiveness.

Source: IT Manager, Medium Enterprise HealthcareCompany

Healthcare Systems DDoS Challenges

The healthcare sector has witnessed an increase in multi-vector dynamic DDoS attacks. Dynamic attacks allow attackers to frequently change the attack vectors and methodologies until the attack successfully clears any existing defenses. To enhance these efforts, attackers also conduct advanced reconnaissance to fine-tune the attacks, making them more effective in reaching priority targets such as specific services, applications, or devices on the healthcare network. Attackers are also expanding their DDoS botnets and using them to launch devastating new direct-path attacks that defenders are unprepared for. The outcomes that these attacks are determined to gain are:

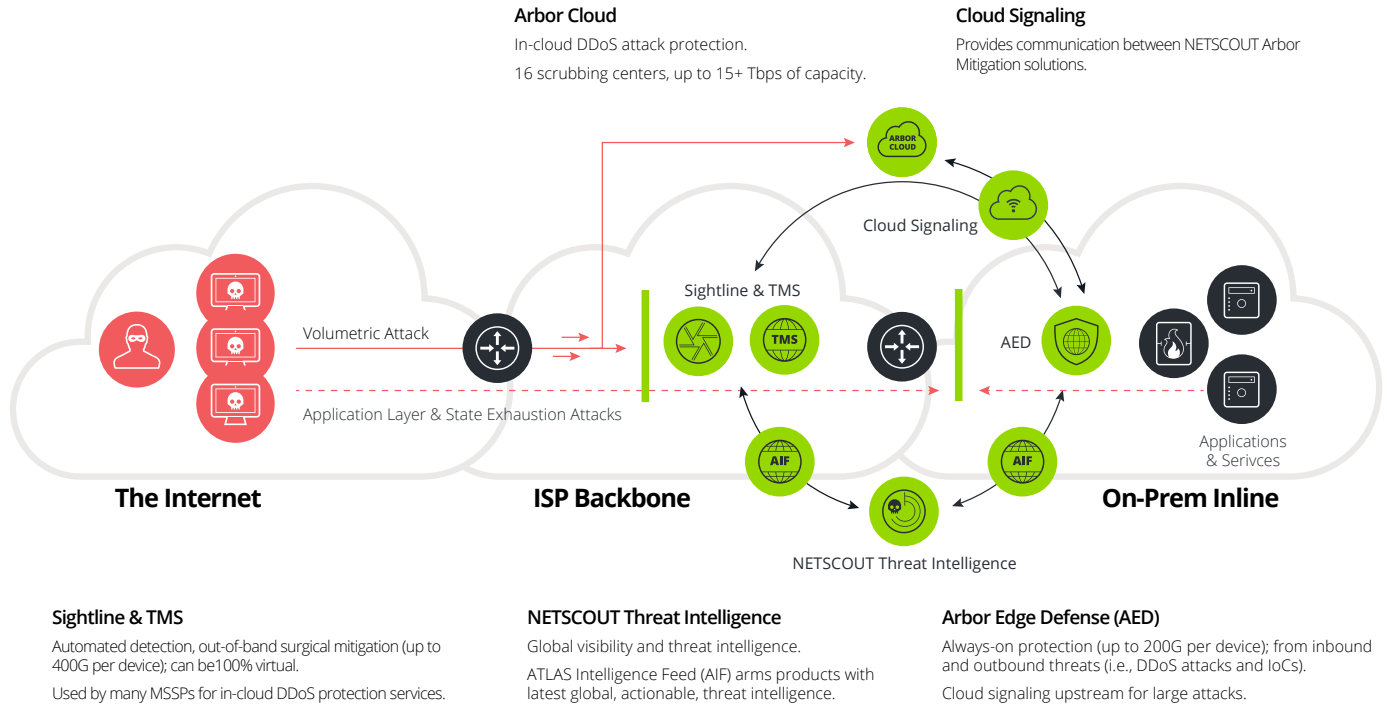
- **Service Disruption:** DDoS attacks can shut down online appointment systems, delay access to electronic health records, and interrupt communication channels within healthcare networks, affecting both patients and providers.
- **Operational Strain:** Healthcare IT teams may become overburdened during an attack, which can divert their focus from other critical IT functions and maintenance.
- **Reputation Damage:** Trust is paramount in healthcare. An institution that falls victim to cyber-attacks may suffer a loss of patient trust, which can be difficult to rebuild.
- **Patient Data Ex Filtration:** Patient data is sensitive and protected globally. It can prove valuable to attackers on the black market because it often contains a person's complete personally identifiable information.

Without proper DDoS protection, healthcare organizations are left scrambling in the dark, desperately trying to mitigate an attack that's already causing major damage. The repercussions of an unmitigated DDoS attack extend beyond mere inconvenience; they manifest in tangible crises. Critical hospital services can grind to a halt, risking lives when seconds count. Healthcare organizations can face an erosion of trust that takes years to build. And for network operators, the relentless barrage of DDoS threats creates a siege-like environment, with a constant state of security fatigue replacing the essential proactive stance needed to safeguard their digital assets.

The bottom line is that these attacks can expose access to patient records which can jeopardize compliance adherence, affect or shut down medical devices, delay vital treatments and procedures, and potentially endanger patients' lives.

Solution

What makes these new attacks hard to detect is that they are low volume and low duration. This year, of the attacks NETSCOUT® analyzed, over 90% only lasted up to 1 hour and over 74% were under 1 Gbps in volume.



While cloud mitigation solutions are useful for stopping high-volume attacks, state-exhaustion or application-layer DDoS attacks can go completely undetected when the volume is low, or the duration is short. On-premise mitigation is a complimentary and necessary addition to cloud mitigation for the protection of healthcare critical services.

Because of these changes in the threat landscape specifically targeting healthcare organizations, NETSCOUT's recommended protection strategy is to employ a multilayer hybrid approach where your ISP or cloud solution is focused on the large volumetric attacks that can shut down the organization's internet circuit, partnered with a dedicated on-premises, always on, stateless, in-line DDoS device that provides the agile defense required to adjust to attack changes and surgically mitigate attacks before they cause irreparable damage.

NETSCOUT® Arbor Edge Defense® (AED) is uniquely positioned on the network edge (i.e., between the internet router and the firewall) to provide an inline, always-on, first and last line of defense. Using stateless packet processing, continuous global threat intelligence, decades of DDoS mitigation expertise, and adaptive DDoS defense technology, AED can automatically stop inbound, dynamically changing DDoS attacks and outbound communication from internal compromised devices communicating with threat actor command and control (C2) infrastructure. Lastly, AED utilizes threat intelligence from the Atlas Intelligence Feed to identify and block IoCs – something cloud mitigation services cannot do, providing the most mitigation and security available both during an attack and even during peacetime.

By combining cloud mitigation such as Arbor Cloud® or your ISP with on-premise mitigation with AED, you have the most comprehensive protection available from massive volumetric attacks, subtle state-exhaustion, or application-layer DDoS attacks. This hybrid strategy is designed to protect the critical services that keep patients of healthcare organizations safe.

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