The Case for Big Data DDoS Protection

Once an occasional annoyance, DDoS attacks have metastasized into an existential threat for every Internet-centric organization. With both revenue and reputation dependent on availability and performance, detection and response must now be a class-one priority for network and security operations. Unfortunately the available options for DDoS protection haven't kept up with the runaway pace of the attacks themselves, which grow not only in frequency and scale but also in the unpredictability of their vectors.

Many DDoS protection systems are stuck in the past, built around scale-up architectures that constrain detection accuracy as well as the speed and agility of response. Technology and business leaders need to reckon with the fact that legacy approaches are ill-suited for today's conditions.

It's time to move beyond first generation answers and embrace cloud-scale, big data-enabled solutions.

DDoS Crosses the Chasm

Not so long ago, the intensity of DDoS attacks was measured in Mbps. It took years to progress to the Gbps range, but the ramp to Tbps-level attacks has been much faster. By now, DDoS has long-since crossed the chasm from the province of outlier misanthropes to the realm of an organized global market, with attacks freely available for purchase by anyone who knows where to look.

The emergence of financial gain as an added motivation for attackers means that DDoS is now:

- **Ubiquitous**: Every online business of any note is continually attacked.
- **Broadly commercialized**: Any gamer, activist, social malcontent, or other "customer" can easily pay a fraction of a bitcoin and launch a multi-Gigabit attack from dozens of easy-to-access commercial DDoS service providers.
- **Widely utilized**: Attacks originate across commercial, hacktivist, and state-sponsored sectors.
- **Open**: Lizardstresser, Mirai, and other tools are regularly being open-sourced.
- **Agile and innovative**: Attacks are evolving rapidly, with a great deal of ingenuity going into creating and deploying new attack vectors. DDoS attacks are increasingly being used as distractions to cover more intrusive exploits.
- **Cloud-scale**: Terabit-plus attacks are the new normal, thanks to billions of poorly secured IoT devices deployed into global consumer and business markets. As a result, attackers can procure — at very low cost — attack-scale that far outstrips the defensive bandwidth of most organizations.

First Gen DDoS Protection is Insufficient

Given the challenges of today's DDoS environment, how do the tools measure up? Frankly, not well: first-generation DDoS protection isn't sufficient to counter today's threat. Architected for the lower attack volumes of yesteryear, first-generation systems commonly share the following key limitations:

- **Inline:** A strategy that's been in use since the start is to steer all network traffic through one or more appliances that scan, detect, and scrub every traffic flow. Inspecting every packet is so costly that only a fraction of organizations that need protection can afford this approach.
- **Scale-up computing:** A more recent approach has been to place detection devices out of band to examine network traffic such as NetFlow, sFlow and IPFIX. This increases the cost-efficiency of mitigation, since traffic associated with attacks is directed to the mitigation devices. But the detection has generally been implemented as Linux-based software running on scale-up computing platforms, where a single, fixed resource controls all processing. Where compute and memory capacity are severely constrained, detection is limited
- **Static, inaccurate detection:** Scale-up processing and memory result in static policy definitions that are either overly broad or require constant and painful manual configuration. The result is inaccuracy: too many false positives and false negatives
- **Slow, reactive, waterfall processes:** DDoS defenses that rely on ongoing manual configuration always fall behind. Personnel are so busy firefighting due to rampant inaccuracies that they can't keep up with normal changes to infrastructure, such as new servers, and policy updates come far too slowly.

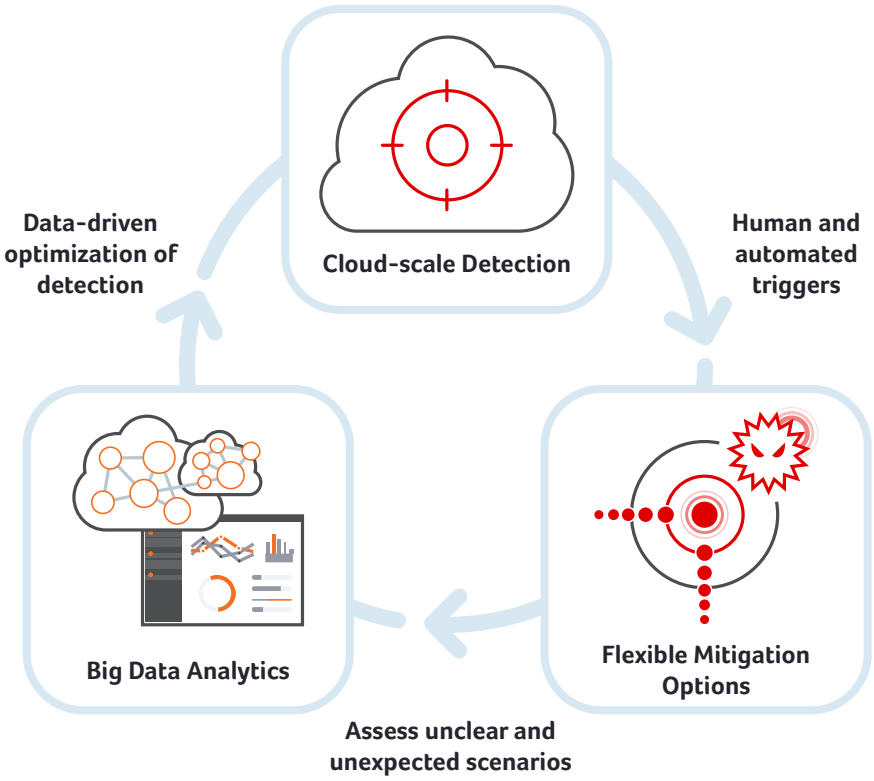
- **Minimal retention and analytics:** When scale-up detection devices meet high-volume traffic, the best you can expect is a few summary reports. There's insufficient memory to retain traffic details and insufficient computing power for deeper investigation. So analytics is barely available from first-generation DDoS protection systems. That reinforces the situational blindness of NetOps and SecOps teams, preventing them from innovating and from adapting defenses to current and emerging conditions.
- **Siloed and shallow:** DDoS detection often depends on network traffic data that's also used by other network monitoring tools in areas such as traffic visibility, performance monitoring, and planning/peering. But the tools themselves remain distinct and siloed, which impedes effective troubleshooting and planning. Sadly, since siloed tools typically share the limitations of scale-up compute and storage, none of them retain detailed history, which leaves forensic insight in short supply.

The Big Data Advantage

Given the inadequacy of traditional tools for DDoS protection, it's little wonder that attacks have become more damaging. To even the playing field, DDoS targets need to rethink their defenses. If attackers can harness distributed computing to amplify their power and scale, so too can defenders, transcending the limits of legacy scale-up designs. The alternative is cloud-scale architecture running real-time big data analytics. The move to a scale-out approach yields not only a significant jump in detection accuracy, but also unified visibility across disparate network realms including visibility, security, and remediation.

Big data systems outperform their legacy ancestors because their underlying architecture removes the compute and storage constraints that have kept older approaches from rising to today's DDoS challenge. The following characteristics are key to this improved effectiveness:

- **Adaptive baselining and anomaly detection:** Big data enables automated tracking of IPs to determine which should be baselined and measured for anomalies. This enables far more accurate detection by making the system responsive to the organic changes in network infrastructure and traffic patterns.
- **Full data retention, deep analytics:** Unlike scale-up systems, big data solutions don't discard network traffic details and keep only summaries. Instead raw data is retained unsummarized, and exploratory analytics enable network and security personnel to keep ahead of the DDoS curve.



- **Hybrid-mitigation ready:** Built for integration via APIs, cloud-scale big data systems are inherently well-suited to hybrid mitigation, which allows a varied, graduated response based on the specifics of a given attack. API-based systems enable interoperability with appliances and cloud mitigation services from multiple vendors, and can also support low-cost mitigation methods such as Remote Triggered Black Hole (RTBH) and Access Control Lists (ACLs).
- **Unified visibility:** Big data provides the opportunity for holistic anomaly detection that addresses not just DDoS but a complete range of issues related to security and general network operations. Big data systems can also unify disparate data sets including traffic flow data (NetFlow, sFlow, IPFIX), network performance monitoring metrics (TCP retransmits and network latency), routing data (BGP path and community attributes), geolocation, and device and interface data (SNMP). Cross-correlation of multiple data types vastly expands analytical scope, which allows engineers to closely examine network conditions and get precise answers to operational questions.

With so many advantages to big data for DDoS protection, large organizations might be tempted to piece together a system based on open source tools or existing big data platforms. But not all big data tools are well suited to the network data use case. Network operations is dynamic and fluid, and answers are needed in real time. It's a daunting challenge to take a technique like MapReduce, which is designed for off-line batch processing, and make it practical for day-to-day network and security operations. Organizations that attempt to construct such systems themselves often fail due to challenging architectural requirements, large capital and operational costs, and a lack of domain expertise.

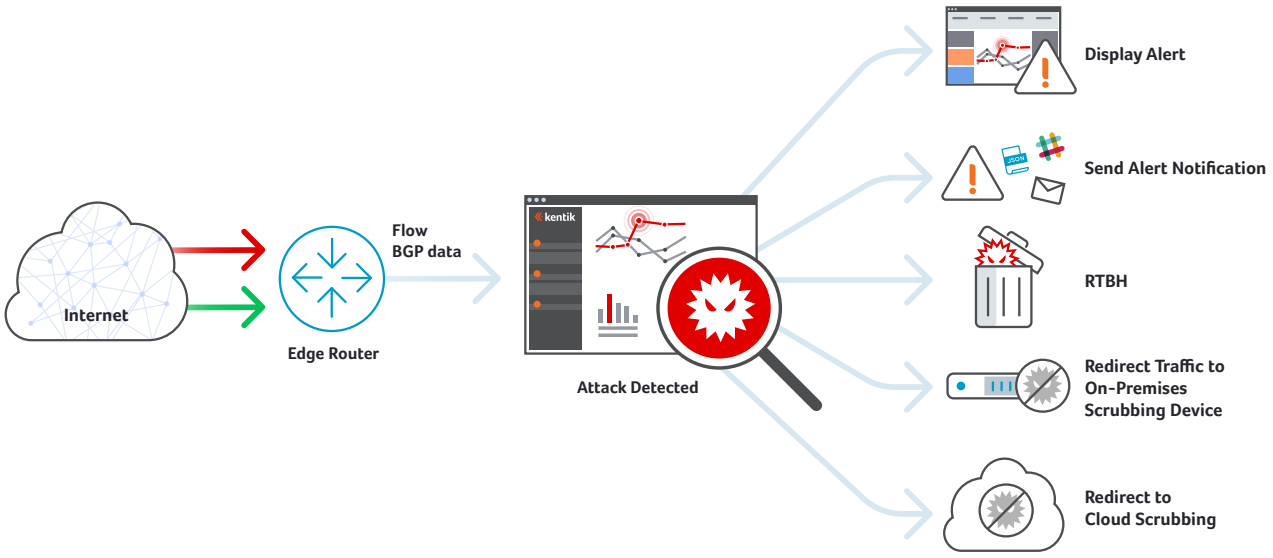
Kentik Detect: Big Data SaaS for DDoS Protection

So far we've learned that the key to effective DDoS protection isn't simply generic big data, but rather a big data-based solution that is tailored to the specific requirements network protection. Based on that realization, Kentik created Kentik Detect: a purpose-built big data platform that addresses multiple realms of network visibility, including DDoS detection. We offer Kentik Detect as a SaaS, as well as for on-premises deployment, so that customers can benefit from advanced DDoS defense without the delays, capital investment, and ongoing costs of building and maintaining their own system.

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

- It ingests and unifies, in real time, massive volumes of NetFlow, sFlow, IPFIX, and BGP data as well as network performance metrics and SNMP device and interface data.
- It applies the scale-out power of the Kentik Data Engine (KDE) to network-wide scanning of billions of rows of data using multi-dimensional criteria and adaptive baselining.
- It automates hybrid mitigation via standards-based remote-triggered black hole (RTBH) and integration with mitigation solutions from leading vendors.
- It enhances the ability to investigate and understand attacks by including deep ad-hoc traffic analysis, flexible dashboarding, peering analytics, and network performance monitoring.

Kentik Detect is the choice of leading digital and online businesses such as Yelp, Box, Pandora, and Neustar. Deployed as SaaS, with exceptionally low total cost of ownership (TCO), Kentik Detect can be put into production within minutes of sign-on. Ready to see the power of big data DDoS protection? Sign up for a free trial, or contact info@kentik.com to schedule a demonstration.



Get in touch with our expert team!

Contact us at sales@kentik.com to request a demo
Or visit www.kentik.com to sign up for a free trial