NOMINET CYBER SECURITY

Nominet NTX Platform Technical Datasheet

Nominet's cyber security services are based on the NTX platform, a DNS-based threat detection and analytics technology. It captures DNS traffic in real-time and analyses it using machine learning algorithms, known as smart heuristics, which can spot a single malicious packet hidden amongst billions.

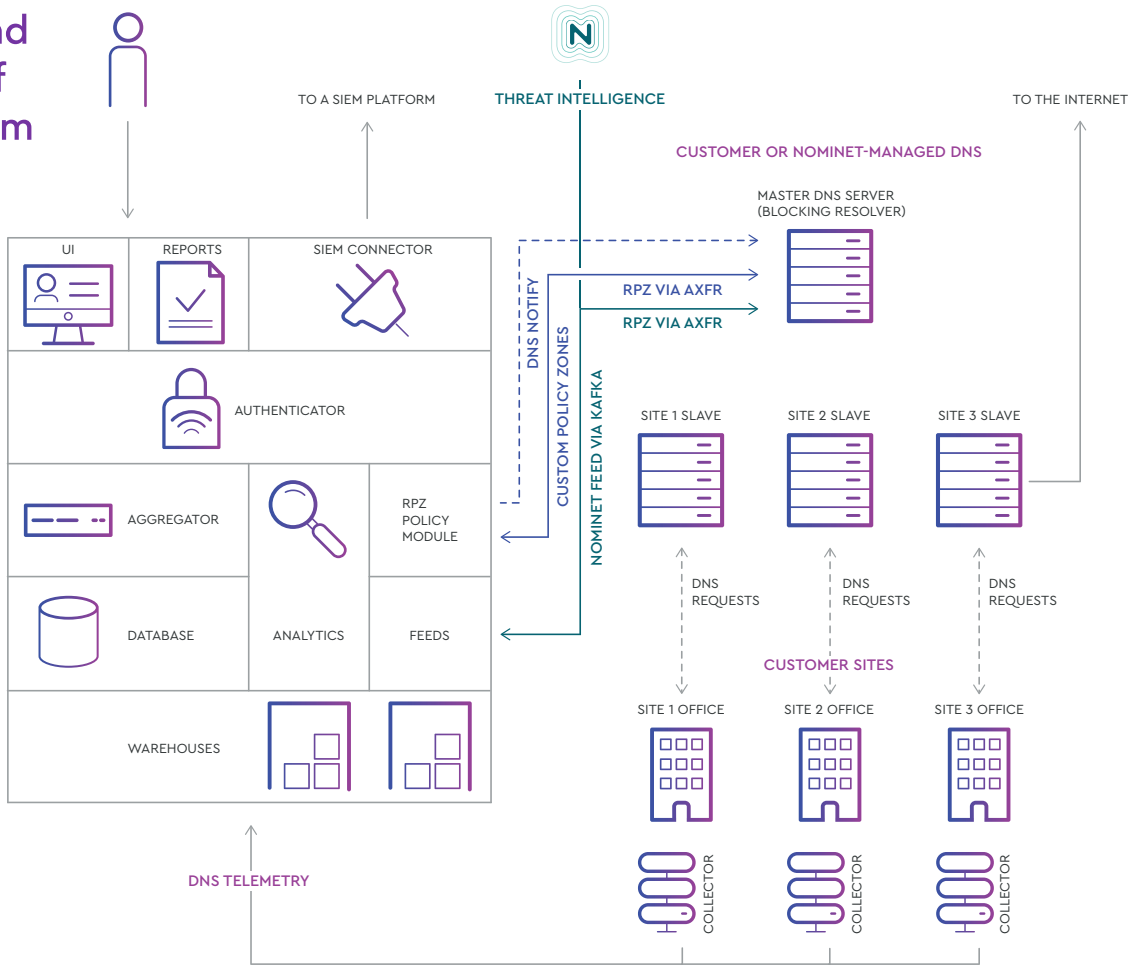
These don't rely on the traditional signature-based approach and are designed to automatically detect:

- Malware command and control traffic.
- Data exfiltration via DNS tunnelling.
- DDoS attacks.
- Botnet activity, such as coordinated spam campaigns.

Alongside the Nominet smart heuristics, the platform ingests and performs correlation of DNS traffic with threat intelligence from Nominet's data science platform

The NTX platform uses its analytics engine as well as threat intelligence to detect known and unknown threats, suspicious activity and out-of-the-ordinary events in an organisation's DNS traffic.

Architecture and Components of the NTX Platform



NTX Platform Components and User Interface

Name	Description
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	Monitors traffic, using the Aggregator API, and checks for any anomalies or unusual activity (events) in traffic reported by Collectors.
Authenticator	Provides an authentication service for Active Defence user accounts – verifies user names and passwords and provides multi-factor authentication.
Collector	Captures DNS packets in one of the following formats: port mirrored traffic, PCAP files, or dnstap files. Each Collector can accept up to 225,000 DNS queries per second.
Database	Schema definitions for the MySQL database.
Feed Manager	Handles Nominet's and third-party security intelligence feeds used by the Analytics module.
Reports	Handles generation and downloading of reports in PDF format.
RPZ Policy	Handles Response Policy Zones (RPZ).
SIEM Connector	Sends security events from the NTX engine to connected SIEM platforms, such as IBM QRadar or Splunk, in a number of different formats.
Warehouse	Stores files received from one or more Collectors in a shared structure, for efficient access.

The user interface

Dashboard

Gives you an at-a-glance view of your DNS traffic and highlights any threats. It displays information such as total queries, events detected, event breakdown, overall risk level and much more.

Custom views

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

Policy explorer

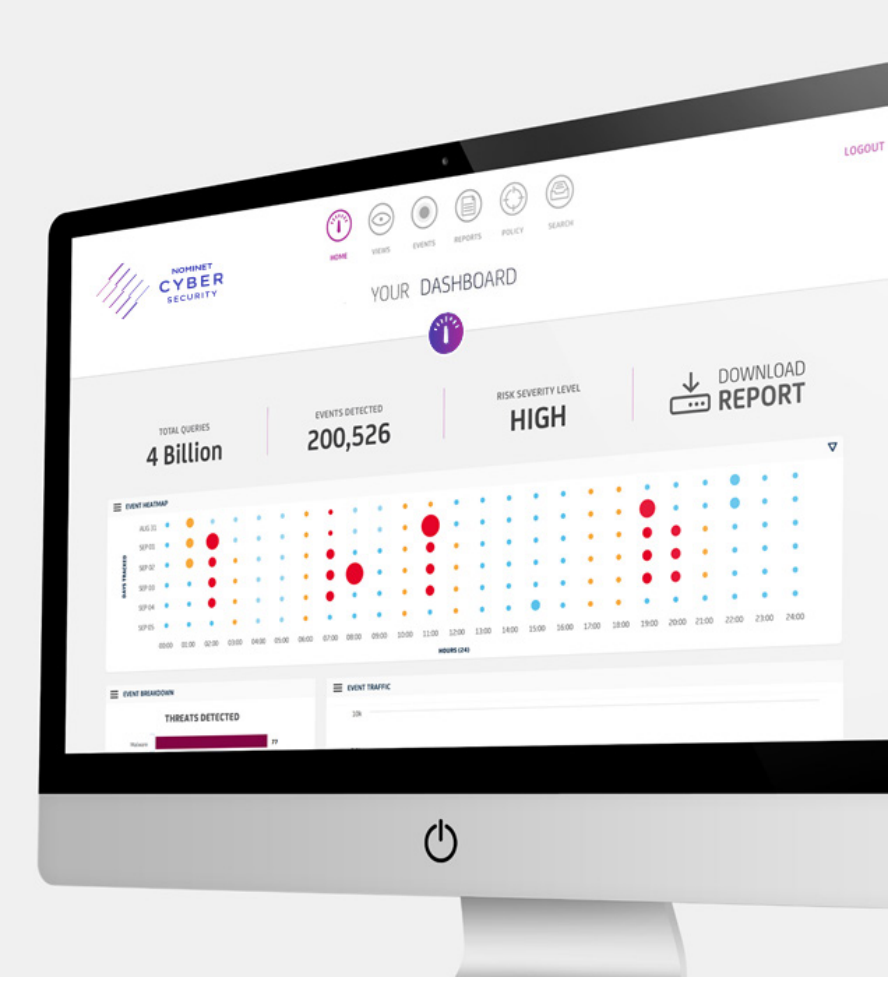
View all RPZs created within the platform.

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

Can be generated at the click of a button.



Events

The nature of threats detected differs depending on whether an organisation chooses to capture DNS traffic on a recursive or authoritative resolver, because of how certain threats manifest themselves within DNS.

Event Category	Description	Recursive	Authorative
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.	Y	N
Exfiltration	Data exfiltration via DNS tunnelling, manifests as data encoded in the subdomain of the domain being used to carry out the attack.	Y	N
DDoS	NTX detects and raises events for the two main types of DDoS attacks: • Reflection attack • Random subdomain attack These are often started from a botnet of compromised machines or IOT devices.	N	Y
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.	Y	N
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.	N	Y
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.	Y	N
Spam Delivery	The delivery of spam from one organisation to another, which registers the arrival of spam to the targeted organisation's infrastructure.	N	Y
Traffic	These events may appear identical to DDoS traffic but can represent a misconfiguration between machines/infrastructure that cause a cycle of failing retries.	Y	Y
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.	N	Y

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, if you select NTXsecure then Nominet can 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

The NTX software captures and analyses DNS traffic in real time and generates events when it detects malicious or unusual activity in the DNS traffic.

Using a 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).

Specification

Operating system	CentOS	RHEL
64-bit Linux	6 or 7	6 or 7

Hardware requirements

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 3GB per collector per day, while 225,000 queries per second will need 27GB 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 Active Defence. 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:

UK: +44 (0) 1865 332 255 | USA: +1 267 908 3004
www.nominet.uk/cybersecurity