NETSCOUT Omnis Security

A Platform for Advanced Threat Analytics and Response

A Platform for Advanced Threat Analytics and Response

Here are some facts. Modern-day enterprise networks are complex as they routinely encompass internal, branch office, virtual, and public cloud environments. The threat surface is expanding, and the number of cyber-attacks is increasing. The number of security tools has increased, giving rise to siloed data. And lastly, the lack of comprehensive and consistent network visibility makes it harder for cybersecurity teams to conduct expedient and effective threat detection and response. To overcome this challenge, organizations must collect and analyze data across as many capture points as possible (e.g., logs, packets, Netflow, and endpoints), computing platforms (e.g., physical, virtual, and cloud) and enrich this data with threat intelligence and business context. NETSCOUT's solution to this challenge is Omnis™ Security - A platform for advanced threat analytics and response.

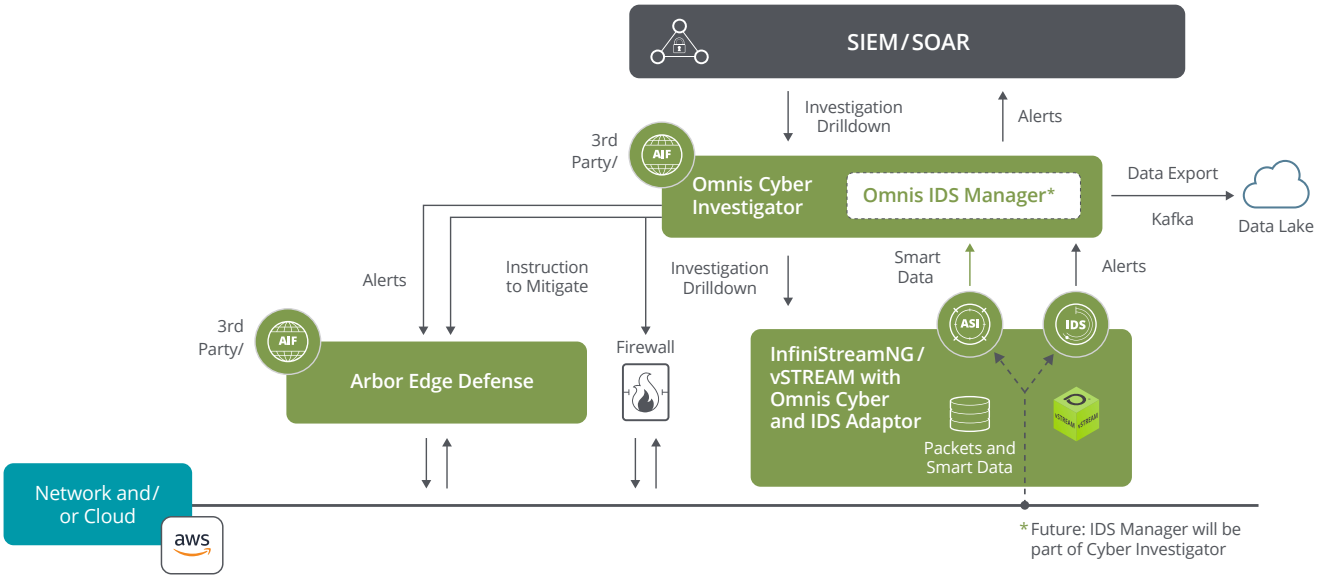
Effective Cybersecurity Starts with Comprehensive and Consistent Network Visibility

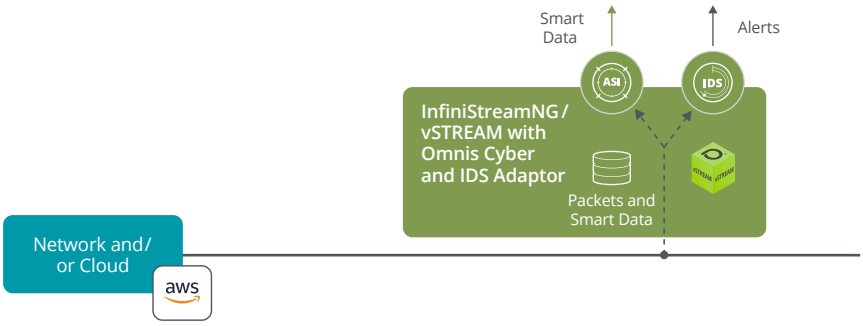
You can't protect yourself from what you can't see. It's a fundamental axiom for cybersecurity. And in today's complex world of legacy networks, branch offices, work-from-home, public and private clouds, gaining the proper level of network visibility has never been so challenging to obtain and so vital for cyber threat protection.

For over 30 years, NETSCOUT has provided organizations with comprehensive and consistent network and application layer visibility across their entire digital infrastructure – no matter where that infrastructure may reside (e.g., legacy, virtual or hybrid-cloud). At NETSCOUT, we call this Visibility without Borders. And we believe this same level of visibility is a foundational requirement for effective threat detection and response - or Security Without Borders

FEATURES AND BENEFITS

- Highly scalable network instrumentation for cost effective, comprehensive network visibility.
- Multiple methods of network-based threat detection using, curated threat intelligence, behavioral analysis, open source, and advanced analytics.
- Contextual investigation via a rich set of locally stored metadata and packets.
- Remediation at the perimeter using industry leading stateless packet processing technology or 3rd party blocking devices (e.g., firewalls)
- A common source of rich metadat and packets, use open standards, and APIs that enable integration and TechOps collaboration.





Underpinning NETSCOUT Omnis Security is the InfinistreatmNG® (ISNG) platform. ISNG is a proven, pantented, highly scalable packet acquisition, classification, and storage solution for providing comprehensive and consistent visibility into any physical, virtual, or cloud environment.

ISNG supports a variety of different platforms, interfaces, and local storage capacities.

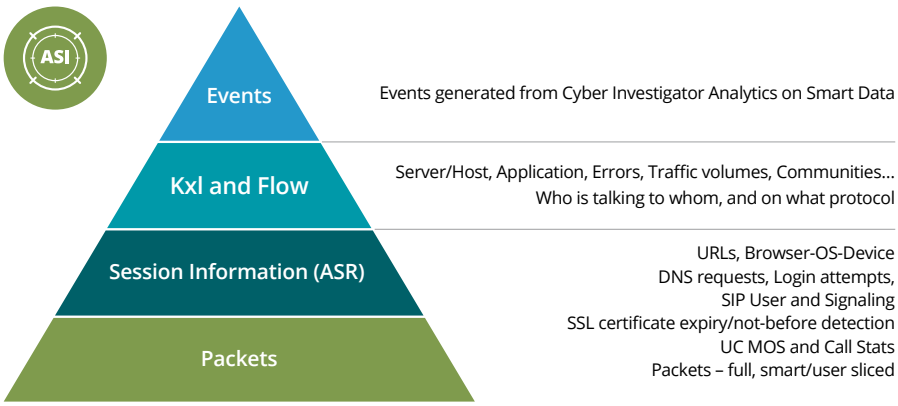
- Platforms include a turnkey appliance, a software-only solution using a certified or qualified COTS hardware or 100% virtual option (called vSTREAM®) that supports cloud or virtual environments such as Amazon Web Services, Google Cloud, Microsoft Azure, Oracle Cloud Infrastructure and VMware NSX-V and NSX-T.
- Full line-rate capture and network interface options up to 100Gbps.
- Local disk storage with capacity up to hundreds of terabytes for local storage of metadata and packets.

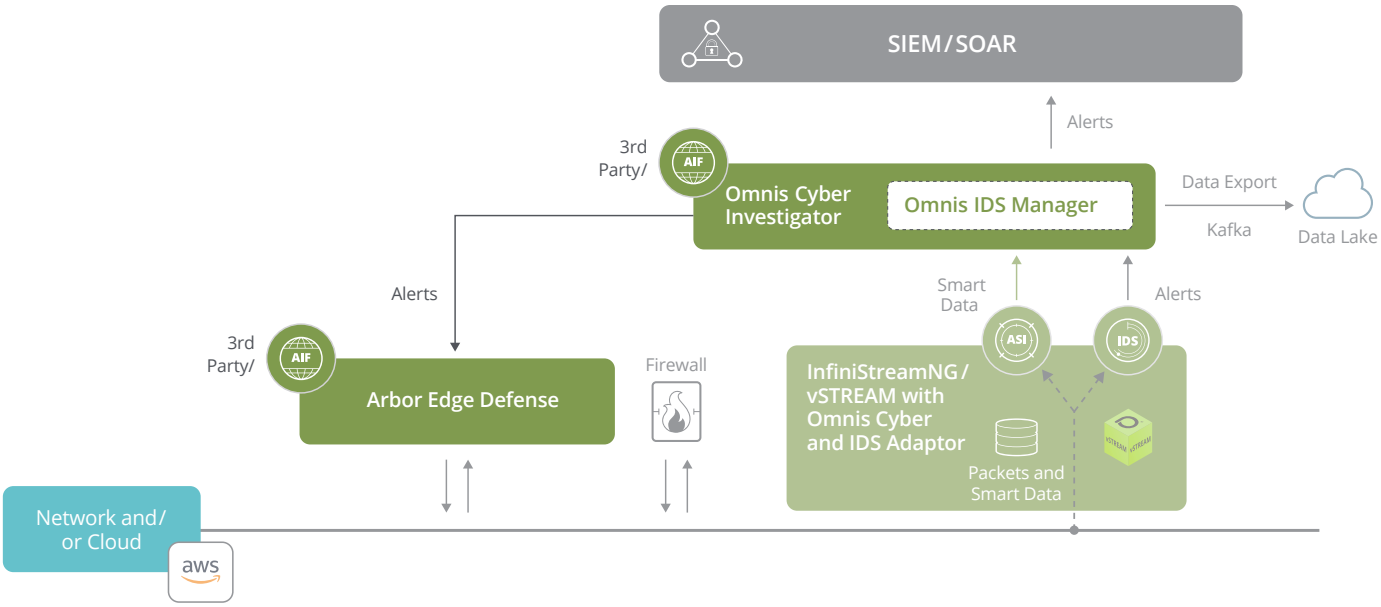
Using patented Adaptive Service Intelligence (ASI) technology, ISNG instrumentation converts raw network packets into indexed metadata - we call this NETSCOUT "Smart Data". NETSCOUT Smart Data contains information such as:

- 5-tuple attributes (source and destination IP, source and destination port and the protocol field).
- Key performance indicators (KPIs) such as error codes, response times, or mean opinion scores (MOS.
- Data from SIP user and signaling planes.
- DNS request/responses, URI, browser and device types
- And more.

In addition to this enhanced metadata, the ISNG platform also stores condensed, raw packets.

ISNG and ASI created Smart Data provide comprehensive North-South, East-West visibility across an organization's entire digital infrastructure. And this single source of robust metadata can be readily available for NetOps and SecOps use cases.





Multiple Methods of Network-based Threat Detection

Leveraging NETSCOUT ISNG instrumentation and ASI-derived, smart metadata and packets, Omnis Security provides multiple methods of cyber threat detection.

Omnis Cyber Investigator – Serving as a centralized console for the Omnis Security platform, Cyber Investigator analyzes Smart Data collected by ISNG instrumentation, network baselines, and ATLAS or 3rd party threat intelligence to detect all types of cyber threats and enable workflows for further visualization and investigation. Cyber Investigator alerts can be sent to 3rd party SIEMs, and its data can be exported to 3rd party data lakes for further analysis by 3rd party applications.

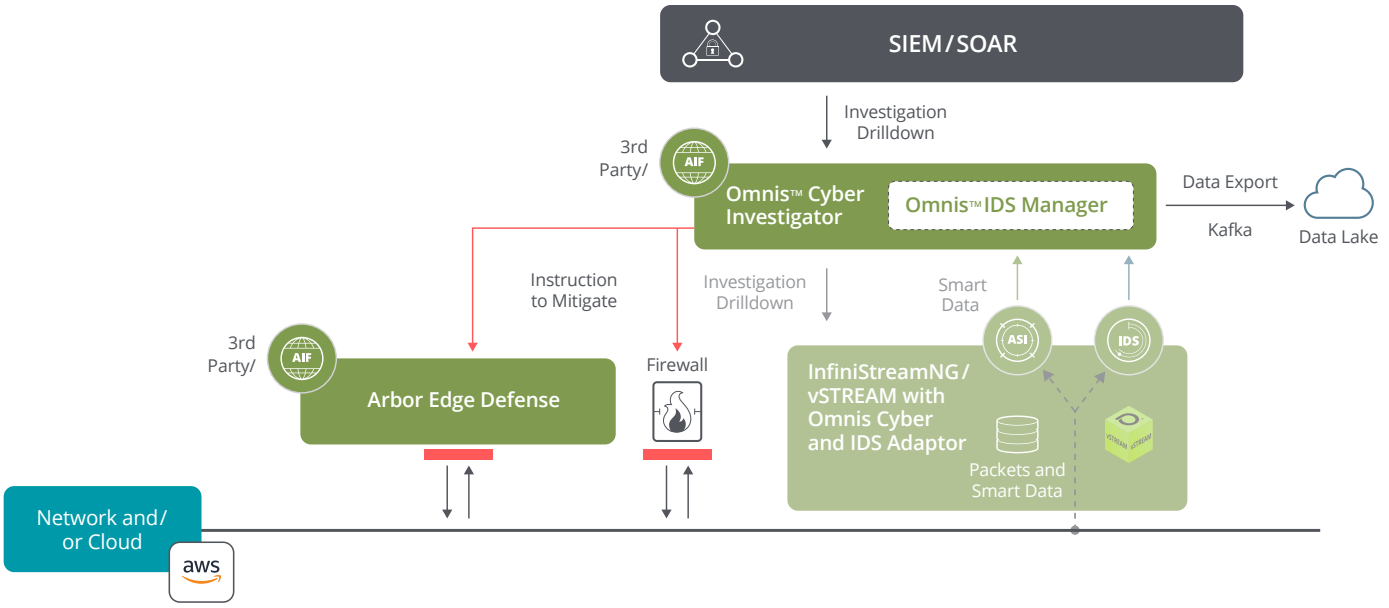
Omnis Intrusion Detection System (IDS) – A standalone solution or software module for ISNG instrumentation, Omnis IDS provides intrusion detection using the Suricata open-source signature and rules engine. Omnis IDS sends contextually rich alerts, including mapping to Mitre Att&ck (in the future), to the IDS Manager application running in Cyber Investigator console or a SIEM/SOAR.

Arbor Edge Defense – Deployed on the network perimeter, inside the router and outside the firewall, Arbor Edge Defense detects inbound and outbound (e.g. north-south) threats such as DDoS attacks, scanning, brute force password attempts, malware and other IoCs using highly scalable, stateless packet processing technology and threat intelligence from NETSCOUT ATLAS and/or 3rd parties. Upon detection alerts can be sent to Cyber Investigator console or 3rd party SIEM/SOAR systems.

Together all three components provide multiple methds of network-based threat detection, and integrate into an existing secuty stack contributing to an organization's defense in depth strategy.

Contextual Threat Investigation and Remediation at Perimeter

Simply "detecting" cyber threats is not enough. Providing security analysts the ability to conduct quick, highly contextual investigations that influences remediation is the next crucial step in cyber threat protection. Omnis Security offers two powerful methods of threat response.



Contextual Investigation - Using the rich source of NETSCOUT Smart Data, Omnis Cyber Investigator not only detects threats but with a single click of a button also enables security teams to mine a rich source of metadata and full packets for fast, highly contextual investigations. The results of Cyber Investigator investigations can influence alert priority or remediation efforts which could include device cleanup or removal, network segmentation or confidence to execute blocking using the network infrastructure or other security devices at the perimeter.

Perimeter Protection – Network-based threat prevention at the network perimeter is one means stop known or unknown cyber threats. However, blocking of any sort must be be done with complete confidence to avoid false positives. Cyber Investogator's access to rich metadata and packets help security teams gain the confidence to block at the network perimeter. Omnis Cyber Investigator can instruct devices like firewalls or NETSCOUT Arbor Edge Defense (AED) to block malicious traffic at the perimeter. Arbor Edge Defense can also automatically detect and block inbound and outbound threats. In particular, AED offers, proven, industry leading DDoS attack protection. It excels at stopping all types of DDoS attacks and due to its stateless packet processing technology, AED can stop state-exhaustion attacks that threaten the availability and performance of stateful devices like firewalls, VPN concentrators and load balancers. Armed with threat intelligence from NETSCOUT ATLAS or 3rd parties, AED can also be configured to stop outbound traffic from compromised internal hosts communicating with external known bad sites – essentially acting as a first and last line of perimeter defense.

Integration is Vital

By itself, NETSCOUT Omnis Security is an effective Advanced Threats Analytics and Response platform. Its focus and strength lie in utilizing network-derived packets and robust source of metadata from the NETSCOUT ISNG/vSTREAM platforms. At NETSCOUT, we believe that the network contains the ultimate source of truth. But we also know that organizations also rely on endpoint detection and SIEM technologies. That is why Omnis Security has made it a priority to be as open as possible and integrate into existing security stacks and processes whenever it can. Examples of Omnis Security integration include:

- Support for all types and speeds of networks.
- The ability to capture, decode and create robust metadata for thousand of network protocols and applications.
- Support any network environment, including virtual (e.g., Oracle Cloud Infrastructure, VMware NSX-V and NSX-T) or public cloud (e.g., Amazon Web Services, Google Cloud, Microsoft Azure),

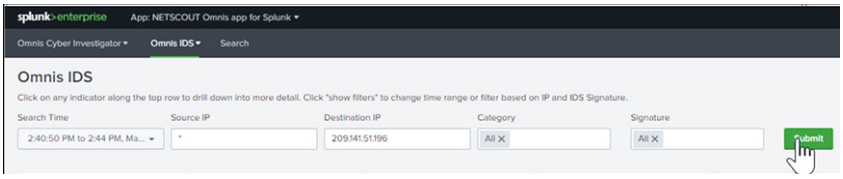
- Use of 3rd party threat intelligence via support for STIX & TAXII or custom interfaces with TIPs (e.g., Anomali or ThreatQuotient).
- Alerts that support common SYSLOG formats.
- Use of open REST APIs.
- Use of open-source threat detection (e.g., such as Suricata) and emerging industry frameworks (e.g., Mitre Att&ck)
- Apps in popular SIEMs (e.g., Splunk, AWS Security Hub)
- Integration with firewalls (e.g., PaloAlto Networks).

All of this enables all or parts of Omnis Security to become a fully integrated and vital part of an organization's cybersecurity infrastructure.

Omnis in Action

Now let's demonstrate how the Omnis Security platform can be used in a real-world scenario. You're a tier 2 security analyst, and you've just been given the task to investigate a suspicious IP address (**209.141.51.196**)

Starting from the Omnis IDS application running in a Splunk SIEM, let's search for what we know about **209.141.51.196**.

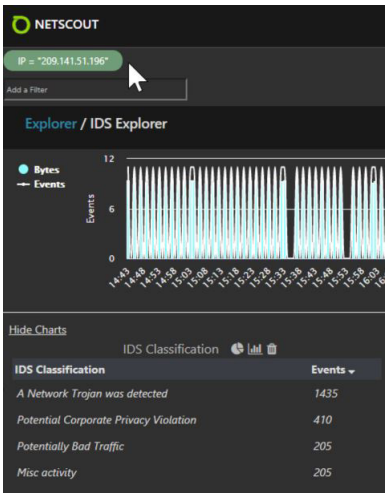


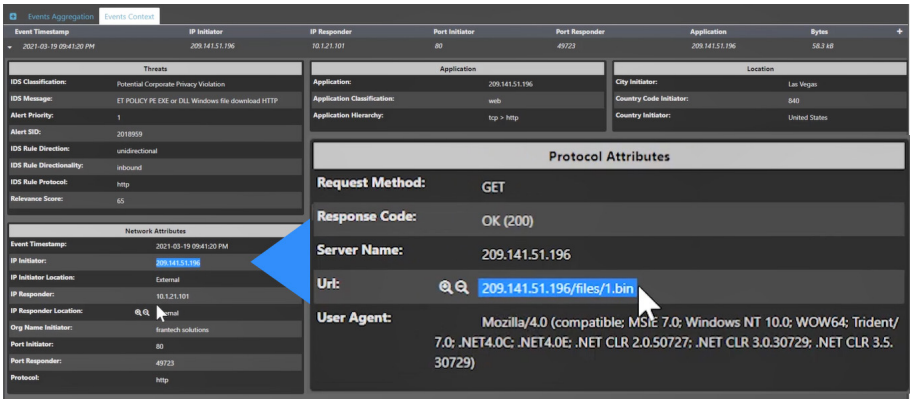
We have a hit. Now a simple click allows us to drill into what Omnis IDS knows about this IP address.

Omnis IDS has identified and classified many events associated with this host including a network trojan, potential corporate privacy violations and more.

If we drill in further we can see more details and context related to the alert such the malicious URL and file that was downloaded onto our internal host.

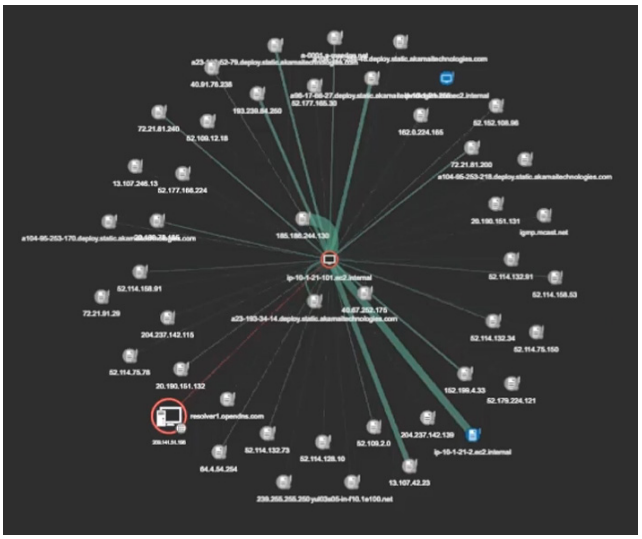
(209.141.51.196/files/1.bin)



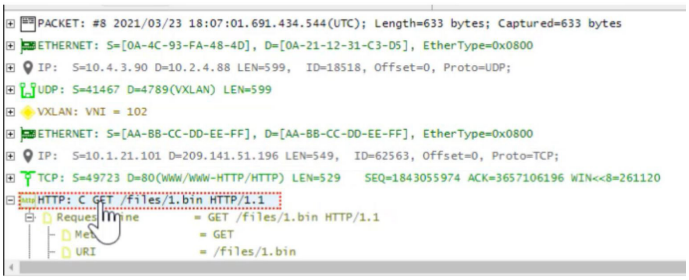


Now let's conduct a further investigation using Omnis Cyber Investigator. From a Cyber Investigator application running in the same Splunk SIEM or from the Cyber Investigator console itself, we can easily filter on the suspicious IP address of 209.141.51.196 and time frame. Instantly you are presented with a host investigation view showing the external address communicating with one of our internal hosts located in our AWS EC2 instance.

With a click of a button, we can quickly see a more holistic view of our suspicious IP address and who it is communuicated with. This view is leveraging the robust source of metadata in the ISNG instrumentation providing telemetry across the entire network.

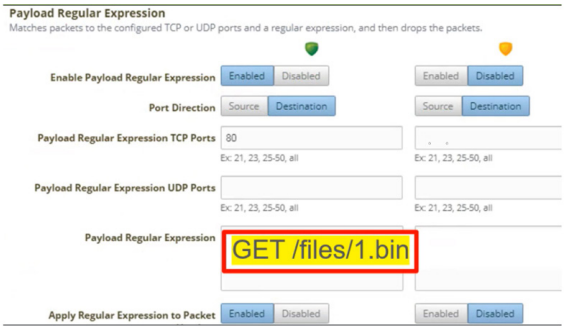


Another click, brings you down to a packet level exposing the malicious URL and file.

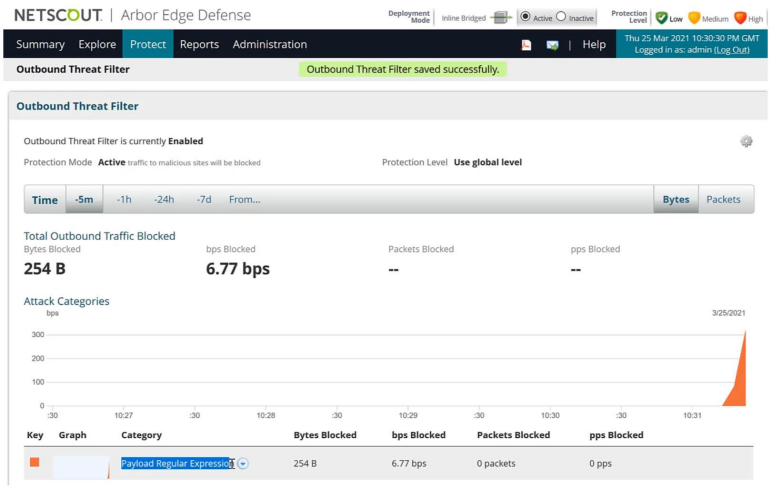


From here you can gather a PCAP file containing all the full packets associated with this event, and hand it off to your forensics lab or Tier -2 security analysts for further analysis.

Based upon our thorough investigation, we are convinced that our network has been breached and now we need to block all communication to/from this malicious IP address to stop lateral movement or a data breach from occurring. Blocking at the network perimeter is one option. With a click of a button Cyber Investigator can create a block command for example, to PaloAlto firewall. Another more intelligent option is to configure our Arbor Edge Defense device, which sits in front of the firewall. This mitigation effort will not only accomplish the blocking of communication to/from the malicious URL, but this will also take the load off the firewall allowing it to focus on other tasks. Below is the AED screen shot where it is configured to block the outbound traffic from any internal device that tries to execute the offending **GET/ files/1.bin** command.



Here we can see AED actively blocking the traffic at the perimeter of the network.



To recap. This demonstrated the Omnis IDS detection of a threat, Omnis Cyber Investigator's robust contextual investigation of metadata and ultimately exposure of the offending packets, and automated blocking of the threat at the network perimeter with Arbor Edge Defense.

Conclusion

NETSCOUT Omnis Security is an Advanced Threat Analytics and Response platform that allows organizations to:

- Leverage highly scalable network instrumentation for cost effective, packet derived, comprehensive network visibility into their entire digital infrastructure. We call this Security Without Borders.
- Leverage multiple methods of threat detection, advanced analytics and highly curated threat intelligence to automatically detect threats at scale.
- Quickly conduct contextual investigation of security threats utilizing an intuitive user interface and access to locally stored, rich metadata and/or packets.
- Go beyond just threat detection and gain the confidence to actively block threats at the network perimeter using industry AED's leading stateless packet processing technology or integration with 3rd party perimeter devices like firewalls.
- Enable TechOps collaboration by leverage a common and consistent platform that can be used across multiple cloud and legacy network environments for both cyber security and service assurance use cases.
- Use open standards to easily integrate into existing security stack and processes.

Bottom line is NETSCOUT Omnis Security offers the Scale, Scope and Consistency required to secure today's digital infrastructure.

For more information or a demo visit https://www.netscout.com/solutions/omnis-security.

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

SECSB_029_EN-2101 04/2021