NETSCOUT

| SOLUTION BRIEF |

NETSCOUT Omnis Security

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.

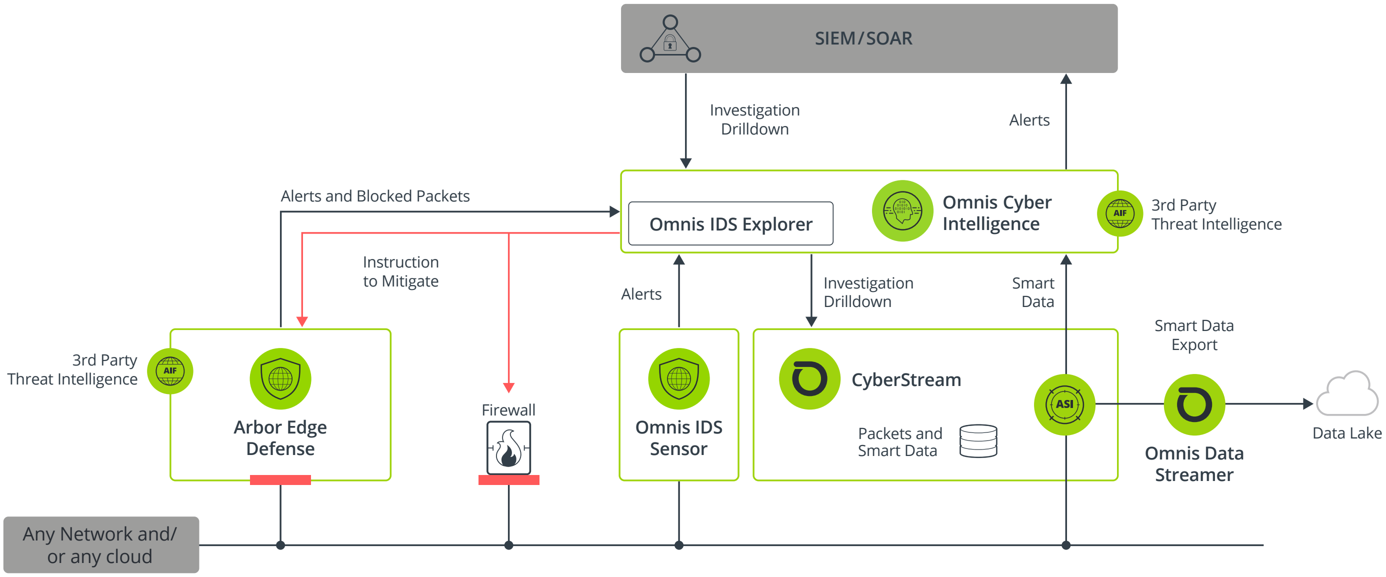
Effective Cybersecurity Starts With Comprehensive and Consistent Network Visibility

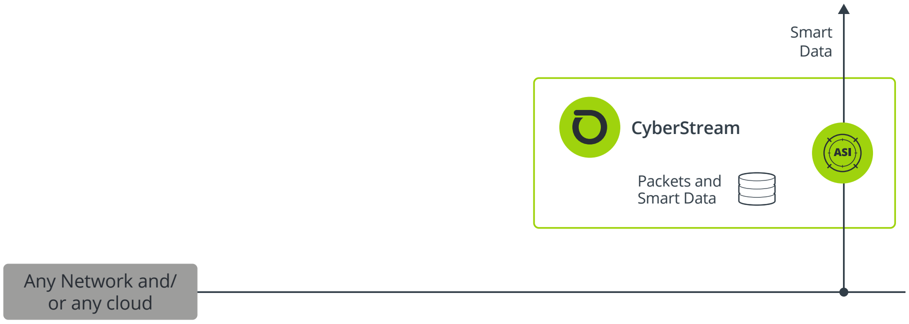
You can't protect yourself from what you can't see. It's a fundamental axiom for cybersecurity. And in today's complex world of legacy networks, branch offices, work-from-home, public and private clouds, gaining the proper level of network visibility has never been so challenging to obtain and so vital 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 metadata and packets, use of open standards, and APIs that enable integration and TechOps collaboration.





Underpinning NETSCOUT Omnis® Security is the CyberStream. CyberStream is a proven, patented, highly scalable packet acquisition, classification, and storage solution for providing comprehensive and consistent visibility into any physical, virtual, or cloud environment.

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

- Uses a certified or qualified COTS hardware.
- 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.

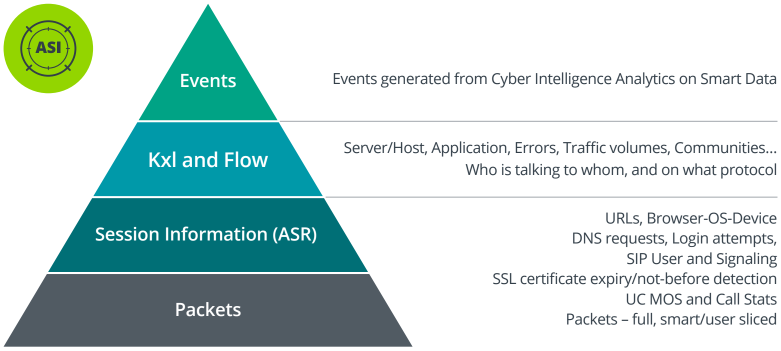
Using patented Adaptive Service Intelligence® (ASI) technology, CyberStream instrumentation converts raw network packets into indexed layer 2-7 metadata – we call this NETSCOUT "Smart Data". NETSCOUT Smart Data contains information such as:

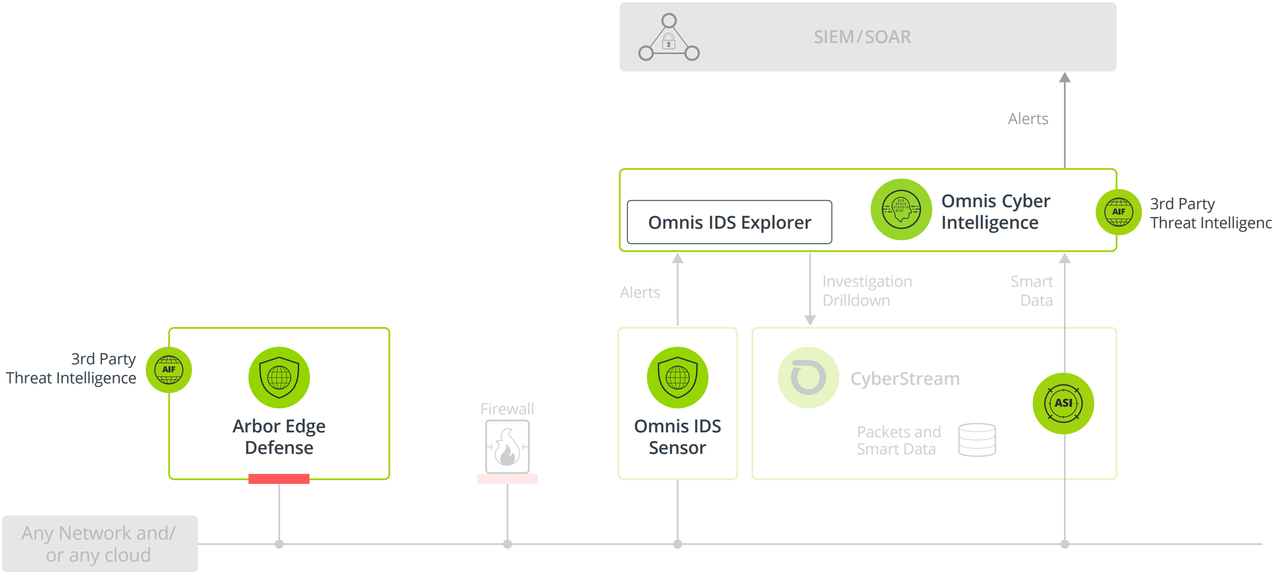
- 5-tuple attributes (source and destination IP, source and destination port and the protocol field).
- Key performance indicators (KPIs) such as error codes, response times, or mean opinion scores (MOS).
- Data from SIP user and signaling planes.
- DNS request/responses, URL, browser and device types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

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

CyberStream 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


ASI
Events
Events generated from Cyber Intelligence Analytics on Smart Data
Kxl and Flow
Server/Host, Application, Errors, Traffic volumes, Communities...
Who is talking to whom, and on what protocol
Session Information (ASR)
URLs, Browser-OS-Device
DNS requests, Login attempts,
SIP User and Signaling
SSL certificate expiry/not-before detection
UC MOS and Call Stats
Packets – full, smart/user sliced
Packets



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

Omnis Cyber Intelligence – Serving as a centralized console for advanced threat detection and response by analyzing Smart Data collected by CyberStream 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.

Omnis Intrusion Detection System (IDS) – A standalone solution or software module for CyberStream 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 Explorer application running in a 3rd party SIEM/SOAR.

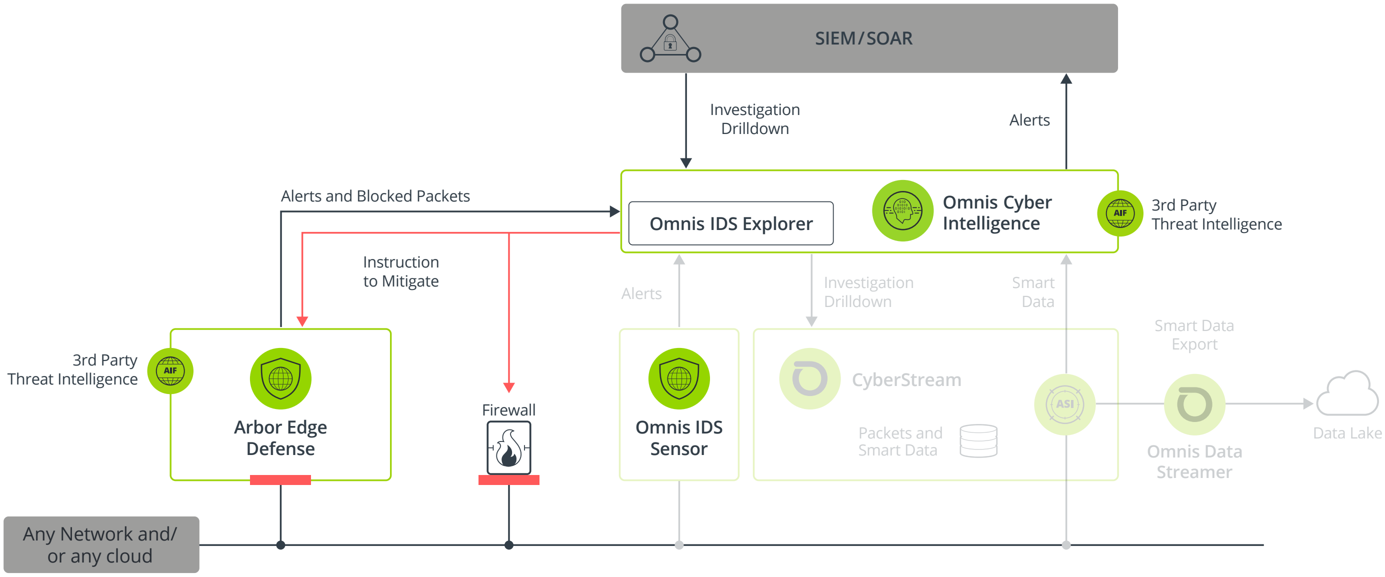
Omnis Arbor Edge Defense (AED) – Deployed on the network perimeter, inside the router and outside the firewall, Omnis Arbor Edge Defense detects inbound and outbound (e.g. north-south) threats such as DDoS attacks, scanning, brute force password attempts, malware and other IoCs using highly scalable, stateless packet processing technology and threat intelligence from NETSCOUT ATLAS and/or 3rd parties.

Together all three components provide multiple methods of network-based threat detection, and integrate into an existing security 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 Network-based Investigation – Using the rich source of NETSCOUT Smart Data, Omnis Cyber Intelligence 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 Intelligence 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.



Edge Protection – Network-based threat prevention at the network edge is one means stop known or unknown cyber threats. However, blocking of any sort must be done with complete confidence to avoid false positives. Cyber Intelligence's access to rich metadata and packets help security teams gain the confidence to block at the network perimeter. Omnis Cyber Intelligence can instruct devices like firewalls or NETSCOUT Omnis Arbor Edge Defense (Omnis AED) to block malicious traffic at the perimeter. Omnis Arbor Edge Defense can also automatically detect and block inbound and outbound threats. In particular, Omnis 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, Omnis 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, Omnis 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 Threat Detection and Response portfolio. Its focus and strength lie in utilizing network-derived packets and robust source of metadata from the NETSCOUT CyberStream 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.

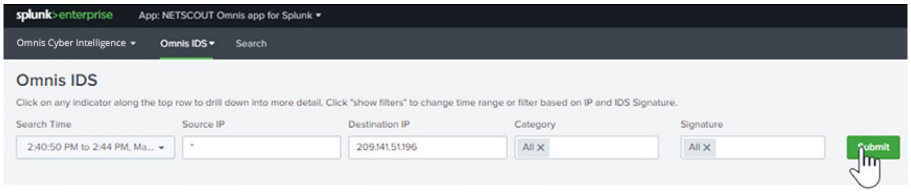
- Use of open-source threat detection (e.g., such as Suricata) and emerging industry frameworks (e.g., Mitre Att&ck).
- Apps in popular SIEMs (e.g., Splunk, AWS Security Hub).
- Integration with firewalls (e.g., PaloAlto Networks).
- Omnis Data Streamer provides the ability to export NETSCOUT's unique Smart data where it can be combined and enriched with other datasets so you can conduct your own customer analysis.

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 portfolio can be used in a real-world scenario. You're a tier 1 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**.


splunk>enterprise
App: NETSCOUT Omnis app for Splunk ▾
Omnis Cyber Intelligence ▾
Omnis IDS ▾
Search
Submit

Omnis IDS

Click on any indicator along the top row to drill down into more detail. Click "show filters" to change time range or filter based on IP and IDS Signature.

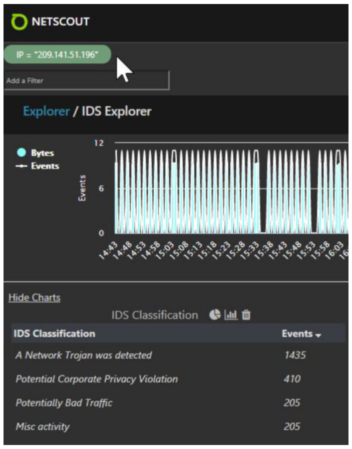
Search Time	Source IP	Destination IP	Category	Signature
2:40:50 PM to 2:44 PM, Ma... ▾	*	209.141.51.196	All ✕	All ✕

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

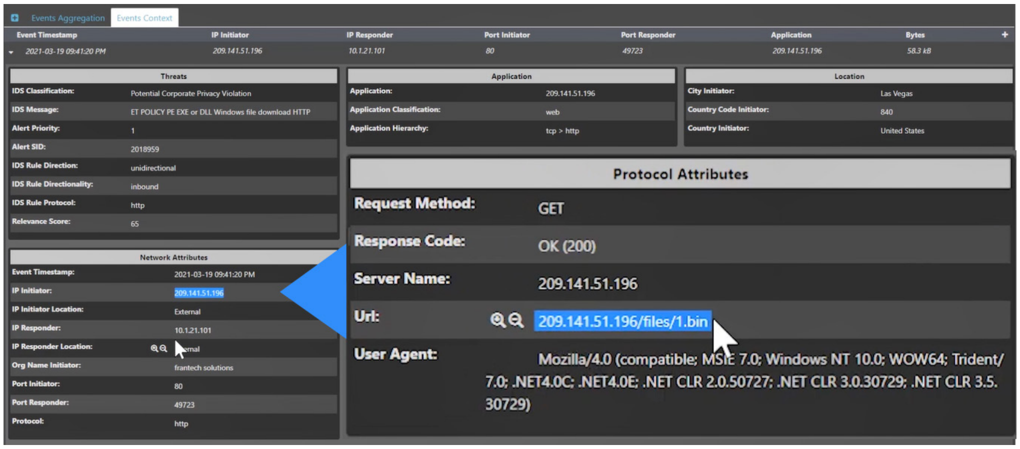
Omnis IDS has identified and classified many events associated with this host including a network trojan, potential corporate privacy violations and more.

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)



IDS Classification	Events ▾
A Network Trojan was detected	1435
Potential Corporate Privacy Violation	410
Potentially Bad Traffic	205
Misc activity	205



Event Timestamp	IP Initiator	IP Responder	Port Initiator	Port Responder	Application	Bytes
2021-03-19 09:41:20 PM	209.141.51.196	10.1.21.101	80	49723	209.141.51.196	58.3 kB

Threats	
IDS Classification:	Potential Corporate Privacy Violation
IDS Message:	ET POLICY PE EXE or DLL Windows file download HTTP
Alert Priority:	1
Alert SID:	2018959
IDS Rule Direction:	unidirectional
IDS Rule Directionality:	inbound
IDS Rule Protocol:	http
Relevance Score:	65

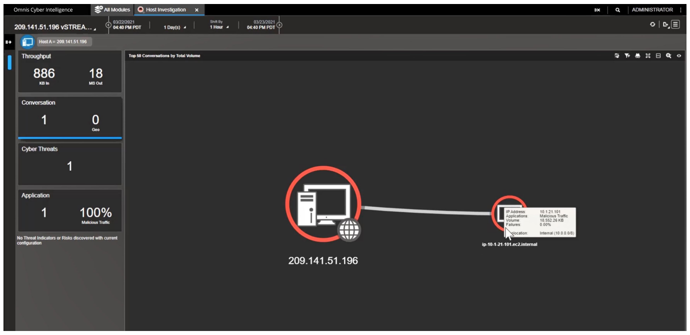
Network Attributes	
Event Timestamp:	2021-03-19 09:41:20 PM
IP Initiator:	209.141.51.196
IP Initiator Location:	External
IP Responder:	10.1.21.101
IP Responder Location:	ernal
Org Name Initiator:	frantech solutions
Port Initiator:	80
Port Responder:	49723
Protocol:	http

Application	
Application:	209.141.51.196
Application Classification:	web
Application Hierarchy:	tcp > http

Location	
City Initiator:	Las Vegas
Country Code Initiator:	840
Country Initiator:	United States

Protocol Attributes	
Request Method:	GET
Response Code:	OK (200)
Server Name:	209.141.51.196
Url:	209.141.51.196/files/1.bin
User Agent:	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/ 7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5. 30729)

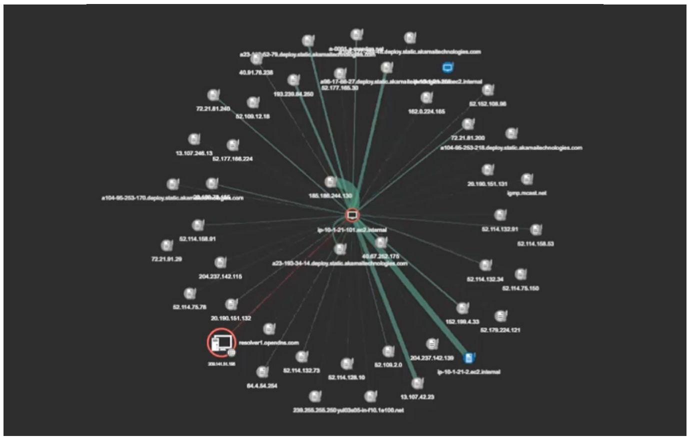
Now let's conduct a further investigation using Omnis Cyber Intelligence. From a Cyber Intelligence application running in the same Splunk SIEM or from the Cyber Intelligence console itself, we can easily filter on the suspicious IP address of 209.141.51.196 and time frame. Instantly you are presented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



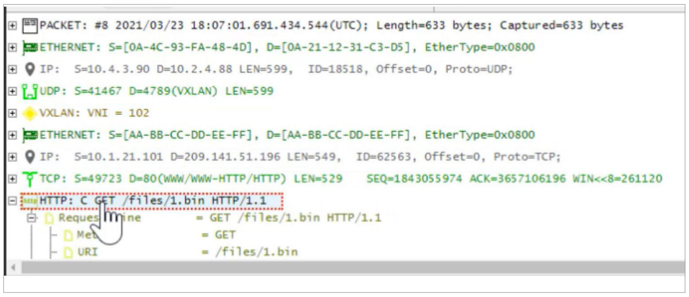
Throughput: 886 KB In, 18 MB Out
Conversation: 1, 0 Geo
Cyber Threats: 1
Application: 1, 100% Malicious Traffic
No Threat Indicators or Risks discovered with current configuration

IP Address: 10.1.21.101
Applications: Malicious Traffic
Volume: 18,552.26 KB
Failures: 0.00%
Location: Internal (10.0.0.0/8)

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



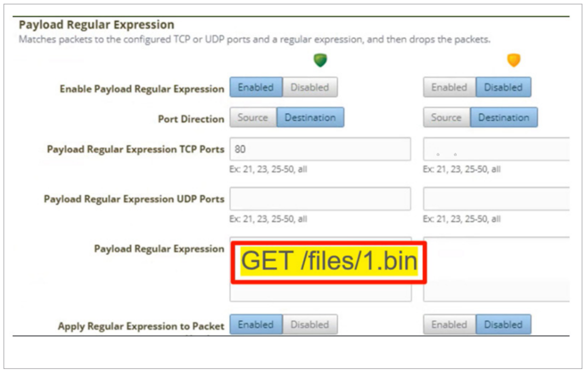
Another click, brings you down to a packet level exposing the malicious URL and file.



```
⊞ PACKET: #8 2021/03/23 18:07:01.691.434.544(UTC); Length=633 bytes; Captured=633 bytes
⊞ ETHERNET: S=[0A-4C-93-FA-48-4D], D=[0A-21-12-31-C3-D5], EtherType=0x0800
⊞ IP:  S=10.4.3.90 D=10.2.4.88 LEN=599,  ID=18518, Offset=0, Proto=UDP;
⊞ UDP: S=41467 D=4789(VXLAN) LEN=599
⊞ VXLAN: VNI = 102
⊞ ETHERNET: S=[AA-BB-CC-DD-EE-FF], D=[AA-BB-CC-DD-EE-FF], EtherType=0x0800
⊞ IP:  S=10.1.21.101 D=209.141.51.196 LEN=549,  ID=62563, Offset=0, Proto=TCP;
⊞ TCP: S=49723 D=80(WWW/WWW-HTTP/HTTP) LEN=529   SEQ=1843055974 ACK=3657106196 WIN<<8=261120
⊟ HTTP: C GET /files/1.bin HTTP/1.1
   ⊟ Reques  ine          = GET /files/1.bin HTTP/1.1
     ├ Me                  = GET
     ├ URI                 = /files/1.bin
```

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 Intelligence can create a block command for example, to PaloAlto firewall. Another more intelligent option is to configure our Omnis 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 Omnis 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.

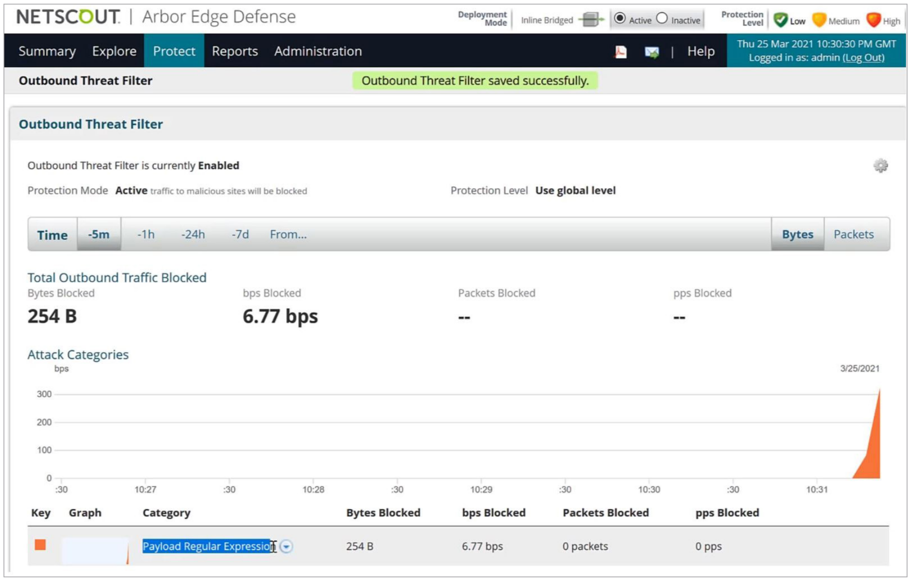


Payload Regular Expression

Matches packets to the configured TCP or UDP ports and a regular expression, and then drops the packets.

Enable Payload Regular Expression	Enabled	Disabled
Port Direction	Destination	Destination
Payload Regular Expression TCP Ports	80 Ex: 21, 23, 25-50, all	Ex: 21, 23, 25-50, all
Payload Regular Expression UDP Ports	Ex: 21, 23, 25-50, all	Ex: 21, 23, 25-50, all
Payload Regular Expression	GET /files/1.bin	
Apply Regular Expression to Packet	Enabled	Disabled

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



Thu 25 Mar 2021 10:30:30 PM GMT
Logged in as: admin (Log Out)

Outbound Threat Filter

Outbound Threat Filter saved successfully.

Outbound Threat Filter

Outbound Threat Filter is currently **Enabled**

Protection Mode **Active** traffic to malicious sites will be blocked

Protection Level **Use global level**

Total Outbound Traffic Blocked

Bytes Blocked	bps Blocked	Packets Blocked	pps Blocked
254 B	6.77 bps	--	--

Attack Categories

Key	Graph	Category	Bytes Blocked	bps Blocked	Packets Blocked	pps Blocked
🟧		Payload Regular Expressio	254 B	6.77 bps	0 packets	0 pps

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

Conclusion

NETSCOUT Omnis Security 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 Omnis 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.
- Export NETSCOUT Smart Data for aggregation and enrichment with other datasets for custom analysis.

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: 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