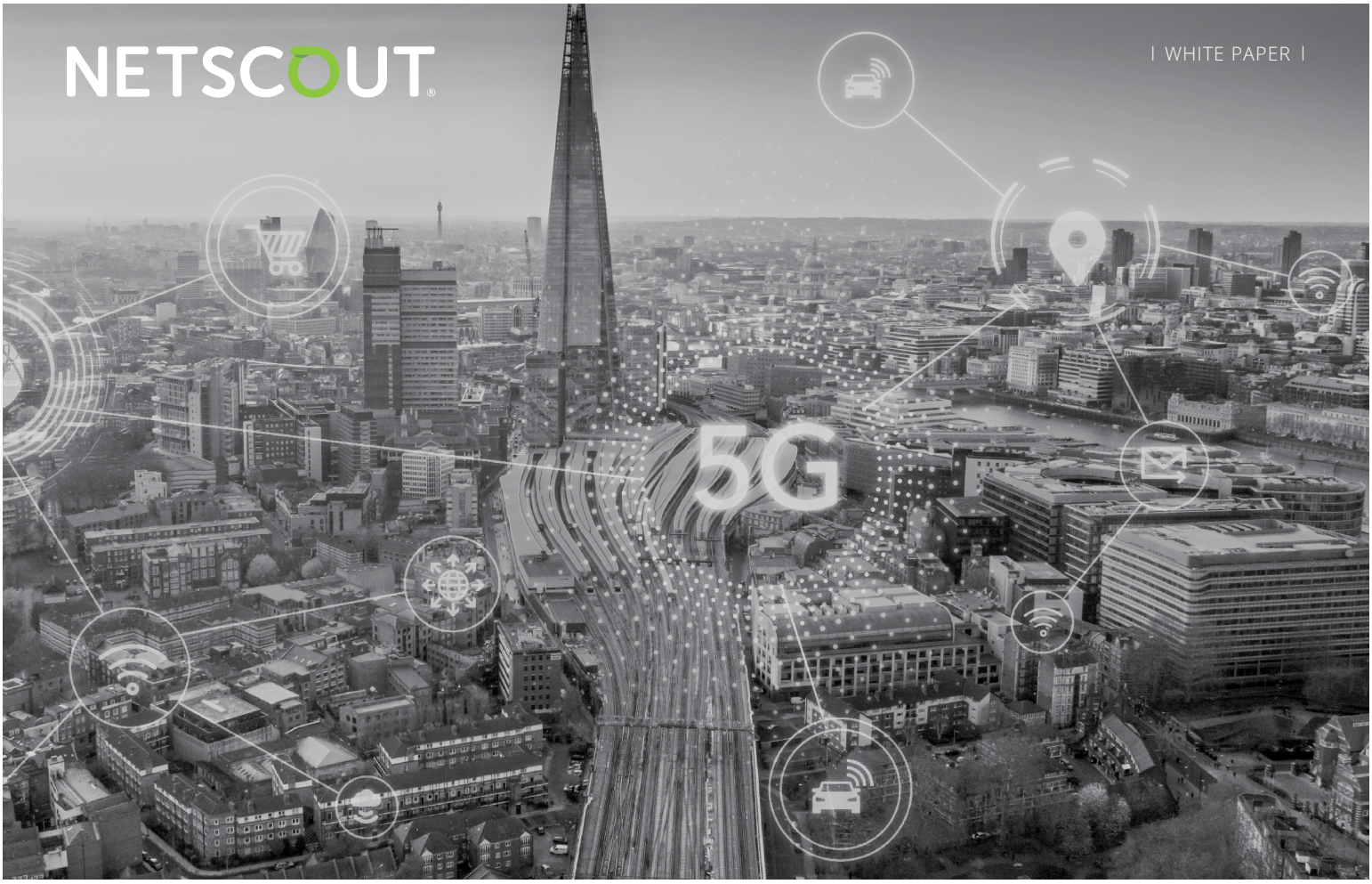

5G: A Blessing and a Curse

5G Networks Open Revenue Opportunities for Service Providers – And Create a Larger Playing Field for DDoS Attacks and Other Threats

SECURITY

TABLE OF CONTENTS

5G, The New Threat Surface

When 4G networks were launched in late 2009, little if any focus was placed on the possibility that those networks would be impacted by distributed denial-of-service (DDoS) attacks or other endpoint-generated threats. In fact, network experts didn't start sounding the alarm about DDoS attacks on 4G networks until 2012, and that focus centered largely on how malware could be used for both DDoS attack and data theft on mobile devices.

Fast-forward 10 years, and 5G non-standalone (NSA) networks have gone live. Unfortunately, unlike with 4G, service providers launching 5G services don't have to wait to see if DDoS attacks will be carried out across their networks: DDoS activity has skyrocketed. And, on top of this, 5G standalone (SA) networks are being deployed, giving attackers an even larger attack surface, with higher-value services to target.

There are many categories of security risk for 5G service providers, ranging from isolation within their infrastructure virtualization platforms, through to integrity of signalling at roaming interfaces. Historically there has been a lot of focus on security of service implementation, but security of service use has now come to the fore. Service integrity and availability are key areas of concern, with DDoS attacks targeting the user and / or control plane a key risk. And, with 5G SA bringing Ultra-Reliable Low Latency Communication (URLLC) services, SLAs around service security are a key consideration (for IoT ad Enterprise services).

There is no doubt that DDoS attacks, compromised devices, and other mobile-specific threats are top concerns for both mobile network operators and enterprise customers that will use 5G SA networks. In an Accenture survey of 2,600 business and technology decision-makers, 35 percent of respondents expressed concerns about the security of 5G, while 62 percent said they fear 5G will render them more vulnerable to attacks as they deploy new services on 5G SA networks.

And they have reason to be concerned. DDoS attacks are incredibly cheap and simple to launch. Some attacks exploit vulnerabilities in an application, protocol, or state machine, whereas others simply rely on brute force. The availability of rental botnets and simple tools has made it quick and easy for anyone to launch a DDoS attack across the internet, regardless of whether they use fixed or mobile connectivity; and, in mobile networks, the control plane represents an additional threat surface.

So, what is it that makes 5G such an attractive target for attackers? The answer, in a word, is opportunity. For every new opportunity 5G opens to service providers, it also creates new and lucrative opportunities for attackers.

Opportunity 1: New 5G Stand Alone (SA) Technology

Currently, there are more than 100 5G networks in more than 40 countries—all of which utilize 5G Non Standalone (NSA). However, operators are launching 5G SA networks. As of March 2021, 68 operators in 38 countries are investing in 5G SA for public mobile networks. Of those, seven operators in five countries already have launched 5G SA networks.

5G SA changes the mobile core architecture, replacing it with a new 5G core that's built on a service-based architecture. 5G SA also introduces a host of new protocols, as well as containerization and orchestration initiatives. Next-generation 5G services will run over new multiplexed, virtualized network infrastructures made possible via cloud-native architecture and network slicing. When combined with higher RAN speeds and multi-access edge cloud, 5G SA will deliver low-latency communications to applications and service infrastructures deployed closer to the end customer.

All of this new technology, along with new vendors and new services, represents opportunity for performance, availability, and security problems—whether from malicious attack or unintentional implementation issue. Network operators must be able to continuously monitor the behavior of their networks, services, and users so they can quickly identify outlier behavior in context.

The risk to the confidentially, integrity, and availability of the 5G core from misbehaving devices and applications—whether from malicious threat actors or benign errors—is orders of magnitude greater than any risk to the 2G, 3G, or 4G core that mobile operators have faced to date.

– 5G SA Networks Trigger A New Era in 5G Security

Opportunity 2: More Services, More Speed

Service providers are using 5G capabilities to innovate on low-latency services and edge compute, enabling enterprises to use 5G to transform their business processes. The global 5G services market size was valued at $41.48 billion in 2020 and is expected to grow at a compound annual growth (CAGR) of 46.2 percent from 2021 to 2028.

Communications service providers (CSPs) have an opportunity to accelerate return on investment (ROI) on their 5G infrastructure deployments, creating new service value from core network assets and positioning their businesses to strongly compete against over-the-top (OTT) providers and tech giants that have drained business—and revenues—away from telcos for years.

The move to 5G SA can also greatly increase both the number of mobile devices and the bandwidth available to them, increasing the capability available for launching DDoS attacks. Attackers realized long ago the importance of service availability—and as service providers are painfully aware, service disruption translates to failure to meet SLAs, customer churn, and increased network costs.

As business 5G services are rolled out across telco networks attack surfaces are growing, as applications and data are more broadly distributed. Enterprises will require visibility and threat detection to manage risk across these new 5G services, as they do with other technologies, to ensure the continued integrity of their operations and confidentiality of their data.

The big risk for operators is that a security incident damages trust in one or more of their services, slowing adoption and impacting all-important ROI.

The age of IoT-based DDoS attacks is not just on the horizon, but is already in its early stages. Hackers have already developed new malware specifically targeting IoT devices. Unfortunately, the IoT explosion has also allowed attackers to hack vulnerable connected devices so they can be used as a network for malware-infected connected devices to send an overwhelming number of requests to a target server.

– Data Driven Investor: 5G to Drive Botnet DDoS Attacks

Opportunity 3: IoT

IoT presents another considerable opportunity for both service providers and attackers. IDC estimates that 152,200 IoT devices will connect every minute by 2025. Each endpoint is both an opportunity for new, recurring revenue for telcos and a potential target for attackers.

The explosion of connected IoT devices, whether consumer, enterprise, or industrial in nature, creates a huge attack surface. In the case of consumer devices, as in wireline networks, devices can be compromised and used for volumetric DDoS attacks designed to overwhelm the network and impact services. In the case of enterprise or industrial IoT, the consequences of compromise can range from reduced lifespan of the device itself, through data breach, to loss of integrity in services that support real-world critical functions. As above, problems can result in SLA violations, customer churn, and reduced ROI.

As such, it's imperative for CSPs to secure 5G-enabled IoT deployments, ensuring they can identify whether unusual behavior is malicious or a malfunction. Maintaining continuous monitoring is key. Operators need solutions that will enable them to stay on top of network, service, and endpoint security, proactively monitoring traffic patterns and resource utilization across both user and control planes to prevent possible service impacts—whatever their source.

What CSPs Can Do to Protect 5G Networks

When the global COVID-19 pandemic hit full force in 2020, service providers managed enormous spikes in legitimate network traffic—streaming video, video conference calls, gaming, and so on—while also defending an increase in attacks that targeted critical network infrastructure and services. In fact, the 2H 2020 NETSCOUT Threat Intelligence Report found that 70 percent of service providers experienced inbound DDoS attacks, and 71 percent said such attacks are their top security concern.

For 5G networks to deliver new services and revenue opportunities, operators must be proactive about protecting the networks, services, and customers—especially enterprise customers—from a broad range of threats.

CSPs should take several actions to protect their 5G networks, services, and customers, including the following:

- **Ensure there is end-to-end visibility of service traffic inside the packet core, as well as when traffic enters and leaves.** For risks to be identified in context, it's essential to have a complete, consistent view across control and user plane activity inside the core. Likewise, providers need the ability to view traffic to or through key infrastructure, including DNS and CG-NAT.
- **Integrate security assurance capabilities within the mobile network.** Doing so provides correlation across both the user and control planes, allowing a broader range of threats to be identified. Additionally, it enables contextual information to be incorporated into any event—a key factor for establishing the potential impact and selecting the right mitigation strategy.
- **Implement automated attack detection, rate limiting, and mitigation.** Threats should be detectable across control and user planes and service-enabling infrastructure. The ability to quickly rate limit or mitigate via either direct intervention or network policy functions is key.
- **Ensure continuous situational awareness via consistent visibility and smart data metrics.** Threat detection capabilities are important, but so is having an ongoing view of trends in network, service, and user behavior. Situational awareness is key to getting ahead of threats and identifying outlier behaviors and misconfigurations.

Adversaries developed new adaptive DDoS attack strategies that evade traditional mitigation techniques. Threat actors custom-tailor each attack to bypass multiple layers of DDoS mitigation and protection, both cloud-based and on premise.

– NETSCOUT Threat Intelligence Report, 1H 2021

- **Utilize threat intelligence.** Threat intelligence is a crucial tool for threat detection and mitigation, identifying compromised devices communicating across a network, as well as automating responses to specific attacks. As mobile malware continues to proliferate, and as more IoT devices are deployed, botnet population monitoring has become ever more important.
- **Integrate datasets and solutions.** The ability to integrate or utilize common sources of data across the security and operations stack multiplies investment value and maximizes the utility of deployed solutions. For example, using a common and consistent source of network-derived packet data that contains a rich set of control and user plane metadata and packets will benefit both NetOps and SecOps teams.
- **Take a risk-based approach to protecting services.** Services drive return on investment, but they don't all have the same requirements or risk levels. Deploying visibility, service, and security assurance capabilities should focus on ensuring the right capabilities for the right services.

All of the above can contribute to a faster response to any detected threat, ultimately protecting 5G networks and accelerating the adoption of services running across them.

Learn More

To learn more about protecting 5G networks, the services they enable, and how they can be defended, contact us today.

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

SECWP_022_EN-2101 10/2021