NETSCOUT

DDoS Attacks Have Changed:

5 Things You Need to Know!

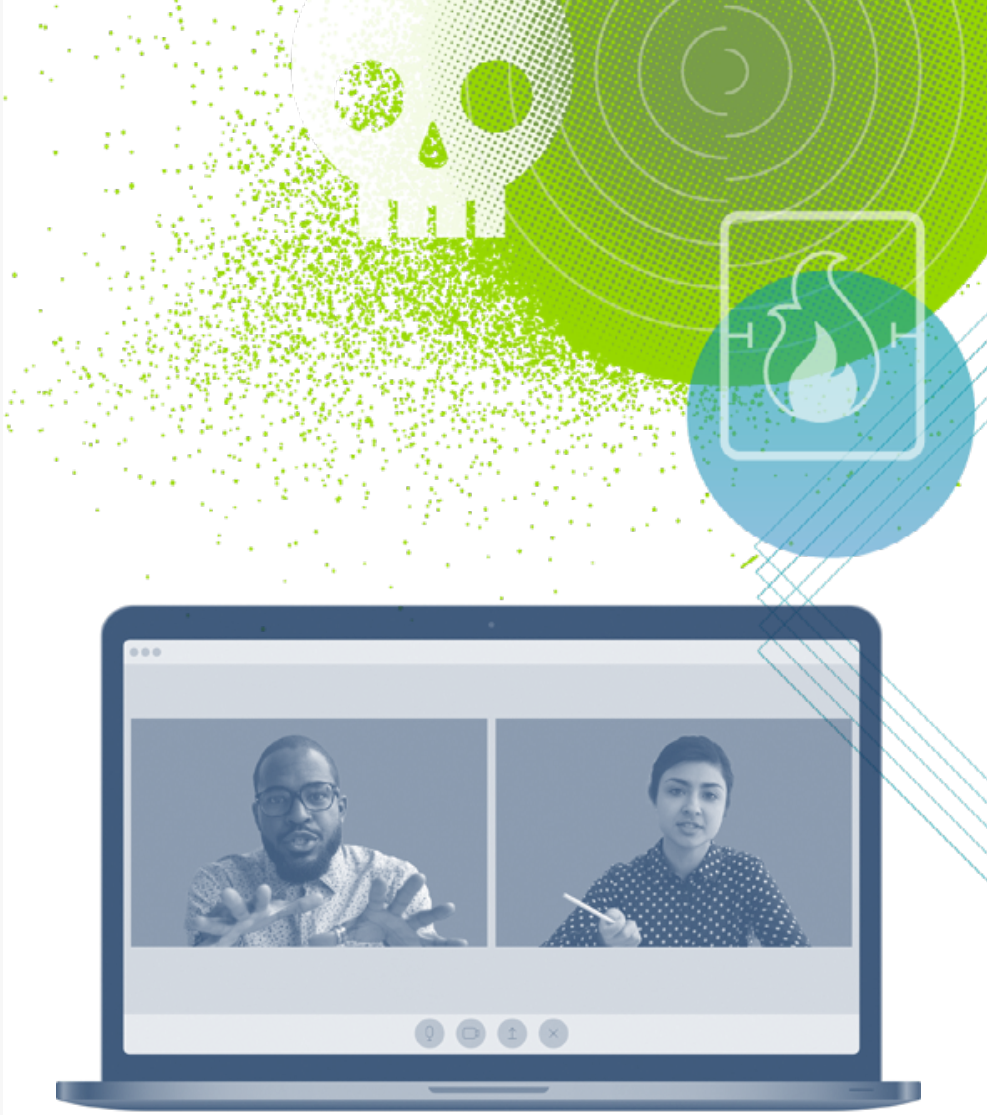
Get the Facts. Get Prepared.

DDoS attackers have multiple motivations and options of attack tools and services.

When it comes to cybersecurity, and specifically Distributed Denial of Services (DDoS) attacks, the question is not if, but when, your organization will be a target. With “bad actors” constantly improving attack methods, the risks of experiencing negative impact to your business including increased costs, lost revenue due to service downtime, or a hit to your reputation are greater than ever.

To accurately determine your organization’s risk of a DDoS attack, and to be ready to stop or mitigate the impact, you need to be aware of the latest trends in DDoS attacks and the best practices in defense.

You can always improve your security, and that starts with questioning your current assumptions.



Read on as an IT professional meets (virtually, of course!) with a NETSCOUT® security expert and learns they may have some surprising gaps in their DDoS protection plan.

Follow the conversation as the major trends in DDoS attacks and protection are discussed in this wide-ranging, virtual conversation.

FREQUENCY 1

"We are confident we have cybersecurity risk under control."

Get the facts ›

TYPES 2

"DDoS attacks are obvious to detect and we know how to respond."

Get the facts ›

PROTECTION 3

"Good thing we are safe– we have our ISP and firewalls."

Get the facts ›

MYTH 4

"Why is the firewall not enough?"

Get the facts ›

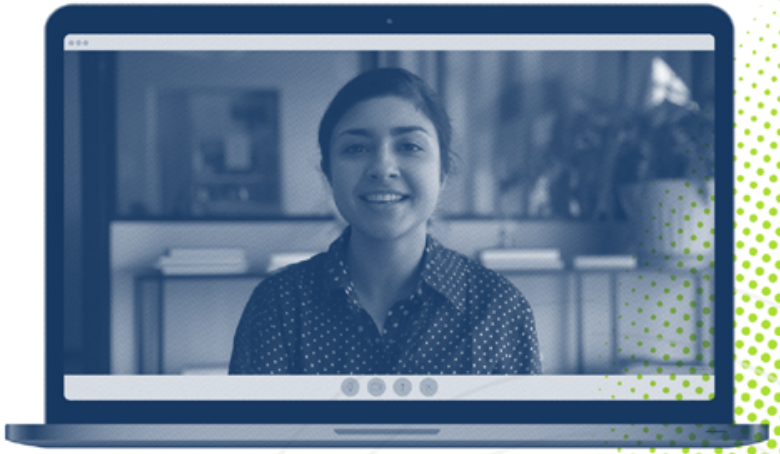
SOLUTION 5

"So, how can NETSCOUT help me?"

Get the facts ›

IT Security Professional:

1 “We are confident we have cybersecurity risk under control. Haven’t had an attack in a long while.”



NETSCOUT Security Expert:

Have you considered DDoS attacks? They are serious attacks that impact availability. DDoS attacks are by name, an attempt to deny a service; that can be any number of services, denied for any purpose.

According to our latest NETSCOUT Threat Intelligence Report, there were over 10 million attacks in 2020, which was a 20% year-over-year increase.

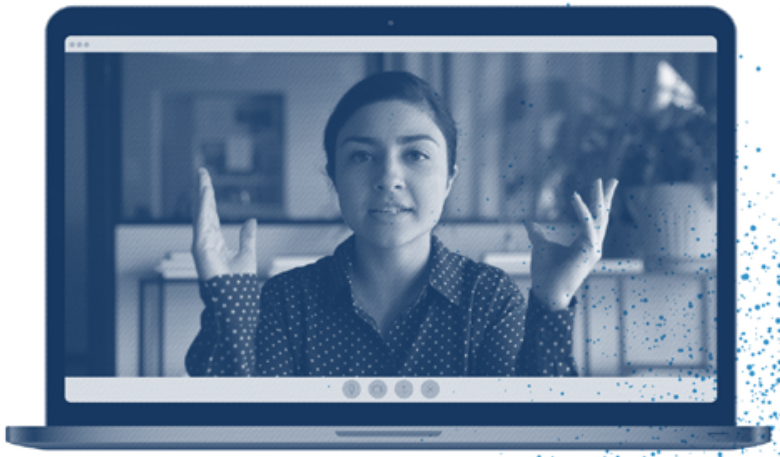
And the new normal is now more than 800,000 a month!

The combination of multiple motivations and plethora of cheap DDoS attack tools and services means the odds of your organization becoming the target of a DDoS attack are increasing.

BACK TO MENU >

IT Security Professional:

2 “DDoS attacks are obvious to detect and we know how to respond.”

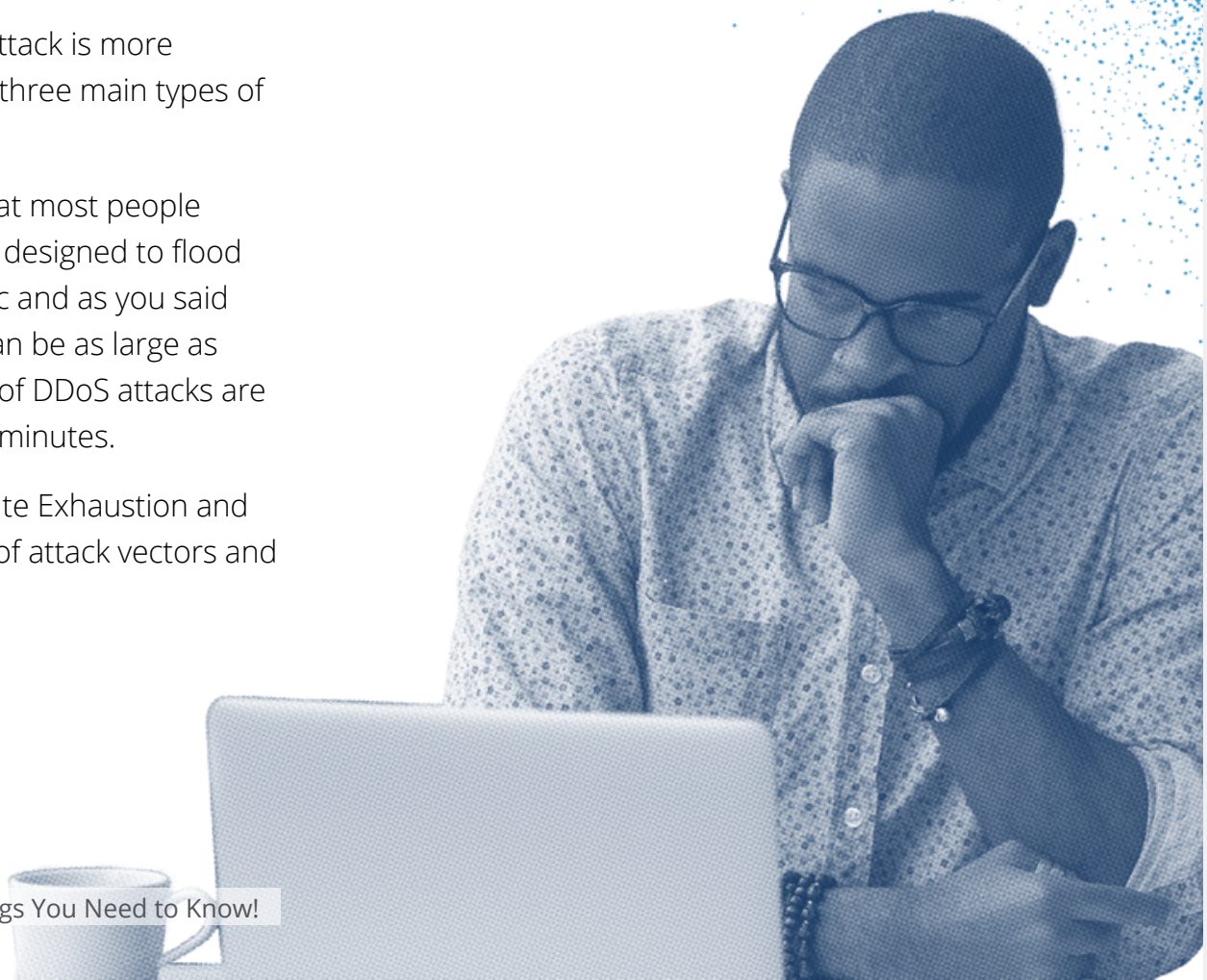


NETSCOUT Security Expert:

We hear that a lot. The modern-day DDoS attack is more complex than you think. There are basically three main types of DDoS attacks.

The first is Volumetric. This is commonly what most people think of as a DDoS attack. These attacks are designed to flood internet facing circuits with illegitimate traffic and as you said are obvious to detect. A volumetric attack can be as large as 1 Tbps, but the fact is that the vast number of DDoS attacks are under 1 Gbps in size and last for only a few minutes.

The two other types of DDoS attacks are State Exhaustion and Application Layer. Each uses a different set of attack vectors and has a different objective in mind.



BACK TO MENU >

“What is a state exhaustion attack and why should I be concerned?”

NETSCOUT Security Expert:

State Exhaustion attacks are designed to fill state tables in stateful devices such as your firewall, VPN concentrator, or load balancer with illegitimate TCP connections. When these state tables fill, legitimate connects cease and the services behind these devices are no longer available.

“What is an application layer attack and why should I be concerned?”

NETSCOUT Security Expert:

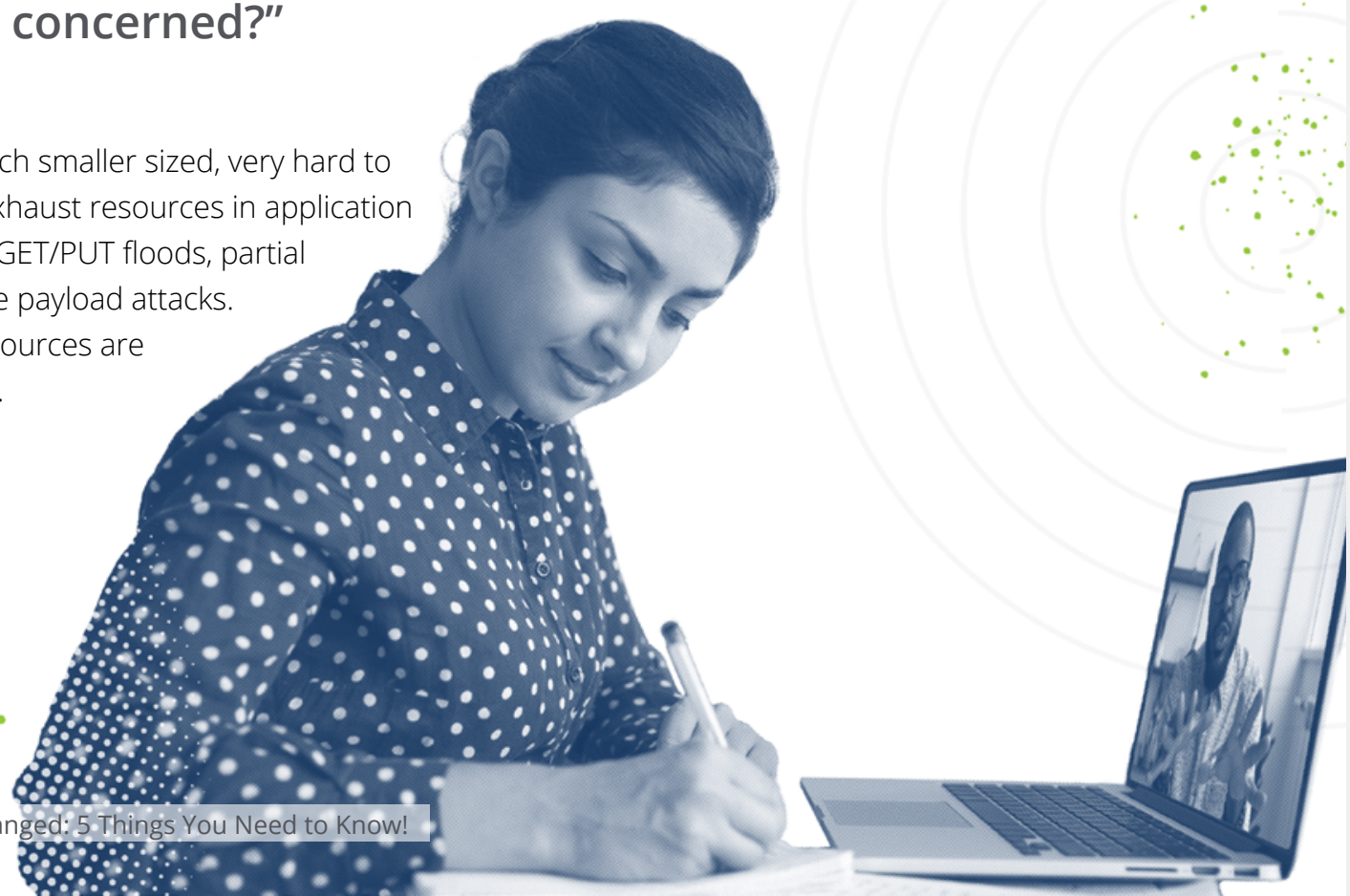
Application Layer attacks are much smaller sized, very hard to detect, and designed to slowly exhaust resources in application servers. Examples include HTTP GET/PUT floods, partial requests, slow reads or excessive payload attacks. When these application layer resources are exhausted, the application stops.

“And you’re saying these different attack types can be used against me simultaneously?

NETSCOUT Security Expert:

Yes absolutely. Remember those cheap readily available DDoS attack tools? They can easily launch a complex multi-vector DDoS attack with a simple click of a button.

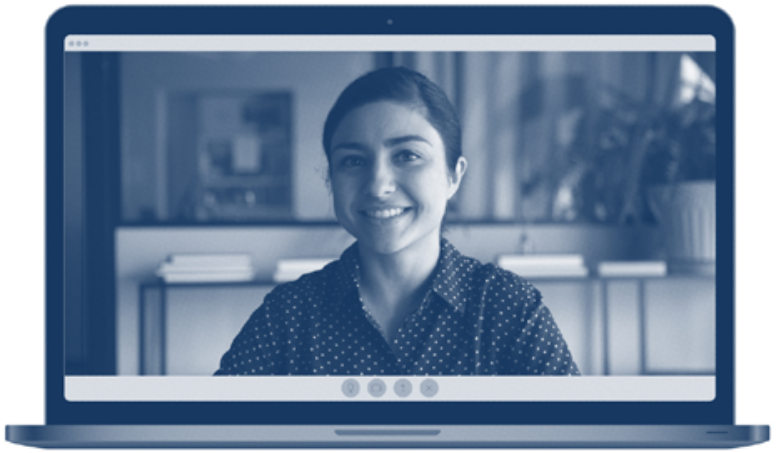
And sometimes a DDoS attack can even be a distraction while other types of cyber attacks are occurring.



BACK TO MENU >

IT Security Professional:

3 “Good thing we are safe– we have our ISP and firewalls for DDoS protection.”



NETSCOUT Security Expert:

Unfortunately, that’s not enough protection.

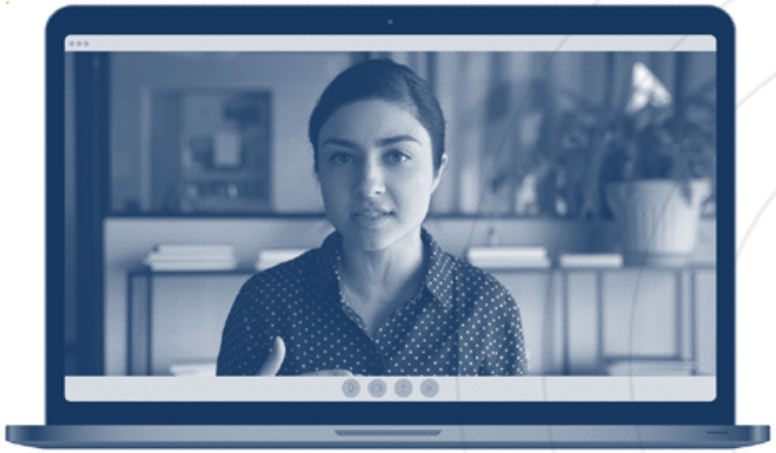
Your ISP will be required to stop the large volumetric attack that is big enough to saturate your internet circuit. But your ISP will struggle to detect and stop smaller, short-lived volumetric attacks, state exhaustion, and especially application layer attacks before the damage is done.

These type of attacks need an on-premise, stateless, DDoS attack protection solution. This on-premise protection is deployed just inside your internet router and in front of your stateful firewall or other stateful devices such as VPN concentrator or load balancer.

BACK TO MENU >

IT Security Professional:

4 "Why is the firewall not enough?"



NETSCOUT Security Expert:

State exhaustion attacks fill finite sized, state tables in stateful devices with illegitimate connections causing it to stop legitimate connections – thus denying service.

There are multiple reasons you should not rely on just firewalls:

- Firewalls do offer rudimentary DDoS attack protection such as basic SYN, UDP, ICMP flood protection. But even this limited protection impacts the performance of more important functionality such as throughput of layer-7 inspection, SSL decryption and VPN termination.
- Since a firewall relies upon inspection of bi-direction connections, it cannot work in an asymmetric-routing scenario where only incoming DDoS attack packets are seen.
- A firewall will not provide you detailed the visibility into dropped DDoS attack traffic.
- A firewall will have no way to intelligently communicate with a cloud-based scrubber solution for mitigation of large DDoS attacks.

BACK TO MENU >

5 So, how can NETSCOUT help me?

NETSCOUT Security Expert:

NETSCOUT Arbor Edge Defense™ (AED) is a stateless device that acts as first and last line of defense against DDoS attacks.

NETSCOUT helps customers all over the world defend themselves and mitigate the risk from DDoS attacks.

BACK TO MENU

Get more answers about DDoS attacks and NETSCOUT Omnis Security solutions:

netscout.com/solutions/omnis-security

NETSCOUT

NETSCOUT SYSTEMS, INC.® (NASDAQ: NTCT) delivers multi-purpose, real-time visibility, troubleshooting and protection wherever your technology infrastructure and business applications reside. NETSCOUT Smart Data gives technology and business teams the next-generation level of visibility to see the full range of performance, availability and security risks, earlier and with more precision, to resolve problems faster. That's why the world's most demanding government, enterprise and service provider organizations rely on NETSCOUT solutions to assure and protect the digital services which advance our connected world.

Visit netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

EQF_006_EN-2101 8/2021