Nominet NTX Platform

The Nominet NTX platform equips you with ground-breaking cyber threat monitoring and analytics capabilities. It uses patented compression, analysis and advanced heuristics to find cyber threats hidden amongst your organisation's DNS data.

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

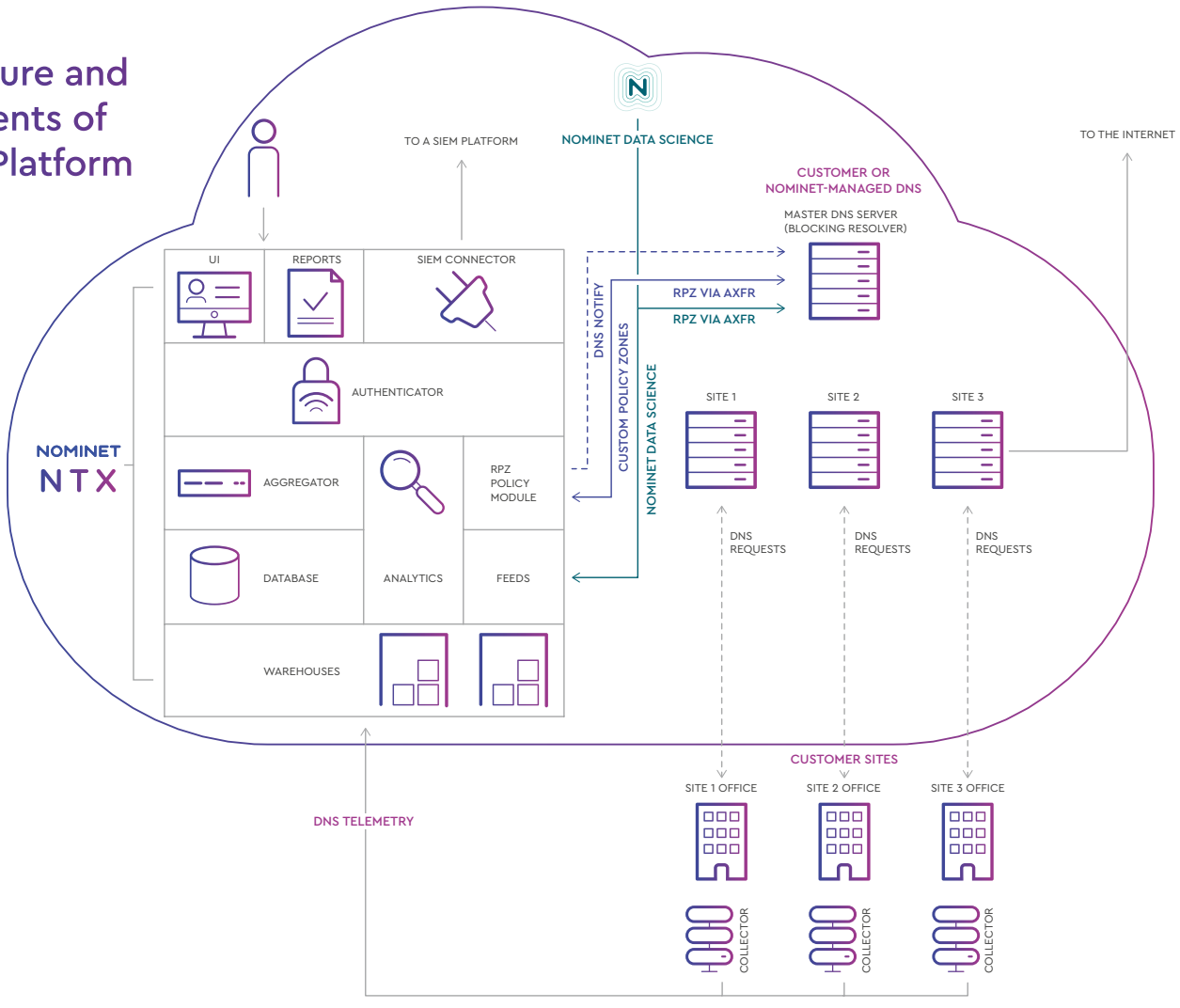
- Command-and-control malware traffic
- Data exfiltration via DNS tunnelling
- Phishing attacks
- Botnet activity, such as coordinated spam campaigns

The NTX platform combines our unique advanced heuristics with our data science intelligence to interrogate your DNS traffic for anomalies and threats. This provides you 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, the platform will highlight attack-related activity before any other security tool would have picked it up.

The NTX platform 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 organisation's DNS traffic.

Architecture and Components of the NTX Platform



NTX Platform Components and User Interface

Name	Description
Warehouse	Stores files received from one or more Collectors in a sharded structure, for efficient access.
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.
Collector	Captures DNS packets using port mirror 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.
Analytics	Analyses DNS traffic in real time, interrogating it against our unique smart heuristics and our Nominet data science intelligence, to spot anomalies and remediate threat activity.
Feed Manager	Receives intelligence from the Nominet data science platform and feeds it into the Analytics module.
RPZ Policy	Handles Response Policy Zones (RPZ).
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.
Reports	Handles generation and downloading of reports in PDF format.
Database	Schema definitions for the MySQL database.
Authenticator	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.

The user interface

Dashboard

Gives you an at-a-glance view of your 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

Build your own dashboard views, to display the information most relevant to you.

Policy explorer

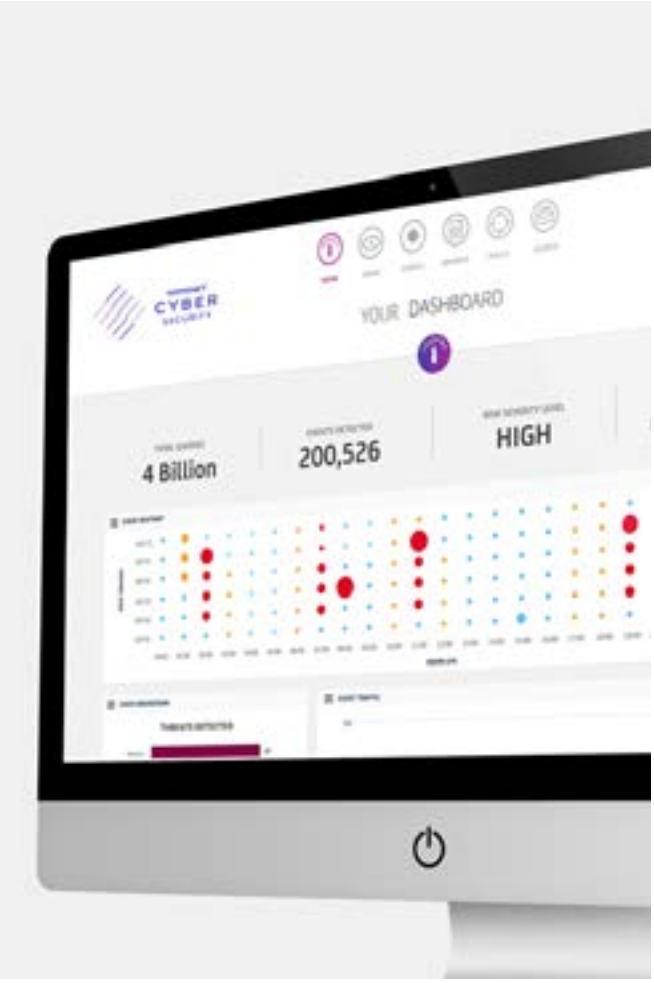
View all RPZs created within the platform.

Event view

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

Reports

Detailed report of your 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 organisation. The advanced heuristics inside our 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 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.
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.
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 organisation to another, which registers the arrival of spam to the targeted organisation's infrastructure.
Traffic	These events may appear identical to DDoS traffic but can represent a misconfiguration between machines/infrastructure that cause a cycle of failing retries.
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.

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.
Loglist	Allows the query to resolve and logs the query.
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

Our 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 our 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.

Component	Hardware Capacity
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.
Aggregator	A dedicated physical or virtualised 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.
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.
Analytics	A dedicated physical or virtualised server with at least 8 GB of RAM and a 4-core CPU.
Feed Manager	At least 8 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.
Reports	At least 16 GB of RAM, 4-core CPU.
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.
Authenticator	At least 8 GB of RAM, 4-core CPU.
UI	Recommended minimum screen resolution: 1280 × 1024 px

Contact us

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

UK: +44 (0) 1865 332 255
US: +1 202 821 4256
cybersecurity@nominet.com
www.nominet.com/cybersecurity