CRYPTOTECH
SECURING YOUR SUCCESS

CryptoTech DDoS Threat Intelligence

Report for Libya

June 2023 - June 2024

Issued in Partnership with

NETSCOUT
GUARDIANS OF THE CONNECTED WORLD

CONTACT INFORMATION:
info@cryptotech.ly
+218 91 051 9985
Gergaresh,
Tripoli - Libya
www.cryptotech.ly

CRYPTOTECH
SECURING YOUR SUCCESS

CryptoTech DDoS Threat Intelligence

Report for Libya

CRYPTOTECH
SECURING YOUR SUCCESS

CryptoTech DDoS Threat Intelligence

Report for Libya

Overview of the report

In collaboration with NetScout, CryptoTech is pleased to present a comprehensive official report on the DDos cybersecurity threats affecting Libya in the past year. By leveraging the expertise and data of both CryptoTech and Netscout, this report aims to provide actionable intelligence and strategic recommendations to fortify digital defenses against evolving cyber threats.

Global DDoS Threat Landscape

DDoS Attack Proliferation

The threat of Distributed Denial-of-Service (DDoS) attacks remains a significant concern globally, with Netscout observing over 13 million DDoS attacks in 2023 alone. These attacks disrupt services, compromise critical infrastructure, and result in substantial financial and reputational damage. Key findings highlight a notable increase in politically motivated DDoS hacktivism, with groups such as NoName057(16) and Anonymous Sudan leading the charge.

Attack Sophistication and Targets

DDoS attacks have grown more sophisticated, targeting crucial internet infrastructure components like authoritative and recursive Domain Name System (DNS) servers. These servers are integral to the functioning of the internet, and their disruption can have widespread repercussions. In the latter half of 2023, public DNS resolvers faced approximately 50,000 DDoS attacks, emphasizing the need for robust protection mechanisms.

Defense Strategies

Effective defense against DDoS attacks involves a multi-faceted approach: eliminating harmful traffic early, increasing network capacity, and making targets less accessible to potential attackers. The goal is to transition from reactive to predictive defense strategies, utilizing advanced threat intelligence to preemptively counteract potential attacks.

Insights for Libya

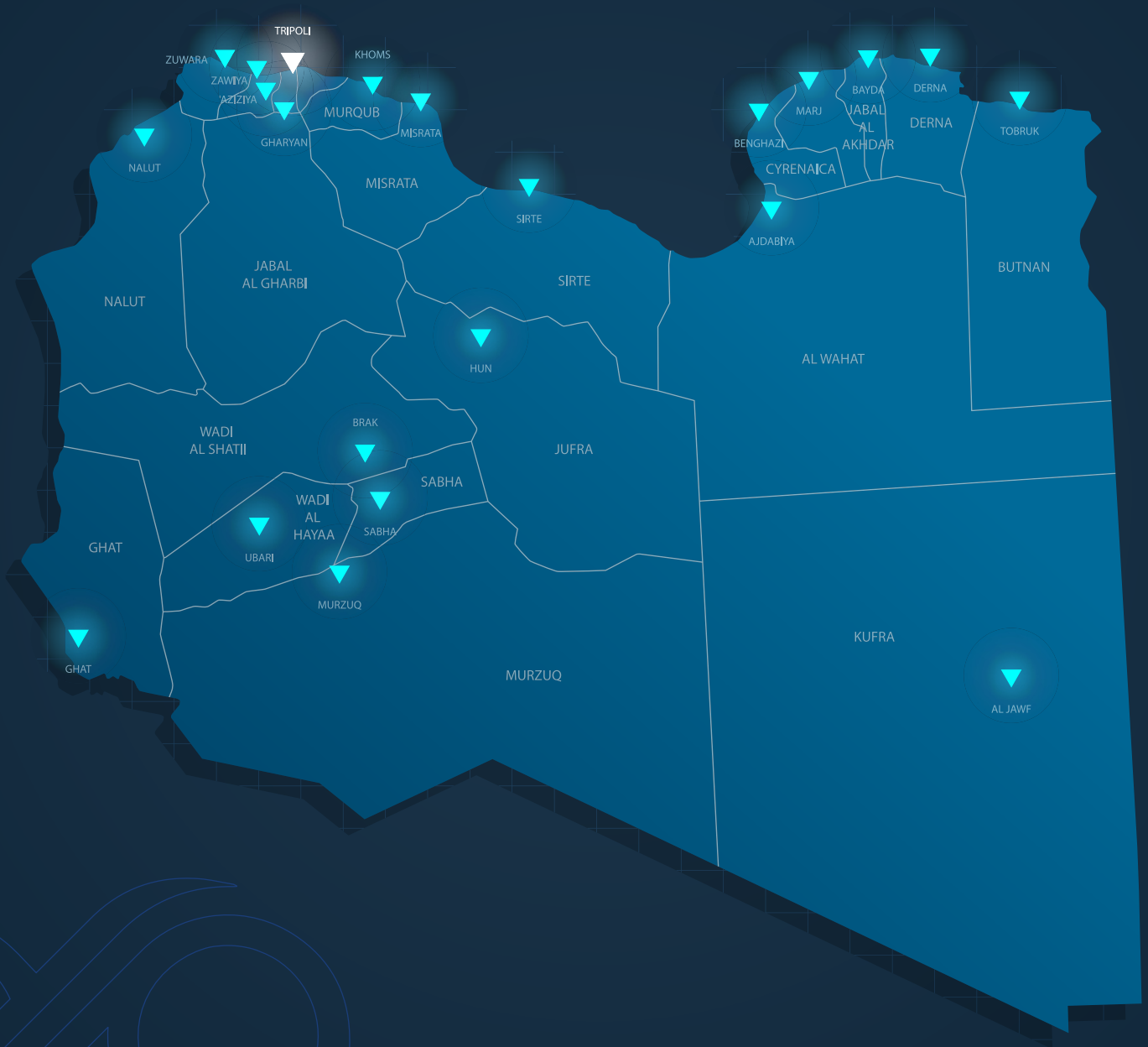
Regional Implications

Libya, like many countries, is not immune to the surge in DDoS attacks. The geopolitical instability in the region exacerbates the threat, as hacktivist groups leverage political motivations to launch attacks that transcend borders. The impact on Libyan infrastructure, businesses, and government services can be profound, disrupting essential services and undermining trust in digital systems.

Strategic Recommendations

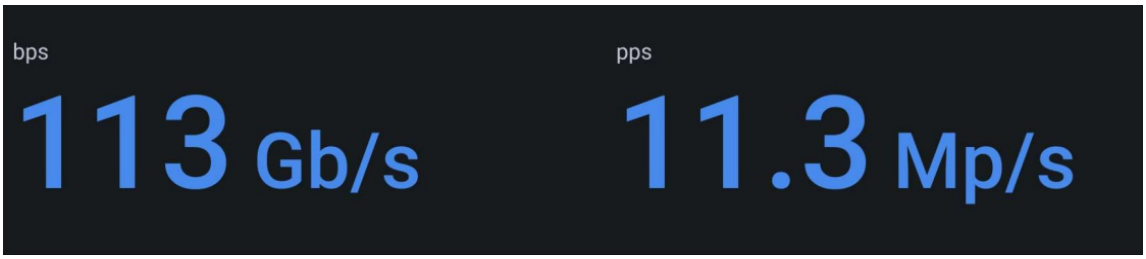
For Libya, the path forward involves adopting advanced DDoS protection technologies and methodologies. This includes investing in predictive threat intelligence to anticipate and mitigate attacks before they cause significant damage. Additionally, reinforcing the security of DNS servers and other critical infrastructure can help reduce the risk of widespread service disruptions.

This report by CryptoTech, in partnership with NetScout, aims to arm stakeholders in Libya with the knowledge and tools necessary to combat the ever-evolving cyber threats. By understanding the global DDoS threat landscape and implementing tailored defense strategies, Libya can enhance its cybersecurity posture and safeguard its digital future.


TRIPOLI
ZUWARA
ZAWIYA
'AZIZIYA
KHOMS
MURQUB
MISRATA
GHARYAN
NALUT
MISRATA
SIRTE
JABAL
AL GHARBI
NALUT
SIRTE
HUN
WADI
AL SHATII
BRAK
JUFRA
SABHA
WADI
AL
HAYAA
SABHA
UBARI
GHAT
MURZUQ
GHAT
MURZUQ
BENGHAZI
MARJ
BAYDA
JABAL
AL
AKHDAR
DERNA
DERNA
TOBRUK
CYRENAICA
AJDABIYA
BUTNAN
AL WAHAT
KUFRA
AL JAWF

The biggest attack over the last 12 months

Maximum malicious traffic towards a UNIQUE target in Libya



One target

A single IP

A single Server

A single Network element

A single service (Web site, DNS resolver….)

Gb/s

Threat volume in Gigabits per second towards a unique IP

Mp/s

Million packets per second towards a unique Target

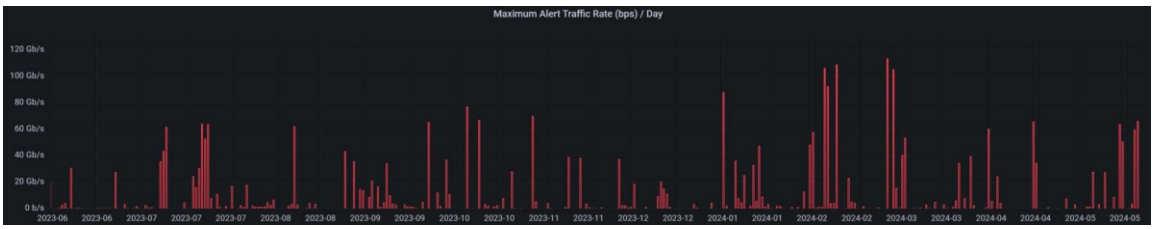
Impact

Amount of traffic (Gb/s) will saturate the victim connectivity (Fiber, Data Center Uplink, Internet Access…)

Amount of packets will saturate The victim devices (routers, servers, Firewalls…)

Biggest threats towards Libya

Each bar represents the maximum bad traffic



Towards a unique IP

Regularly, overs 100Gb/s threats targeting assets in Libya

High volumes

No month under 20Gb/s

Almost an over 60Gb/s threat every month

Over 100Gb/s in January and February 2024

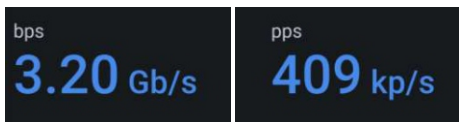
Acceleration in Q1

February and March were the most impacted months with 4 attacks over 100Gb/s

60Gb/s is the norm

The trend is showing an acceleration in big attacks

Total attacks towards Libya



3183 Major threats

Major attacks are those with actual impact on target (unique IP) assets and services

556 attempts

Attackers are no more in scan, discovery or test phase, they launch directly impacting attacks

3.2Gb/s

Average attack volume over the 3800 attacks (all types)

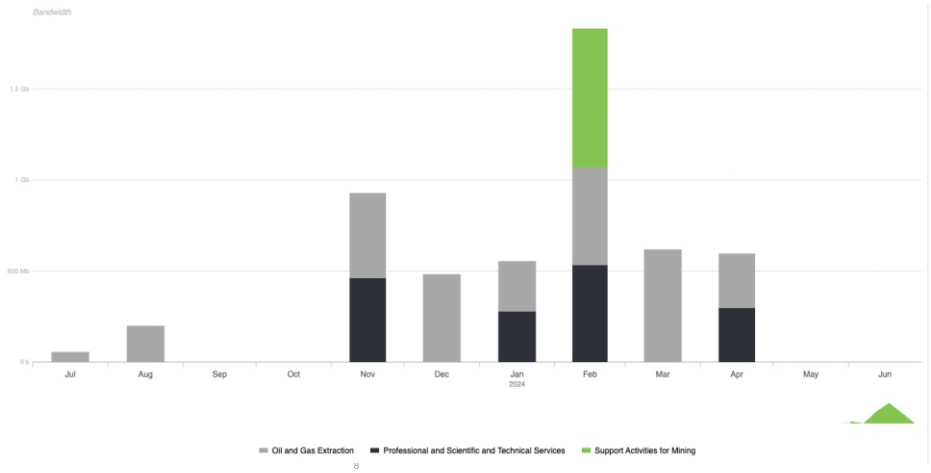
Still enough to saturate target uplink (fiber line under 3Gb/s)

409 Kp/s

Can bring down most of servers and enterprise Firewalls

Focus on Oil and Gas for published services

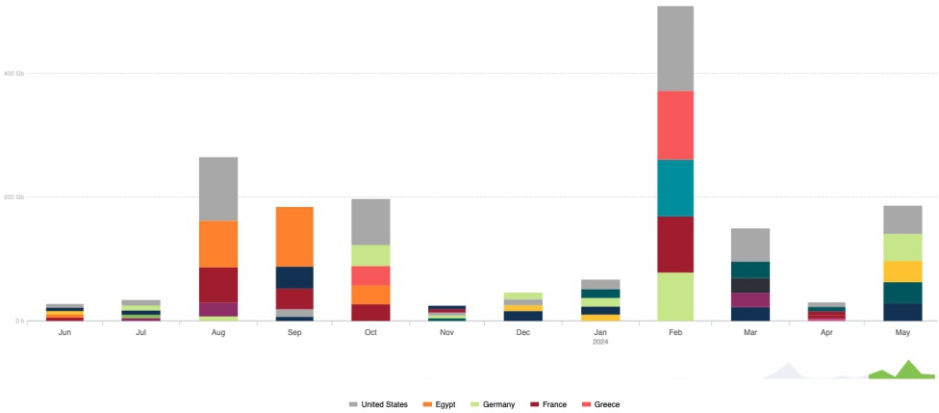
Only for Ips known as Oil and Gas (web sites and published services) Threats targeting hidden Ips and assets like Datacenters, headquarters and other facilities are under service provider categories



8

Top countries from where cyber threats are coming

- The graph is showing the TOP origin countries, the rest of threats is coming from other countries.
- USA, Egypt and Germany are the most represented.



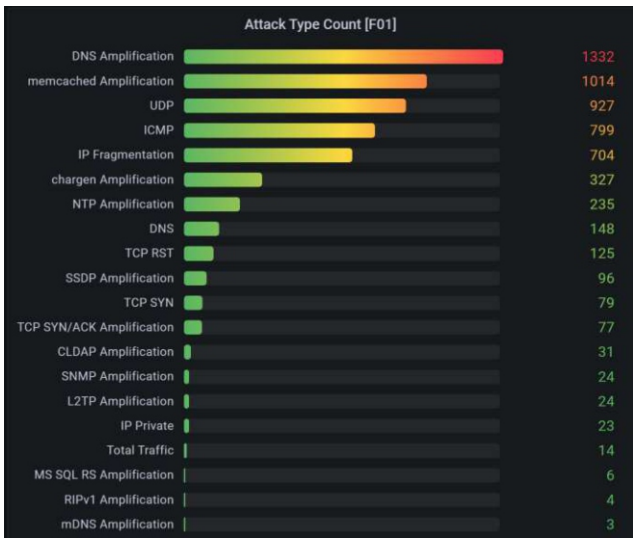
9

Outgoing threats and infected devices in Libya

- More than 150Tb of cumulated bad traffic every month coming from Libyan infected hosts
- This shows the presence of Botnets, Malware, Ransomware and Data Exfiltration.

10

Type of threats



DNS Vector

DNS is the most used attack vector

Bringing down the DNS of a target will lead to bring down the published services (website, web application, browsing…)

TCP Vectors

TCP RST, TCP SYN and TCP SYN/ACK are targeting Firewalls, WAFs and other security devices and will lead to get the target out of the network or vulnerable without any protection

Attack duration towards Libya (average and Max)

10 Days

The longest attacks lasted for 10 days

It was a critical attack

2H for Low

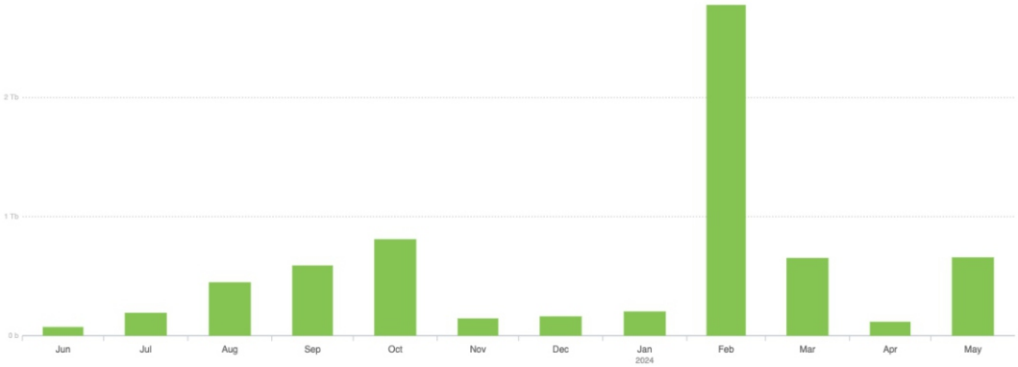
Reconnaissance did not last for more than 2 hours the last 12 months

Average values

Average duration for critical threats is 1h03 during the last 12 months

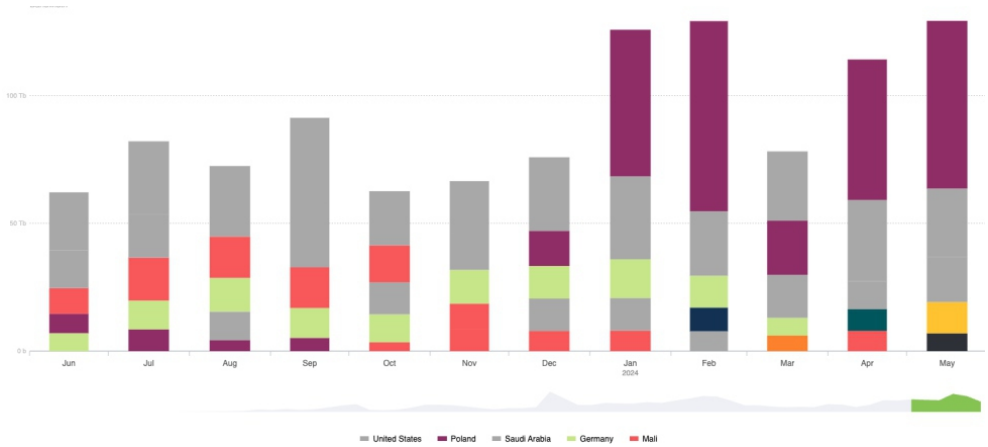
Total amount of bad traffic targeting Libya

2.78 Tb/s as total of threats towards Libya in February 2024



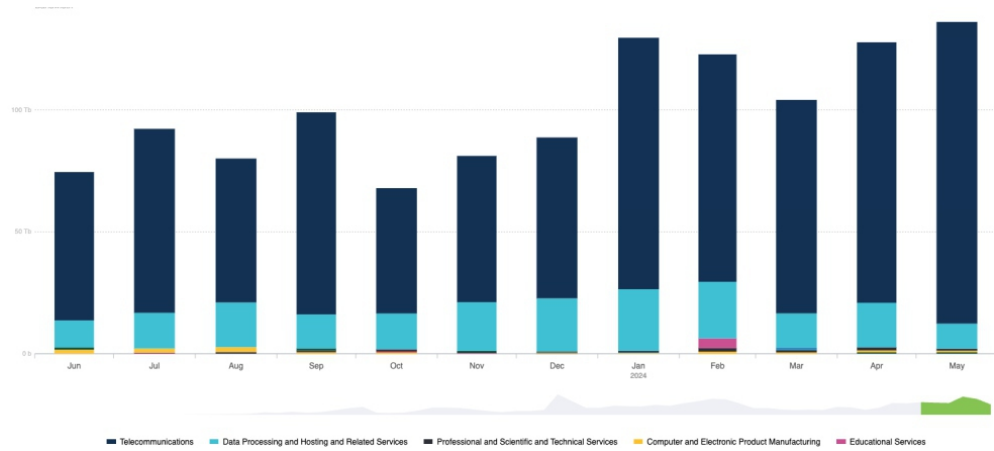
Who is being targeted by Libyan botnets

- Here are the top targeted countries, USA and KSA are in Grey and are the most targeted
- Poland threats linked to the war in Ukraine



What are the targeted organizations

- Telecommunications covers all type of Internet access including Headquarters
- Data processing includes software as a service, Cloud and published services.



How We Can Help

1. Stay Updated with New Threats and Attack Types

Partnering with CryptoTech ensures that companies, especially large enterprises, have access to a consistent and up-to-date source of threat intelligence. Staying informed about the latest threats and attack methodologies is crucial for maintaining robust cybersecurity defenses.

2. Enhanced Visibility and Threat Detection

Internal asset management is essential to prevent the spread of threats across the network. Our "visibility without borders" approach enables comprehensive monitoring and detection of malware, ransomware, and advanced threats, ensuring that no malicious activity goes unnoticed.

3. Coordination with Service Providers

Effective coordination with service providers is key to mitigating the impact of DDoS threats, especially in strategic locations. NetScout' technology is designed to automate the collaboration between customer devices and the service provider' core network protection, intelligence in collaboration with CryptoTech team this will help to prevent saturation and direct impacts from DDoS attacks.

4. Network and Application Performance Monitoring

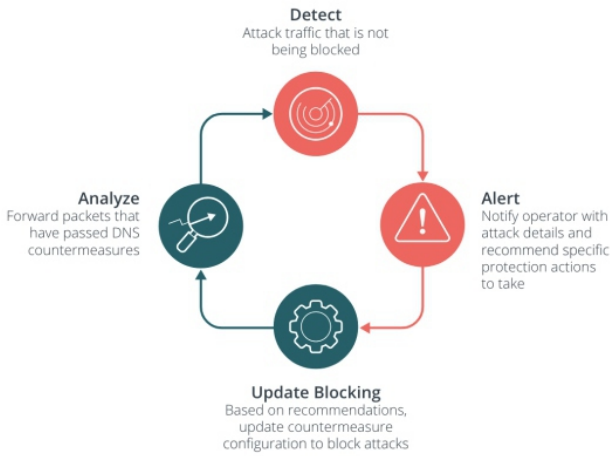
Monitoring network performance and application health is crucial for identifying user experience issues and detecting abnormal activities that may indicate a security compromise. We offer technologies that leverages machine learning and artificial intelligence to provide automated monitoring and threat detection, enabling experts to maintain the health of their assets and effectively block cyber threats.

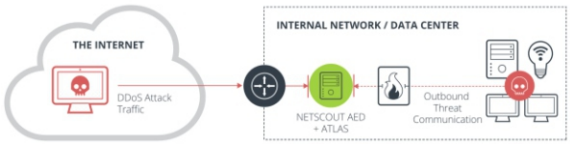
By implementing these strategies, We help organizations strengthen their cybersecurity posture and protect their critical infrastructure from evolving threats.

NETSCOUT AED and AEM with Adaptive DDoS Protection

Solution that Adapts to Dynamically Changing DDoS Attacks To Provide Effective First and Last Line of Automated Perimeter Defense

AED unique location on network edge + stateless packet processing engine + ATLAS Global
Threat Intelligence = First and Last Line of Defense from advanced cyber threats.

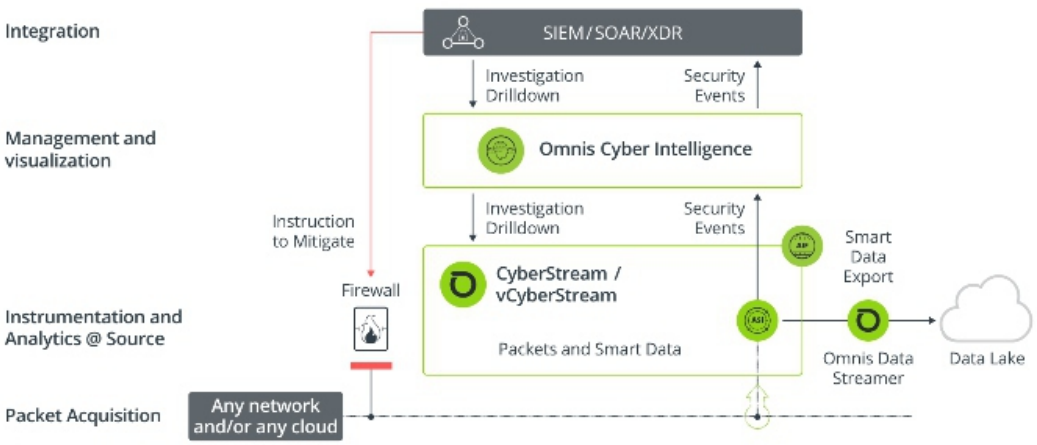




Omnis Cyber Intelligence Advanced, DPI-Based Network Detection and Response

Comprehensive Visibility Without Borders, Proactive Hunting
Leverage local, long-term,

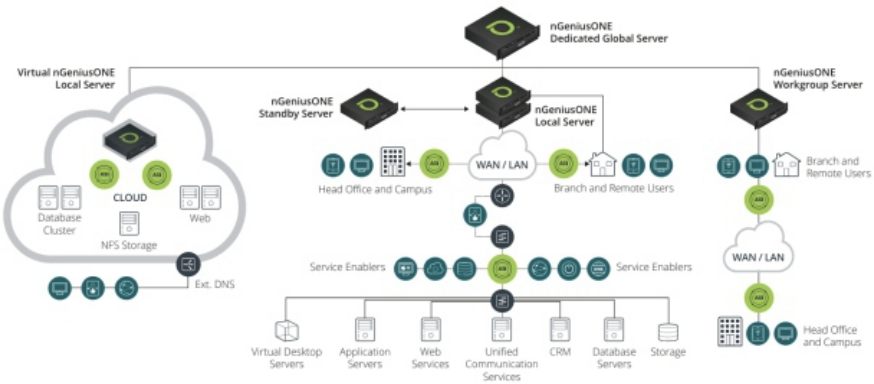
storage of historical metadata to conduct unguided hunting looking for evidence of compromise, network, or data breach.



Performance Management with nGeniusONE

The nGeniusONE® Service Assurance solution provides real-time visibility into the performance of business critical applications

nGeniusONE with NETSCOUT' patented Adaptive Service Intelligence® (ASI) technology leverages to generate "mart data"for smarter analytics to assure performance, manage risk, and facilitate superior decision making regarding application and network services.



User Experience Monitoring with nGenius PULSE

Visibility to the Business Edge to Ensure Availability and Performance From Anywhere.

nGeniusPULSE monitors availability and performance of an organization' revenue-generating applications and services. It also offers Path Analysis with hop-by-hop views of the network path from remote sites to the service being used