# THE NSFOCUS NEXT GENERATION ADVANCED THREAT PROTECTION (APT) SOLUTION

Enterprises are constantly assaulted by malware, ransomware, botnets and other forms of attack that can easily circumvent traditional firewalls and legacy Intrusion Prevention Systems. That's because most modern attacks are content based and sophisticated detection mechanisms that can perform deep content inspection are not adequate for finding the next-gen bad hiding among the good.

**The NSFOCUS Next Generation Intrusion Prevention System (NGIPS)** protects against known and zero day Advanced Persistent Threats (APTs) assaulting your enterprise. NGIPS goes beyond deep packet inspection by using the Smart Learning advanced heuristics engine to examine all inbound and outbound traffic so that malicious content and traffic is blocked while safe content is allowed through.

<table>
<tr><th colspan="3">INTRUSION PREVENTION</th></tr>
<tr><td>Travel Control</td><td>Anti-DDoS</td><td>Web Security</td></tr>
<tr><td colspan="3">Context-Aware User and Application Identification</td></tr>
<tr><td colspan="3">Management and Threat Visualization</td></tr>
</table>

## KEY FEATURES OF THE NGIPS INCLUDE:

- ✓ Intrusion prevention using NSFocus' Intelligent Detection technology as well as over 7500 unique deep packet inspection signatures and behavioral analysis algorithms.
- ✓ The optional Threat Analysis Engine detects sophisticated content-based attacks including Zero Day.
- ✓ Active use of NSFocus' Threat Intelligence feeds.
- ✓ Context aware user identity to monitor and map users to specific IP and protocol utilization.
- ✓ Active Web Security to protect against Cross Site Scripting (XSS), SQL injection, directory traversal and more.
- ✓ Detection and control of over 2,500 different network-based applications.
- ✓ Sophisticated traffic control mechanisms.
- ✓ Active in-line anti-virus.

# INTELLIGENT DETECTION

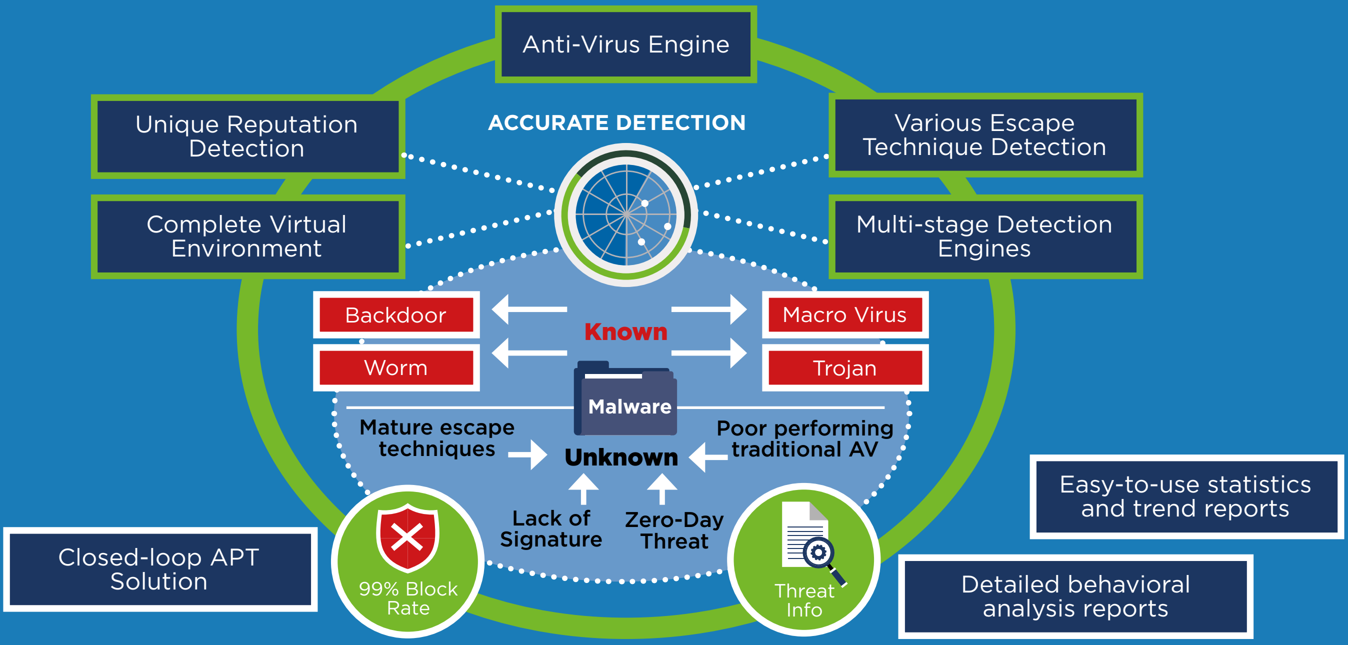
NSFOCUS Intelligent Detection (patent pending) uses advanced heuristics analysis of over several million web requests to differentiate proper HTTP request syntax from potentially malicious requests. This gives NGIPS a higher degree of accuracy identifying attacks like XSS and SQLi as well as an order of magnitude higher rejection rate of false positives/negatives then using traditional signatures and pattern matching.

| SQLi | False Negative | False Positive |
|---|---|---|
| **Intelligent Detection** | 0.026874% | 0.000754% |
| **Signature-based Detection** | 0.604676% | 0.342720% |

# THREAT ANALYSIS ENGINE

## The NSFocus multi-stage Threat Analysis Engine stops content-based and even zero-day attacks cold.

By employing IP reputation with threat intelligence, anti-virus with millions of entries, a static analysis engine and an execution sandbox, your enterprise is protected against a wide variety of modern threats.


Anti-Virus Engine
ACCURATE DETECTION
Unique Reputation Detection
Various Escape Technique Detection
Complete Virtual Environment
Multi-stage Detection Engines
Backdoor
Worm
Known
Macro Virus
Trojan
Malware
Mature escape techniques
Unknown
Poor performing traditional AV
Lack of Signature
Zero-Day Threat
99% Block Rate
Threat Info
Closed-loop APT Solution
Easy-to-use statistics and trend reports
Detailed behavioral analysis reports

Most ATP attacks begin with phishing, and if you can stop the phishing, you can stop the attack from ever gaining a foothold in your environment. The Threat Analysis Engine helps by providing support for HTTP, POP3, SMTP, IMAP and SMB protocols so that virtually any kind of inbound traffic can be inspected.

For detecting malicious content, the Threat Analysis Engine supports a wide variety of file types, including EXE, RAR, XLSW, HTML, PDF, SWF, DOC, DOCX, JPEG and more. Detailed static analysis is performed on many types of content to detect malicious intent, including JavaScript, SWF and shell code. Finally, for executables, a multi-environment sandbox is provided so content can be executed safely for inspection of behavioral patterns indicative of malware.

# THREAT ANALYSIS ENGINE KEY FEATURES

The Threat Analysis Engine provides a rich set of active protection technologies including:

**File processing** which rebuilds and parses file content detected over HTTP, FTP, SMTP, POP3 and IMAP protocols.

**Threat Visualization** provides multiple views for threat information: locations, users, and assets.

**Static Detection** of shellcode.

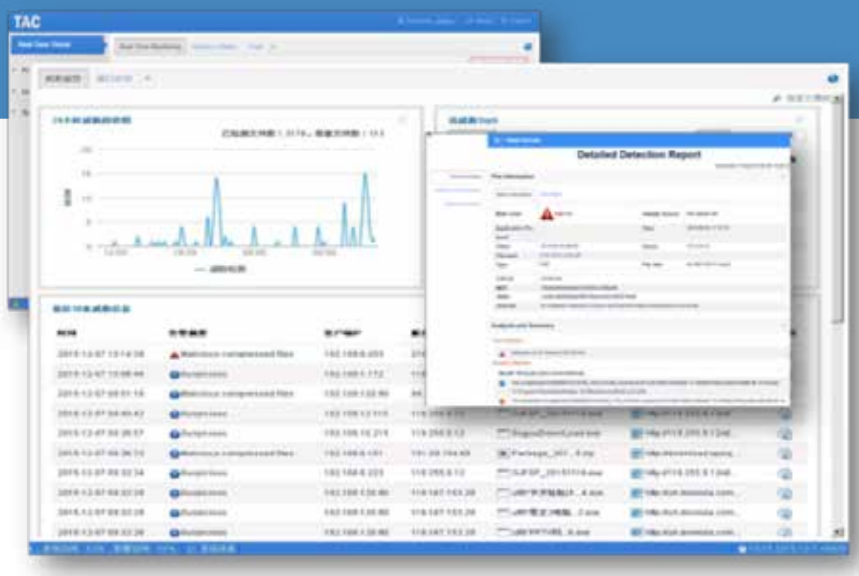
**Tight Integration with the NGIPS** function so that detected attacks can be mitigated.

**Dynamic Detection by virtual execution** allowing for dynamic behavior detection independent of static signature-based techniques, providing accurate detection of Day Zero attacks and previously unknown malware.

**Virus Detection** against rebuilt files to protect against known malware.

**Full Integration with Threat Intelligence** allowing the reputation of the data source to be evaluated for potential risk, command & control behavior, or previous malware relationships.

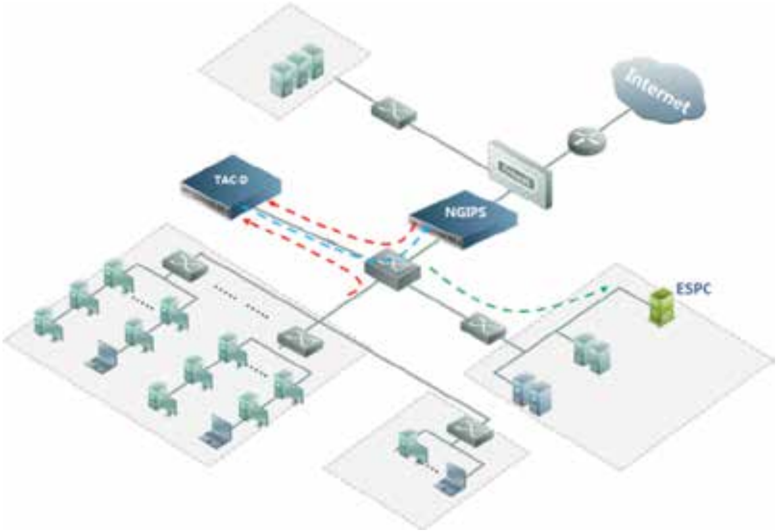
**Extensive Reporting and Logging** allows for easy understanding of your threat situation including the latest threat events, 24-hour threat trends and daily, weekly, monthly or annual reporting options.



## TYPICAL OPERATIONAL MODEL

In this model, the Threat Analysis Engine is connected to a network switch. The NGIPS transmits content requiring analysis (files) to the Threat Analysis Engine. When the Threat Analysis Engine detects malicious content, it informs the NGIPS to block the traffic, protecting the network. Optionally, an alert can be sent to a third-party SIEM if necessary.

The typical deployment model for the NGIPS and Threat Analysis Engine is shown below.



In detail, the system works like this:

01 External attacks try to go through the NGIPS.

02 The NGIPS detects known attacks via behavior analysis, statistical collection and signatures.

03 NGIPS sends Threat Analysis Engine the suspicious files transferred in the traffic.

04 Using the both the static and virtual execution engines, an in-depth analysis of the dynamic execution behavior of the software is performed to determine if it is malicious or benign.

05 The Threat Analysis Engine compiles threat intelligence data about detected malware and sends it to NGIPS, which will then take action such as blocking the malicious traffic.

## CONCLUSION

Defending the modern enterprise has evolved into a complex problem requiring multiple technologies that can inspect traffic and content. The NSFOCUS NGIPS and Threat Analysis Engine provide the enhanced protection needed to deal with the problems of modern malicious static and active content that flows across the network.