NOMINET CYBER SECURITY

Nominet NTX Platform

Nominet's NTX solution equips you with ground-breaking cyber threat monitoring and analytics capabilities. It uses machine learning and unique algorithms to find unknown threats hidden in your network.

In addition, it is designed to work in tandem with leading-edge third-party threat feeds in order to find (and block) the known bad threats.

All this makes NTX the ideal solution for protecting your organization – all using your DNS data.

This unique approach enables your organization to instantly detect single malicious packets hidden inside vast quantities of legitimate enterprise data, including:

- Command-and-control malware traffic
- Data exfiltration via DNS tunnelling
- Phishing attacks
- DNS hijacking attempts and brand adjacency identification with the Digital Brand Safe option

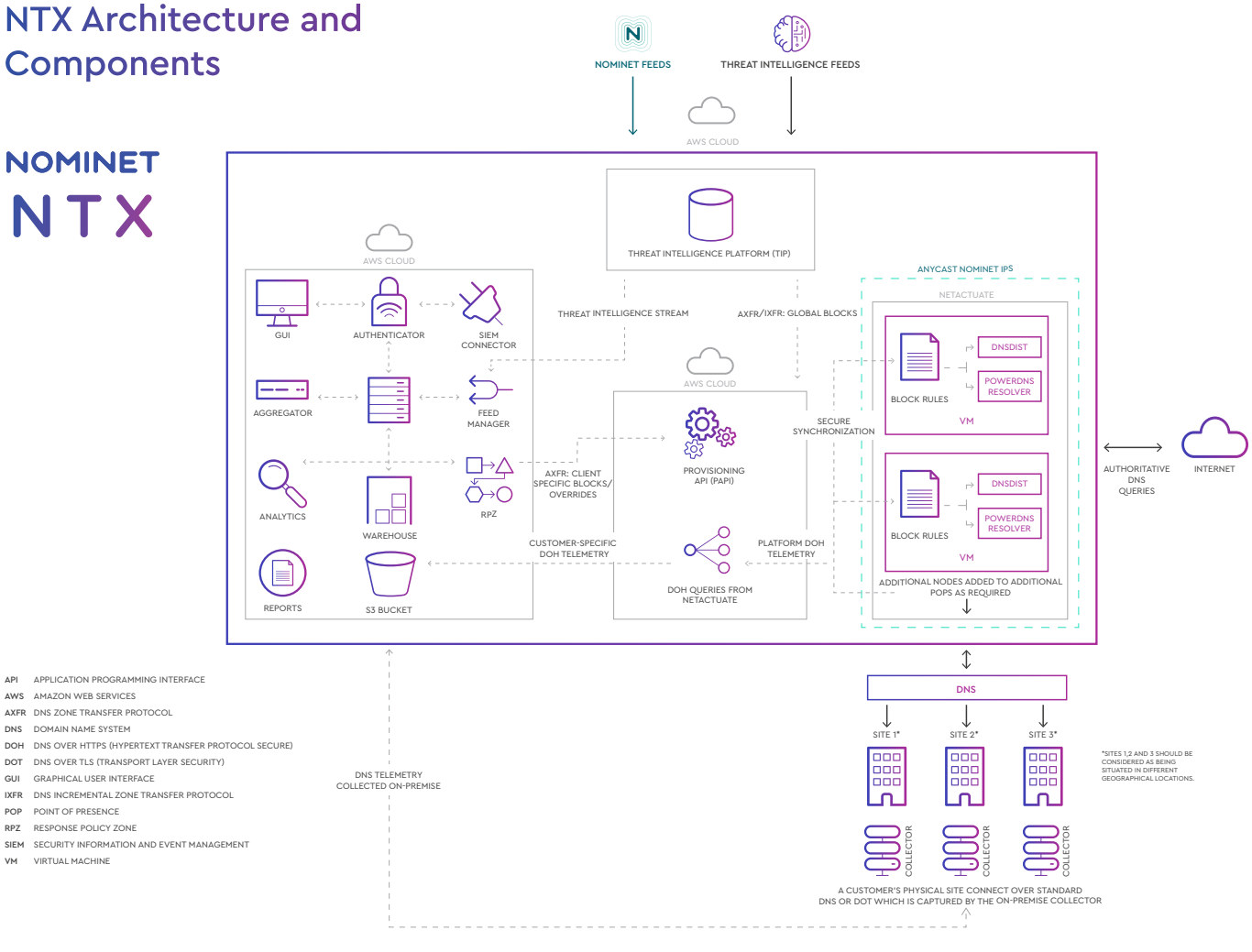
NTX combines Nominet's unique advanced heuristics with data science intelligence to interrogate your DNS traffic for anomalies and threats. This provides your organization with immediate visibility into attacks hitting your network and enables you to block them before they penetrate and spread throughout your enterprise.

As a result, NTX will highlight attack-related activity before any other security tool would have picked it up.

NTX uses its analytics engine as well as its 'network learning' capabilities to detect known and unknown threats, suspicious activity and out-of-the-ordinary events inside your organization's DNS traffic.

NTX Architecture and Components

NOMINET NTX



API	APPLICATION PROGRAMMING INTERFACE
AWS	AMAZON WEB SERVICES
AXFR	DNS ZONE TRANSFER PROTOCOL
DNS	DOMAIN NAME SYSTEM
DOH	DNS OVER HTTPS (HYPERTEXT TRANSFER PROTOCOL SECURE)
DOT	DNS OVER TLS (TRANSPORT LAYER SECURITY)
GUI	GRAPHICAL USER INTERFACE
IXFR	DNS INCREMENTAL ZONE TRANSFER PROTOCOL
POP	POINT OF PRESENCE
RPZ	RESPONSE POLICY ZONE
SIEM	SECURITY INFORMATION AND EVENT MANAGEMENT
VM	VIRTUAL MACHINE

NTX Platform Components and User Interface

Component	Function
Aggregator	Queries one or more Warehouses in order to answer queries about traffic data collected by Collectors. Results are cached in a MySQL database for reuse. Each Aggregator can handle up to 225,000 DNS queries per second.
Analytics	Analyzes DNS traffic in real time, interrogating it against Nominet's unique smart heuristics and data science intelligence, to spot anomalies and remediate threat activity.
Authenticator	Queries one or more Warehouses about collected traffic data. Results are cached in a MySQL database for reuse.
AWS S3	Provides storage and retrieval of an unlWimited amount of data from any location.
Blocking DN Resolver	Filters specific domains, preventing them from being accessed.
Collector	Captures DNS packets using port mirroring and passes them to the Warehouse component for real-time analysis and archiving for post-breach forensics. One Collector is installed per network location that is being monitored. Should the Collector be installed on a machine different to the Warehouse, a Streamer is required to stream data to the remote warehouse.
Database	Schema definitions for the NTX database.
DNS Resolver	Respond to requests to resolve domain names, translating them into IP addresses.
Firewall	Monitors network traffic, determining whether to allow or block data packets based on a set of security rules.
Forwarding Resolver	Directs specific DNS requests to designated DNS servers for resolution.
Provisioning API (PAPI)	Provides authentication syncing with the organization's identity server.
Reports	Handles generation and downloading of reports in PDF format.
SIEM Connector	Sends security events from the NTX engine to connected SIEM platforms, like IBM QRadar, Splunk and ArcSight, in a number of different formats such as LEEF, syslog and JSON-formatted.
Threat Intelligence Platform (TIP)	Aggregates, correlates and analyzes threat data from multiple sources in real time to inform defensive action.
Warehouse	Stores files received from one or more Collectors in a sharded structure, for efficient access.

The user interface

Dashboard

Gives you an at-a-glance view of your organization's DNS traffic and highlights all captured threats. It displays information such as total queries, events detected, event breakdown, overall risk level and the ability to click and drill down on single packets and threats.

Custom views

Enables you to build your own dashboard views, to display the information most relevant to your organization.

Policy explorer

Enables you to view all response policy zones created within the platform.

Event view

Provides you with a view of all the individual events and enables you to deep dive into as much detail as your organization needs, including a packet level view.

Reports

Enables you to generate and view detailed reports of your organization's risk score and the point-in-time attacks that have targeted your enterprise.

Events

The nature of threats detected differs depending on the type of campaign that cyber criminals are launching against your organization. The advanced heuristics inside Nominet's NTX analytics engine are designed to detect and protect against the event types in the following table.

Details of this activity are displayed visually on your dashboard and can also be fed into your organization's SIEM platform.

Event Category	Description
Malicious	NTX analytics detect traffic bound to domains associated with malware activity and Domain Generation Algorithms (DGAs). Typically, these domains are non-human readable and signal command-and-control traffic between an infected endpoint in an enterprise and a server hosted on the internet.
Exfiltration	Data exfiltration via DNS tunnelling, manifests as data encoded in the subdomain of the domain being used to carry out the attack.
New Domains	Newly observed domains are simply recently registered domains. Enterprise users don't tend to access a domain which has only just appeared. When you see bursts of traffic to a new domain, this is usually DNS-related abuse.
Phishing	This category includes phishing websites and abusive registrations. Endpoints trying to communicate with phishing websites are at risk of potential malware infection from a malicious download.
Spam Delivery	The delivery of spam from one organization to another, which registers the arrival of spam to the targeted organization's infrastructure.
Tor	Use of the Tor anonymity network. While many network operators and commercial sites block Tor completely, it's useful to know if it's there.
DNS Hijack*	Modifications to DNS where a correlation against existing threat intelligence is made.
DDoS	A distributed denial-of-service (DDoS) attack is an event where the attackers try to make the victim's server unavailable by overloading it with DNS requests from a large number of endpoints under their control (e.g. a botnet).
Spam Campaign	This manifests as a large spike in email-related requests originating from an IP range and delivered to a large number of recipients. This is normally caused by infected machines sending coordinated bulk email as part of a botnet.
Traffic	These events may appear identical to DDoS traffic but can represent a misconfiguration between machines/infrastructure that cause a cycle of failing retries.
DNS Change*	Modifications to DNS where no correlation can be made against existing threat intelligence.
Brand Adjacency*	An attack carried out through attempting to use a new, malicious domain that mimics an existing, legitimate one, with the ultimate aim to point it at a rogue DNS server.

*This feature is part of the NTX Digital.Brand.Safe functionality, which generates threat events designed to alert an organization when its authoritative DNS records change for any reason.

Remediation – Policy Engine

Nominet NTX provides Response Policy Zones (RPZ) for DNS firewall configuration. It uses Nominet's RPZ feed applied directly to a resolver and gives the users the ability to configure their own RPZ actions; for example, to block websites that haven't been blocked by other rules. The following RPZ policy actions are available on both NTXprotect and NTXsecure. If you select NTXsecure then Nominet will manage this for you:

Policy Action	Description
Whitelist	Always allows the query to resolve correctly.
Sinkhole	Always returns the same user-defined IP address, allowing re-directing to a sinkhole.
Blacklist	Drops the query with an "NXDOMAIN" (non-existent domain) response.
Blocklist	Always returns the same user-defined IP address, allowing re-directing to a block page.

SIEM integration

Nominet's rich APIs enable you to enrich your SIEM data with DNS threat intelligence. As a result, you can reduce noise, speed up response times to critical threats and improve intelligence for post-breach forensics.

Through Nominet's SIEM Connector, these events can be sent to connected SIEM platforms, such as QRadar, Splunk and ArcSight, in a number of different formats (such as LEEF, syslog, JSON-formatted file).

Operating system and hardware requirements

Components run on 64 bit Linux. Nominet supports CentOS 6 or 7 and RHEL 6 or 7.

Services	Instance types	Notes
Aggregator, Authenticator, SIEM Connector, GUI	r4.xlarge	A SIEM endpoint is located remotely
Analytics, Feeds, RPZ Policy Module	r4.xlarge	25 GB encrypted storage volume
Database	m3.2xlarge	
Warehouse	d2.2xlarge	

Component	Hardware Capacity
Aggregator	A dedicated physical or virtualized server should be provided for the Aggregator. The requirements for number of CPU cores, RAM and storage type and capacity depend on traffic volumes and desired performance.
Analytics	A dedicated physical or virtualized server with at least 8 GB of RAM and a 4-core CPU.
Authenticator	At least 8 GB of RAM, 4-core CPU.
Collector	The Collector component can be installed on either: • Each DNS Server to be monitored • On a separate server using port mirror to capture the DNS traffic Recommended hardware requirements for a Collector: Intel®Xeon®Processor or equivalent, at least dual-core CPU, 8 GB of RAM, 100 GB HDD.
Database	At least 32 GB of RAM, 8-core CPU. The disk space required for the database depends on the traffic rate and data collection mode, and is calculated per Collector per day. For example 25,000 DNS queries per second would need 3 GB per collector per day, while 225,000 queries per second will need 27 GB per collector per day.
Feed Manager	At least 8 GB of RAM, 4-core CPU.
Reports	At least 16 GB of RAM, 4-core CPU.
RPZ Policy	At least 8 GB of RAM, 4-core CPU.
SIEM Connector	At least 8 GB of RAM, 4-core CPU.
UI	Recommended minimum screen resolution: 1280 × 1024 px
Warehouse	For very high DNS traffic volumes (over 200,000 QPS) we recommend use of SSDs in the server on which the Collector component is installed. Storage capacity required will depend on traffic volumes and the final configuration of NTX. For example, at a traffic rate of 25,000 QPS, 238 GB of storage will be required for 1 day of data.

Contact us

For more information on how Nominet can help secure your business, get in touch today:

US: +1 202 821 4256
UK: +44 (0) 1865 332 255
info@nominetcyber.com
nominetcyber.com