kentik

The NetOps guide to network security

Detect and mitigate threats like
DDoS attacks, BGP hijacking, and more

Table of Contents

Introduction

Modern networks present a uniquely challenging landscape for cybersecurity professionals. They are complex, involving connections to data centers, private and public cloud services, the internet, CDNs, WANs and SD-WANs, VPNs, container environments, IoT, third party infrastructures, and more. These connections can be short-lived, difficult to monitor, and occur across thousands of instances.

To help manage this complexity, cloud providers have made it easy to configure infrastructure-as-a-service (IaaS), including the network constructs, allowing application developers to easily change network configurations. This ease can create problems such as introducing unnecessary security risks, unforeseen costs, and performance reductions. Without a NetOps team and network security strategy in place, problems such as ingress and egress points with no security policies, internal communications routed over internet gateways, abandoned gateways, abandoned subnets with overlapping IP address space, or VPC peering connections with asymmetric routing policies can proliferate and expose your network to threats.

To make matters more challenging, IaaS, PaaS, and SaaS often black box the majority of their networking decisions, adding another layer of complexity that gives traditional network monitoring solutions limited visibility into important networking data. The applications depending on these cloud services are also often deployed with CI/CD systems, allowing for application updates to be deployed at a rapid pace, requiring an equally agile system of network security updates.

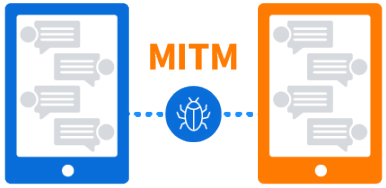
All combined, this represents a widespread attack surface to secure against potential threats. And, unfortunately for network security specialists, the planet-scale virtualization of computing resources pioneered by cloud providers has provided malicious agents with cheap, difficult-to-track resources that can levy quick and powerful attacks.

In this guide, we will take a closer look at some of today's most pressing network security threats and show you how to use the leading principles, best practices, and tools of network observability to secure your applications against them.

Network security threats

While internal vulnerabilities are commonly exploited, external threats such as Distributed Denial of Service (DDoS) and man-in-the-middle (MITM) attacks represent significant risk to your network's health and performance.

DDoS attacks with botnets are cheap, widely accessible, and fairly easy to implement and execute. They target a network's capacity and seek to cause downtime. The downtime itself can cost companies hundreds of thousands of dollars in missed revenues and SLA violations.



MITM attacks involve a party intercepting data with techniques like eavesdropping, hijacking, and spoofing. These attacks can create significant data vulnerabilities.

Why network observability matters for cybersecurity

Traditional network monitoring typically requires human intervention to first baseline normal network and traffic behavior. Then, monitoring tools identify and alert teams about changes to the expected behavior.

For example, teams can use SNMP to baseline throughput behavior of a critical network link over time. Once administrators determine the baseline behavior, the monitoring tool can alert them when throughput behavior spikes above what's typical. A network operations (NetOps) technician then fields the alert and troubleshoots why the change in network behavior occurred.

The complexity of a cloud network's topology, the ephemeral nature of many cloud resources, and the speed and sophistication of modern attacks create a security environment that can cripple networks that rely on this traditional monitoring approach. With attacks specifically designed to fly under the radar of these human-centric monitoring protocols, modern cloud networks need powerful, intelligent, and automated solutions that can handle threats before the network is compromised.

Network observability offers the best line of defense to external attacks on your networks. By being able to use your aggregate network data intelligently, network observability can help your team surface the threat, point to likely sources, and even automate proactive mitigation solutions under the right conditions.

Here is a simple framework for what it takes to make this level of network observability possible:

- **See all networks**
  You need a visual representation of all the networks over which your traffic flows, whether you own them or not.
- **Ingest telemetry**
  Have a system that can receive or poll for all kinds of network telemetry, and then ingest it efficiently so it can be analyzed, correlated, and measured over time.
- **Enrich the telemetry with context**
  Enrich the telemetry you collect with metadata that adds useful context such as application, business unit, geolocation, or security group. This context helps you analyze traffic and granularly enforce policy, and will provide business and security insights.
- **Ask any question**
  Context-rich telemetry will enable systems that let you query, filter, drill in, zoom out, and map your network telemetry, no matter how large or complex the data set. Getting super-fast responses to your queries is key here.
- **Get unprompted insights**
  Beyond being able to ask questions, network observability allows you to benefit from proactive insights, alerting to things like degrading performance, anomalous traffic changes, or possible attacks before they compromise your network.
- **Take action**
  Network observability gives your NetOps and SecOps teams the ability to automate internal or third-party workflows, including sending alerts, opening service tickets, initiating mitigations, or sharing enriched data with other applications.

Now that we've gotten a closer understanding of what it takes to make a network observable, let's see how these systems and strategies can help your organization defend against today's biggest network security threats.

DDoS attacks

DDoS attacks are a cyber attack that most often have the purpose of causing application downtime. This downtime can itself be the ultimate goal for the attacker, but can also be used as a way to weaken security systems, cover tracks, or act as a red herring for investigators, while a more significant vulnerability is exploited elsewhere in a network.

These attacks can involve coordinating thousands of devices, virtual or otherwise, to overwhelm the target server's resources.

According to Radware's 2022 H1 Global Threat Analysis Report, DDoS attacks have risen dramatically in 2022, continuing a trend seen since the beginning of the pandemic in early 2020. Compared to their 2021 data, they saw over a 200% increase in DDoS attacks in the first six months of 2022.

With such a huge emphasis on the network by attackers, any serious DDoS security solution needs intelligent, capable network observability to automate rapid detection and mitigation.

Types of DDoS attacks

1

Volume-based

These attacks are measured in bits per second (Bps), and aim to overwhelm a service's bandwidth capabilities with prohibitively high traffic volumes. Common volume-based DDoS attacks are ICMP and UDP floods.

2

Protocol-based

These attacks are measured in packets per second (Pps), and overwhelm network infrastructure resources, targeting layer 3 and layer 4 communication protocols. Common protocol-based attacks are Ping of Death, Smurf DDoS, and SYN floods.

3

Application layer

These attacks are measured in requests per second (Rps), and typically seek out web server vulnerabilities with malformed or high-volume requests in layer 7 services. Common application layer attacks include HTTP floods and slowloris.

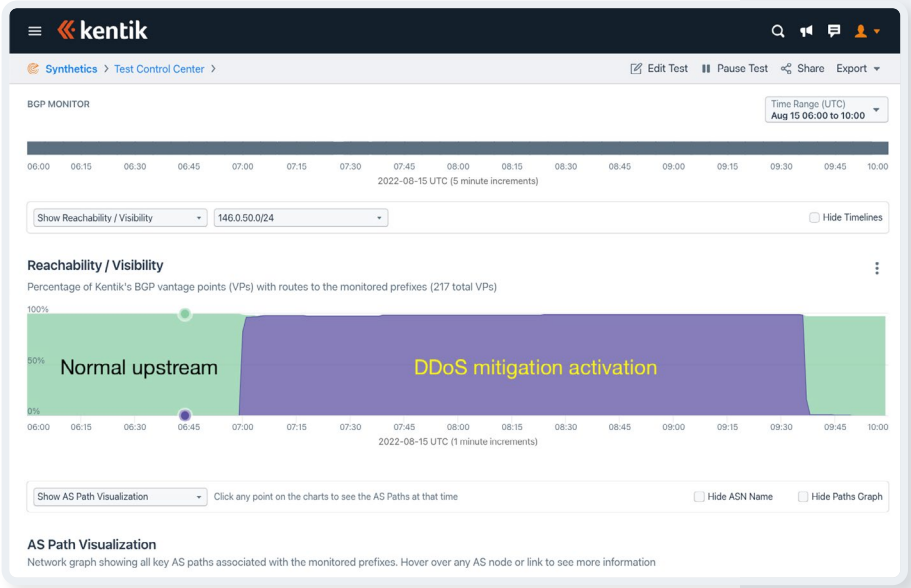
Using network observability to detect and mitigate DDoS attacks

At Kentik, we see thousands of DDoS mitigations activated each week.

DDoS attacks continue to increase in number, volume, and sophistication. A June 2022 blog by our partner Cloudflare detailed one of the largest and most powerful DDoS attacks ever. The Mantis botnet was able to launch an attack that generated 26 million HTTPS requests per second! The cost to undertake DDoS attacks is plummeting, while the tools for carrying them out are becoming more sophisticated.

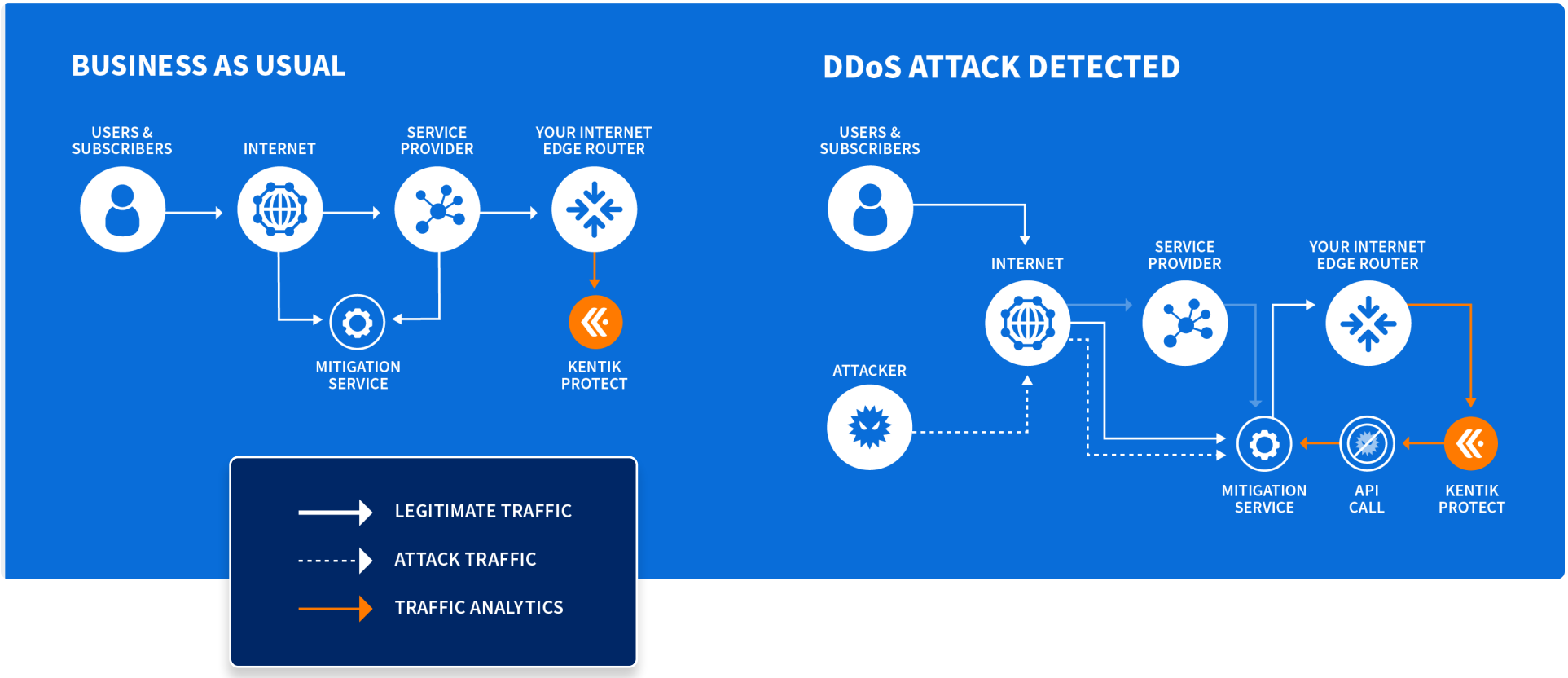
Traditional network monitoring, with its disparate tools, processes, and human checkpoints, is too slow to prevent modern DDoS attacks from impacting a system. And every minute counts! A 2020 Neustar report on cyber threats and trends found that even though DDoS detection and mitigation needs to happen within a minute, as of November 2020, only 25% of DDoS mitigations are initiated soon enough. Why? Because so many network DDoS defense strategies still rely on some degree of manual intervention.

But, with context-rich telemetry from all your networks, and a powerful, data-informed analytics engine, you can give your NetOps and SecOps team an edge in the fight against DDoS.



The following are ways network observability can help you detect and mitigate DDoS attacks:

- Early detection
- Low-volume detection
- Understanding the context of the attacks
- Eliminating false positives
- Evaluating mitigation strategies
- Performing attack forensics
- Cost control and optimization



Early detection

The importance of early detection and mitigation of a DDoS attack cannot be overstated. It will save you time, frustration, revenue, traffic cost, brand equity, and help you keep your infrastructure secure.

Capable network observability solutions will automatically detect early signs of attacks, such as traffic spikes, excessive latency, or other anomalous traffic behavior by analyzing your real-time and historic NetFlow data. This traffic flow data is constantly compared against benchmarks to catch anomalous traffic patterns, giving network and security engineers what they need most: the awareness and the time to mitigate the attack and protect their network before the attack can cause damage.

Low-volume detection

When most people think of DDoS attacks, they think of massive volumetric attacks that crash websites or networks. In reality, most DDoS attacks are small in size and duration, often less than 1 Gbps and only a few minutes long. DDoS detection tools are often configured with detection thresholds that ignore or are incapable of seeing these attacks.

These low-volume attacks are often used to mask security breaches. Hackers will use a DDoS attack to distract SecOps, while simultaneously launching a more rewarding security breach. The security breach could involve data being exfiltrated, networks being mapped for vulnerabilities, or infiltration of ransomware.

Network observability solutions allow you to baseline against small traffic volumes, enabling network engineers to fine-tune thresholds and alerts accordingly.

Understanding the context of the attacks

SNMP metric data is simply not enough. Flow data enriched with SNMP gives you the ability to understand the attack in context. It gives details on where the attack is coming from, as well as what IP addresses, ports, or protocols make up the attack.

Identifying where traffic originates and normal traffic flows from those sources is keystone data to a defense strategy. The context-rich telemetry that network observability solutions use includes critical network information like geolocation.

To protect your infrastructure, you need to be able to build policies based on certain geographies, such as an alert if the traffic is from an embargoed country. Being able to identify the source of the traffic can help tremendously in the detection of security breaches. Identifying traffic from an unusual traffic source may be the key to early mitigation.

Context helps with mitigation by clarifying the nature of the attack with relevant details, as well as providing a means for applying more accurate filters against the traffic.

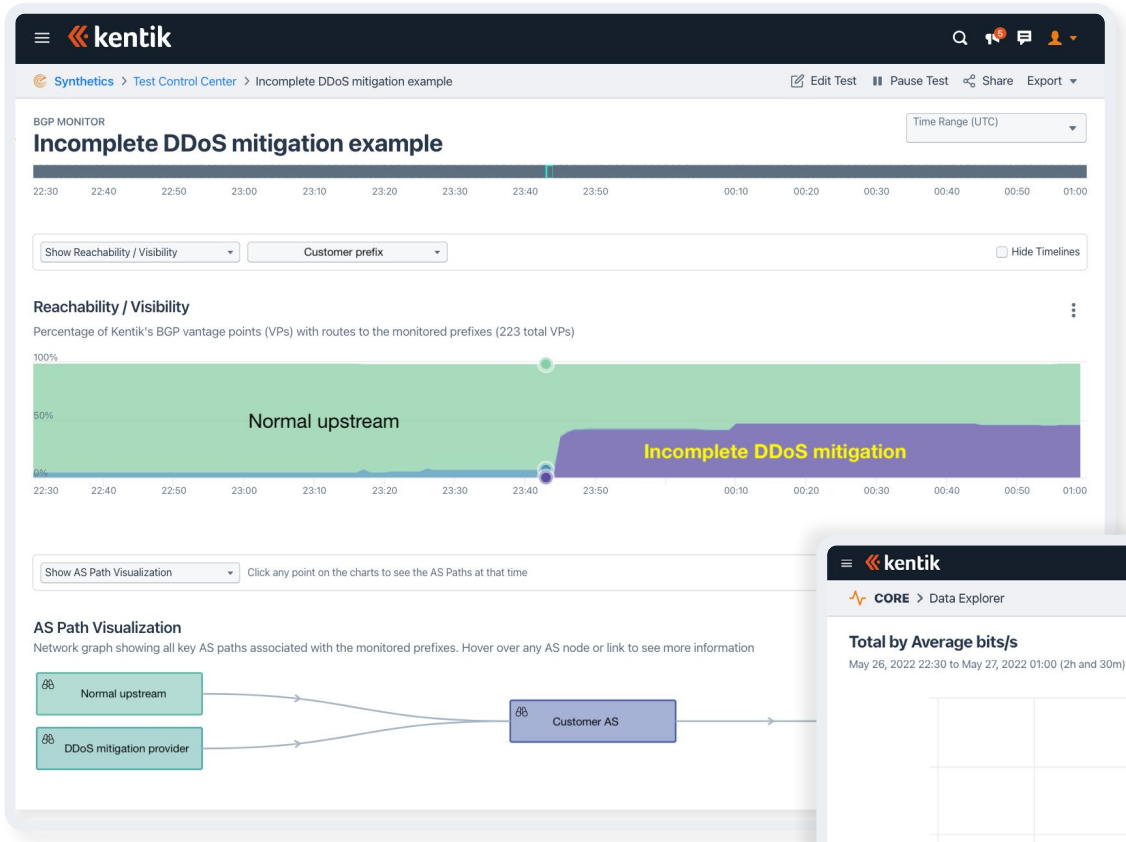
Eliminating false positives

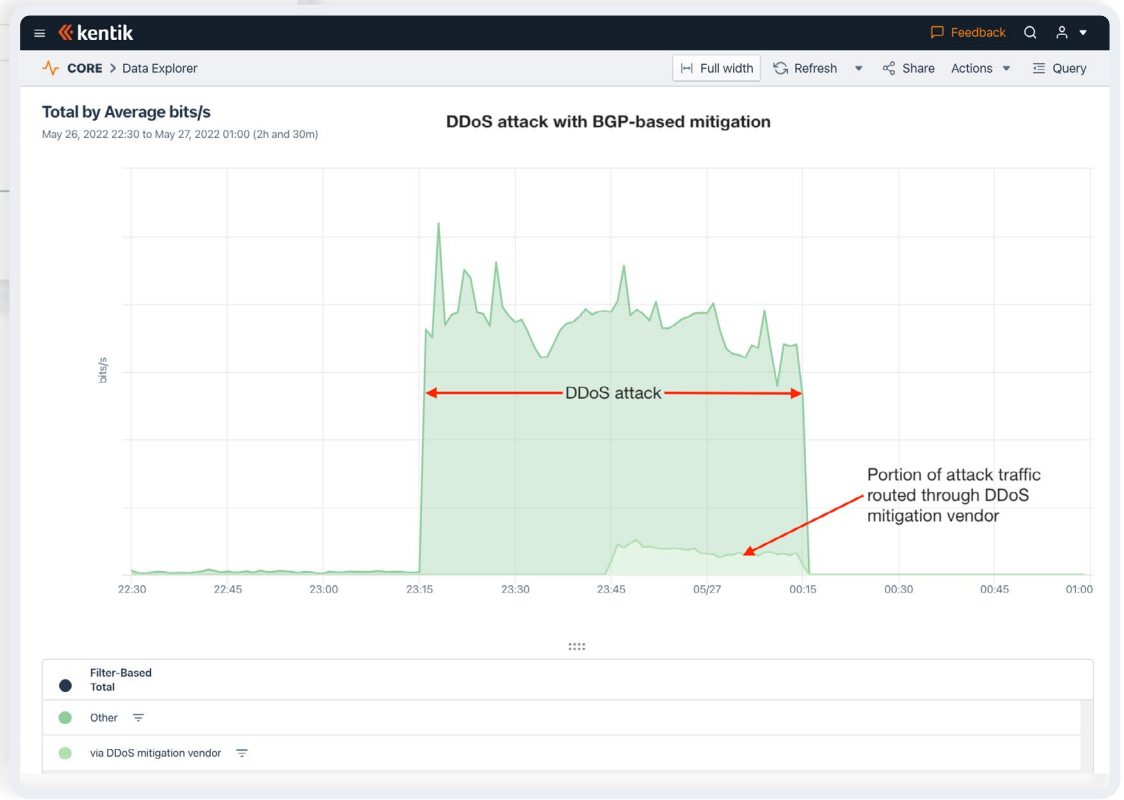
Without a network observability platform that gives you granular traffic analysis, automated mitigations can cause you to filter traffic that is needed by your end-users. This can result in you causing an outage for your users in an attempt to block an attack.

False positives can be a big distraction for your SOC team. Alerts that, upon investigation, are revealed to be normal traffic result in alert fatigue. Eventually, your security experts will stop paying attention to the noise, leaving you open to malicious attacks.

Evaluating mitigation strategies

Mitigation services and technologies sometimes don't achieve full coverage and attack traffic can circumvent the mitigation leaving you exposed. It's important to be able to use NetFlow to analyze what DDoS traffic has been redirected for scrubbing and what traffic has been missed. And perhaps just as important, being able to monitor BGP from hundreds of vantage points can enable you to understand how quickly your mitigation service achieved full coverage, if it did at all.





The BGP visualization on the left shows a DDoS mitigation vendor (purple) appearing upstream of the customer network but never achieving complete coverage of the customer network. Below, we can see the result of this incomplete activation as only a portion of DDoS traffic is ultimately redirected to the DDoS mitigation vendor. An incomplete DDoS mitigation permits attack traffic to reach the target network, imperiling critical services.

Performing attack forensics

Many DDoS attacks fit a pattern. Many of the same bad actors perpetuate them and their fingerprints can be well masked. A good network observability solution will allow you to look back in time to understand and ask any question about the traffic.

- Have we seen this attack before?
- Where was the attack from?
- What protocols are associated with the attack?
- Are there patterns?
- How can a similar attack be prevented in the future?

Cost control optimization

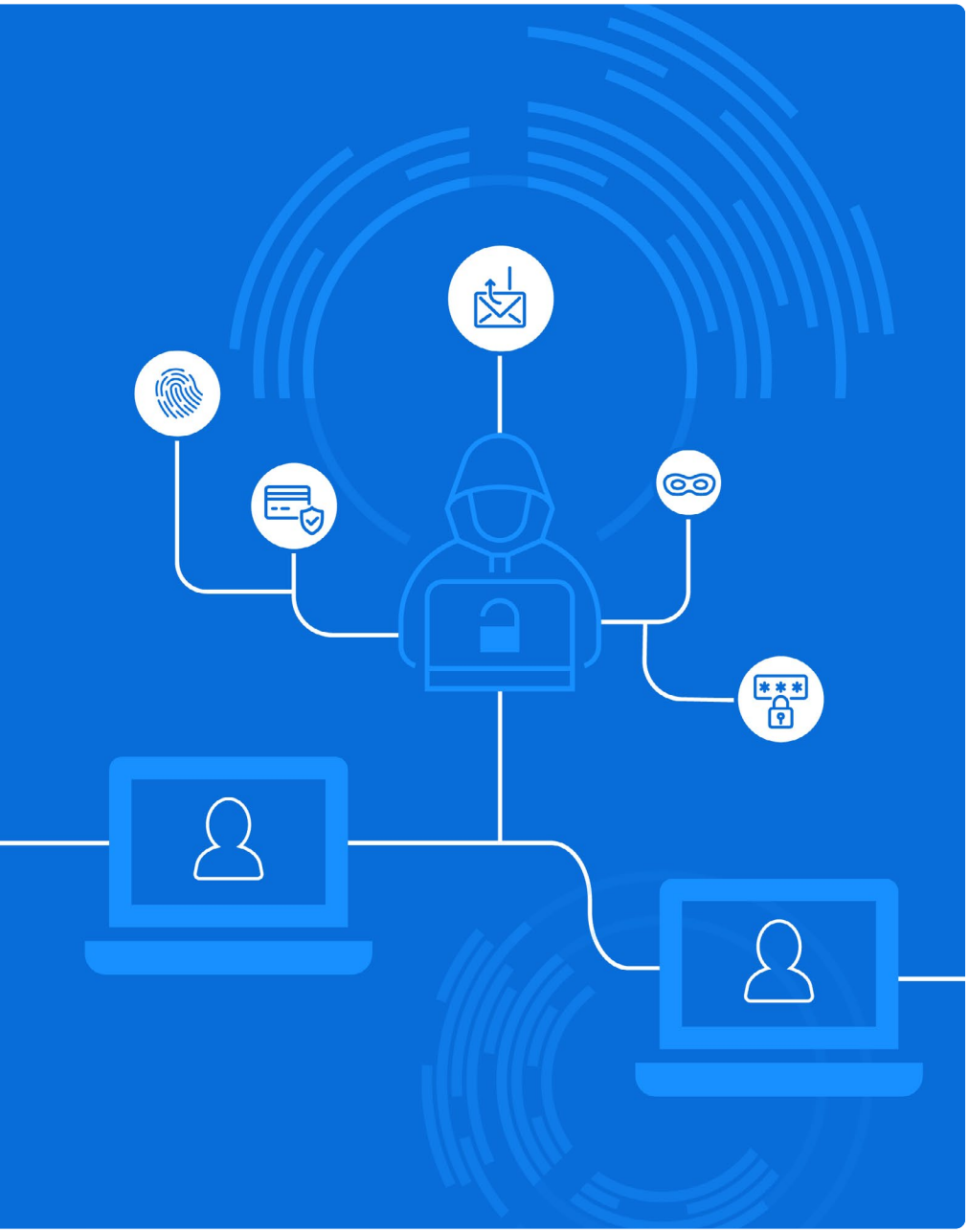
DDoS traffic can cause havoc in 95th percentile pricing models and always-on mitigation services can be expensive. True network observability will give you the ability to detect attacks at their onset, decreasing the chances of exceeding traffic limits, protecting your infrastructure, and giving you the ability to engage a mitigation service before the attack takes hold.

Remote-triggered black hole (RTBH)

One of the main benefits of early DDoS detection is the ability to divert malicious traffic away from critical services. RTBH routing is a fast, cost effective way to automate the redirection of suspect traffic, giving operators the ability to quickly mitigate DDoS and enforce routing policies.

Though there are many RTBH implementations, destination-based RTBH is considered the gold standard as a first line of defense against DDoS attacks. Once anomalous traffic is spotted, a “black hole” route is redistributed via BGP to the affected routers, which will then send the anomalous traffic to a harmless destination.

With a network observability solution like Kentik Protect, traffic thresholds, alerts, and triggers can all be configured as code, automating cost effective DDoS mitigation strategies like RTBH and protecting your networks before malicious traffic can cause harm.



Man-in-the-middle attacks

Taking advantage of weaknesses in protocols, both human and software, can allow malicious agents to intercept data via false or redirected interfaces.

Spoofing

Spoofing is a hallmark MITM strategy, wherein a malicious agent intercepts and redirects traffic with false credentials. The attacker can spoof IP addresses, DNS, HTTPS headers, and more to deceive users into interacting with compromised applications.

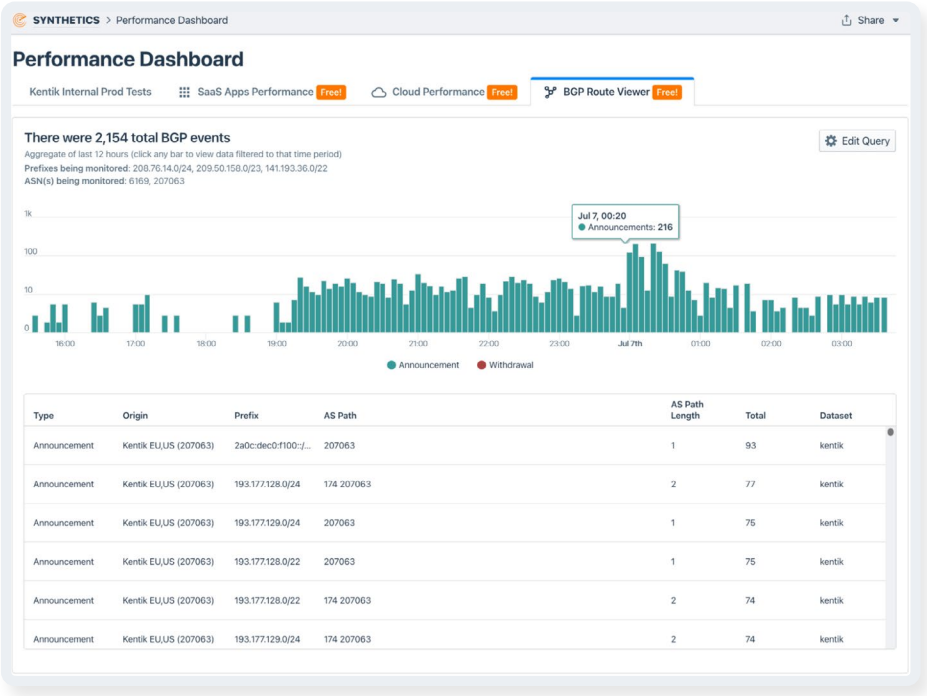
Hijacking

Similar to spoofing, hijacking involves compromising a network component and using the incoming traffic to compromise sensitive data.

In recent years, BGP hijacking has increasingly become a concern for businesses that need to ensure quality internet traffic flow. Border Gateway Protocol (BGP) is a long-established, policy-based routing protocol for the internet. BGP exploits cause changes to the routing of the internet's autonomous aystems, and can cause serious disruption to a web application's internet traffic.

Using network observability to handle MITM attacks

As part of the “See all networks” component of network observability, gaining full visibility into not only your network’s BGP status, but global BGP status data, is a crucial step in being able to act quickly and mitigate attacks against your network.



BGP monitoring

Although MITM attacks are difficult to observe directly, a state-of-the-art BGP observability solution will be able to provide the following security benefits:

✓ Event tracking

See route announcements and withdrawals over time and filter the data by day, hour, AS, prefix, and announcement type.

✓ Hijack detection

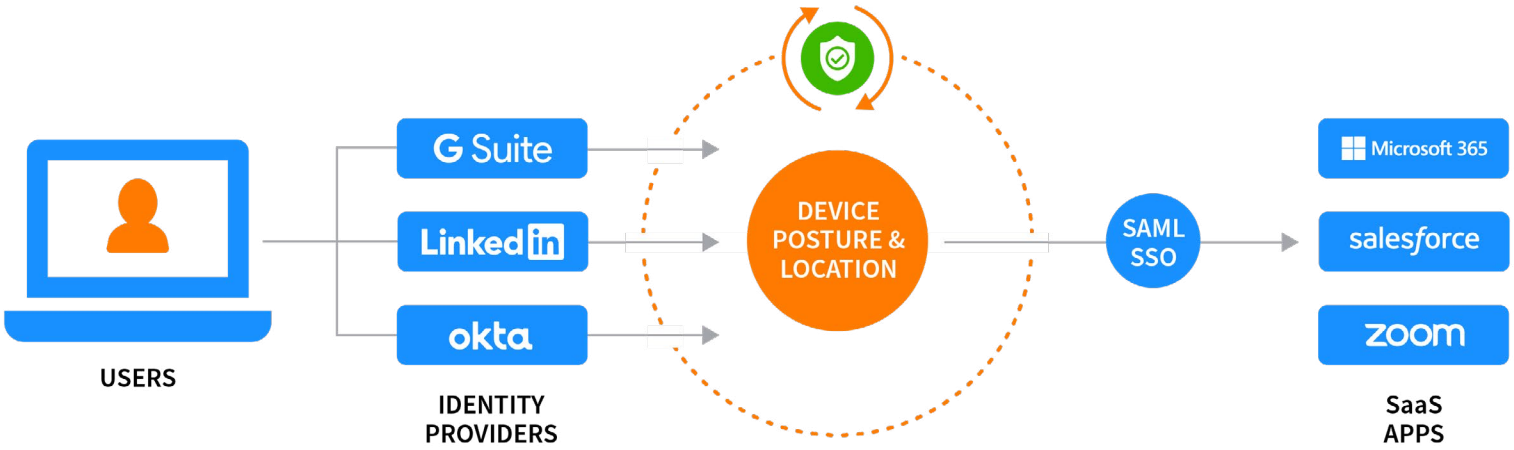
Be alerted as soon as an unauthorized origin or upstream appears in the global routing table for one of your routes, not after news breaks on Twitter.

✓ Route leak detection

Find misconfigurations and bad code that expose your network’s BGP routes to vulnerability.

✓ RPKI status checks

Get alerted to any route containing your address space that is being evaluated as RPKI-invalid. This would include accidental leaks, intentional hijacks, but also a misconfigured ROA that is causing your authorized route to be rejected.



Zero Trust

Traditionally, the go-to identity verification model has been castle-and-moat, where access to the network (the castle) is well-protected, but once access is achieved, a user is trusted to move freely about the network. This model has proven unsustainable as the boundaries of an organization's network become less firm. With the incorporation of cloud and edge services, third-party dependencies and infrastructures, and remote work forces, a new model has developed to handle the growing security concerns of working in a distributed environment: Zero Trust.

Zero Trust security has a foundational technology attached, Zero Trust Network Access (ZTNA), but more importantly encompasses a holistic approach to security in a simple phrase: trust no one and nothing. What does implementing Zero Trust in your network security look like? There are several tenets of Zero Trust, that, when implemented together, represent a vigilant network security strategy:

- **Continuous validation** – sessions should timeout and users should be forced to re-verify frequently.
- **Multi-factor authentication (MFA)**, such as 2FA, where login credentials must be separately verified, such as on a previously trusted device.
- **Device verification** to ensure only trusted devices are trying to access your network.
- **Least privilege access** to users to minimize threat exposure.
- **Network segmentation** to prevent lateral movement – coupled with least privilege access, identity verification between network segments helps ensure that an exploited vulnerability does not bring down the entire network.

Summary

NetOps teams must adapt to keep pace with the ever-shifting tactics of attackers. Traditional network monitoring relies on too many separate processes and points of manual intervention to be agile enough for today's security threats.

But implementing network observability tools and best practices gives your NetOps and SecOps teams the edge they need to protect your networks.

With benefits like early attack detection, context-rich telemetry that paints a clear picture of the attack for mitigation and forensics, and the ability to automate and optimize mitigation strategies, network observability can help you protect your network before an attack can cause damage to your customers or reputation.

Thanks for reading **The NetOps Guide to Network Security —** stay tuned for more great content from Kentik.

Kentik Protect: Neutralize DDoS attacks. Analyze incidents. Catch botnets.

Kentik Protect is the industry's most accurate DDoS and network anomaly detection solution, offering field-proven accuracy gains of 30 percent in attack recognition.

With Kentik Protect, you can:

- Ingest and unify, in real-time, massive volumes of NetFlow, sFlow, IPFIX and BGP data, network performance metrics, and SNMP device and interface data.
- Apply the scale-out power of the Kentik Network Observability Cloud to network-wide scanning of billions of rows of data using multi-dimensional criteria and adaptive baselining.
- Automate hybrid mitigation via standards-based BGP Flowspec and remote-triggered black hole (RTBH), as well as integrations with mitigation solutions from leading vendors, including Cloudflare, A10, Juniper, and Radware.
- Enhance the ability to investigate and understand attacks with deep ad-hoc traffic analysis, flexible dashboarding, botnet detection, and network performance monitoring.

Your network's best defense against attacks

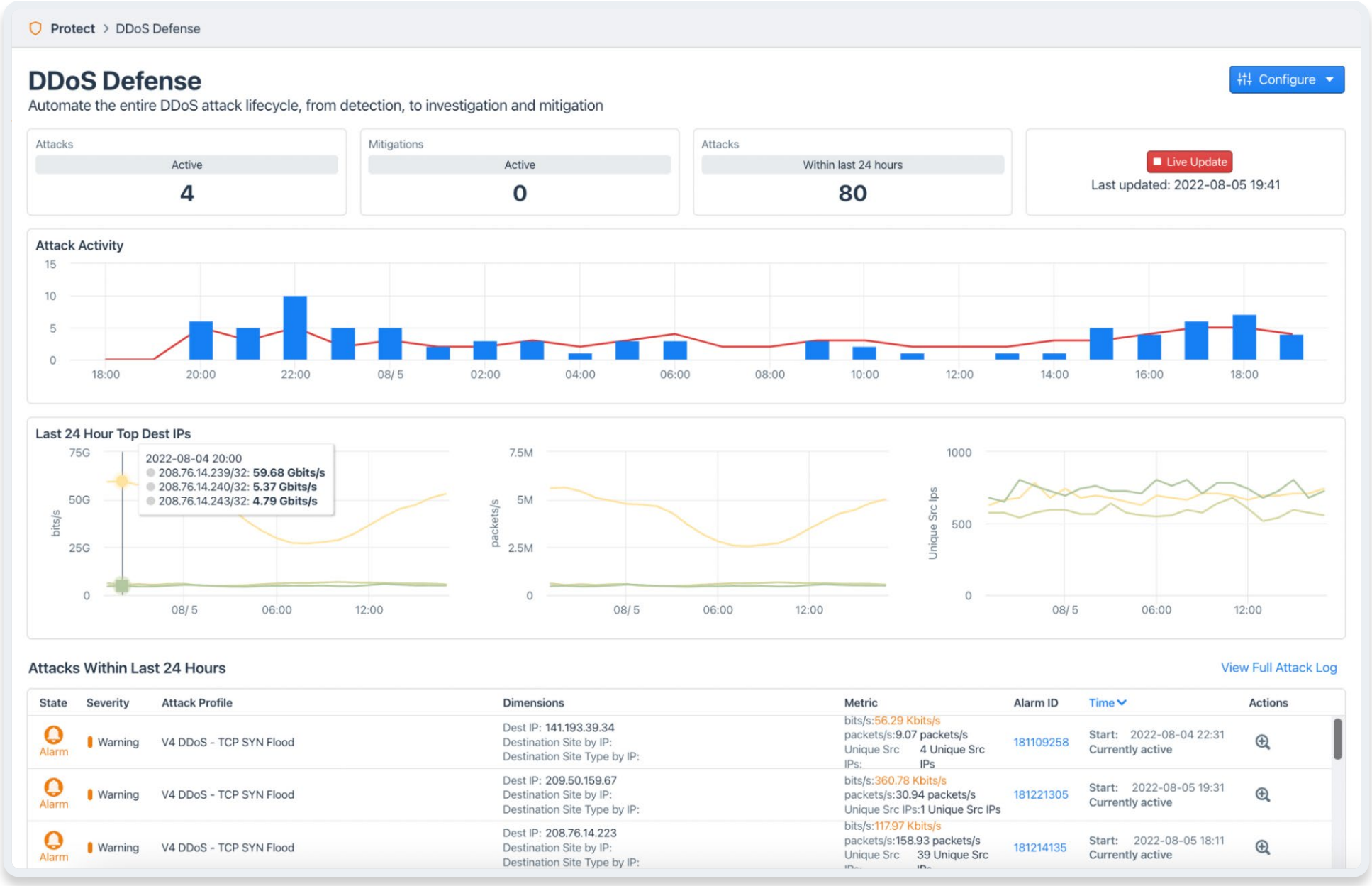
Just getting an alert that traffic patterns have changed is not enough. Kentik Protect allows you to quickly double-click from an alert into an advanced Data Explorer query. These powerful queries allow you to filter down into the details of an attack, and compare this data across time frames. Most legacy application-based DDoS detection systems cannot do this because they only aggregate data.

Kentik Protect helps you find traffic from infected or compromised hosts by enriching flow records with IP reputation data from Spamhaus. The result is two dimensions, Botnet Command, and Control and Threat List Host, which are then used to identify threats to your network, such as botnet command and control servers, malware distribution points, phishing websites, spam sources, and more.

"Kentik is our **global standard** for detecting DDoS attacks. There isn't a single minute in the day that we're not attacked somewhere, so it's crucial for us to have a **reliable service** to detect attacks and trigger mitigation measures."

GoDaddy

Malte von dem Hagen,
Director of the Global Backbone



Understand incident details and causes. Drill down into forensic analytics in real time or retroactively.

Kentik is the network observability company.

Our platform is a must-have for the network front line, whether digital business, corporate IT, or service provider. Network professionals turn to the Kentik Network Observability Cloud to plan, run, and fix any network, relying on our infinite granularity, AI-driven insights, and ridiculously fast search. Visit us at kentik.com and follow us at @kentikinc.

kentik

The world's most valuable enterprises rely on Kentik.

zoom twitch GoDaddy IBM Cloud GitHub Dropbox

Revised 20220909