# Cyber Threat Analysis and Management

## KEY BENEFITS

- Identify infections earlier, allowing proactive intervention before major problems appear
- Define the correct mitigation strategy and select from the most surgical policies
- Gain visibility on actions preceding the attacks: What happened in the network during the attack? Where are the attacks coming from? How policy changes were able to mitigate the impact on the attack traffic?
- Prevent attacks with the ability to apply policies inline to do real-time mitigation and block malicious attacks on your network and ultimately to your subscribers

**Network Operators are (and have always been) targets of choice for cyber criminals and they will continue to be for a long time. Being builders and operators of critical infrastructures and hosting a large customer base, service providers are seeing attacks targeting their networks and subscribers growing in volume and complexity year over year.**

Here are some challenges that service providers face:

- The outcomes of a single major failure impacting their services can affect millions of subscribers
- The skillset required to launch a cyber-attack is prevalent
- Launching an attack can be done at a low cost and can still trigger a significant monetary benefit
- Multiple motivations supporting an attack including political and geopolitical factors

With applications moving into the cloud and virtualization on the rise, security perimeter devices like firewall and intrusion detection/prevention systems are not enough to protect data center infrastructure.

Increasingly sophisticated cyber activities have far-reaching implications on network infrastructure, services, customer experience, and brand reputation.

Service providers leave themselves vulnerable to cyberattacks by not addressing these day-to-day threats and infected devices. The infected devices also act as agents to launch attacks unknown to the end user. Visibility into these issues is imperative.

As a result, service providers need new insights to operate more efficiently.

## SOLUTION OVERVIEW

Sandvine’s Cyber Threat analysis and Management Use Case allows service providers to manage these security challenges and maintain high network QoE. The Cyber Threat Analysis Use Case delivers two key components in building actionable cyber threat intelligence: it collects near real-time information from the network, and provides trends and analytics with crucial insights that enable service providers and security specialists to choose the best approach in defining long term strategies.

Sandvine has the ability to extract Cyber Threat Indicators  that are part of the Crowdstrike threat database, and detect and mitigate volumetrics and connection-related DDoS style attacks.

The Cyber Threat Management inline Use Case adds to these capabilities the ability to execute real time mitigation policies to block malicious attacks, and therefore protect subscribers from a range of network threats and malicious traffic that can compromise equipment and data.

This Use Case offers three essential views:

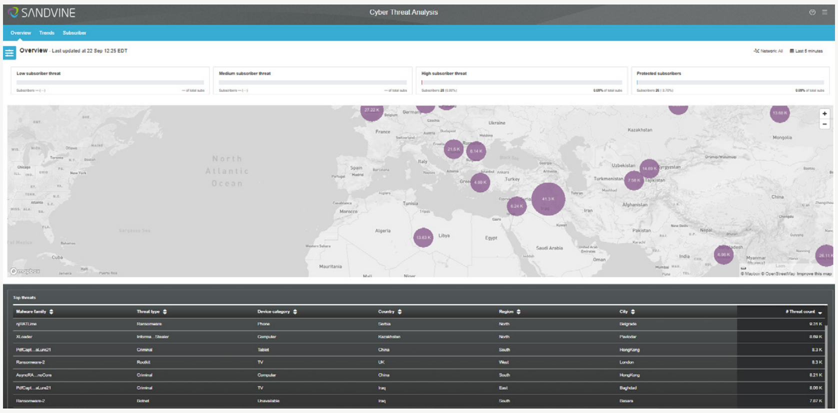
- The overview dashboard
- The trends dashboard
- The subscriber dashboard

## Overview Dashboard

- Shows a worldwide map view of where threats are originating, including a table sorted by the highest number of threats
- Allows for the selection of specific threat categories, devices, and locations using global filters

**Figure 1**

Cyber Threat Overview



Overview - Last updated at 22 Sep 12:25 EDT

Top threats

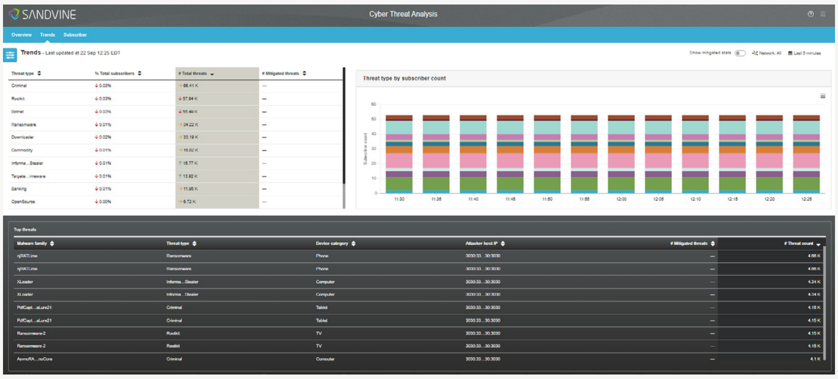
| Malware family | Threat type | Device category | Country | Region | City | # Threat count |
|---|---|---|---|---|---|---|
| njRATLime | Ransomware | Phone | Serbia | North | Belgrade | 9.31 K |
| XLoader | Informa...Stealer | Computer | Kazakhstan | North | Pavlodar | 8.69 K |
| PdfCapt...aLure21 | Criminal | Tablet | China | South | HongKong | 8.3 K |
| Ransomware-2 | Rootkit | TV | UK | West | London | 8.3 K |
| AsyncRA...noCore | Criminal | Computer | China | South | HongKong | 8.21 K |
| PdfCapt...aLure21 | Criminal | TV | Iraq | East | Baghdad | 8.06 K |
| Ransomware-2 | Botnet | Unavailable | Iraq | South | Basara | 7.87 K |

## Trends Dashboard

- Provides details on threat types and a trend view of the threats over time
- Statistics on mitigated treats (with Cyber Threat Management)

**Figure 2**

Cyber Threat Trends



Trends - Last updated at 22 Sep 12:25 EDT

| Threat type | % Total subscribers | # Total threats | # Mitigated threats |
|---|---|---|---|
| Criminal | ↓ 0.03% | → 66.41 K | — |
| Rootkit | ↓ 0.03% | ↓ 57.94 K | — |
| Botnet | ↓ 0.03% | ↓ 55.49 K | — |
| Ransomware | ↓ 0.01% | → 34.22 K | — |
| Downloader | ↓ 0.02% | → 33.19 K | — |
| Commodity | ↓ 0.01% | → 16.82 K | — |
| Informa...Stealer | ↓ 0.01% | ↑ 16.77 K | — |
| Targete...imeware | ↓ 0.01% | ↑ 13.92 K | — |
| Banking | ↓ 0.01% | → 11.95 K | — |
| OpenSource | ↓ 0.00% | → 6.72 K | — |

Top threats

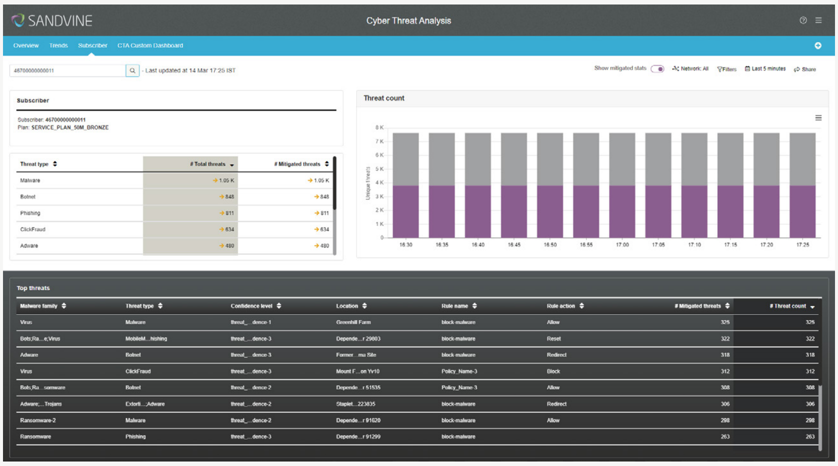
| Malware family | Threat type | Device category | Attacker host IP | # Mitigated threats | # Threat count |
|---|---|---|---|---|---|
| njRATLime | Ransomware | Phone | 3030:33...30:3030 | — | 4.66 K |
| njRATLime | Ransomware | Phone | 3030:33...30:3030 | — | 4.66 K |
| XLoader | Informa...Stealer | Computer | 3030:33...30:3030 | — | 4.34 K |
| XLoader | Informa...Stealer | Computer | 3030:33...30:3030 | — | 4.34 K |
| PdfCapt...aLure21 | Criminal | Tablet | 3030:33...30:3030 | — | 4.15 K |
| PdfCapt...aLure21 | Criminal | Tablet | 3030:33...30:3030 | — | 4.15 K |
| Ransomware-2 | Rootkit | TV | 3030:33...30:3030 | — | 4.15 K |
| Ransomware-2 | Rootkit | TV | 3030:33...30:3030 | — | 4.15 K |
| AsyncRA...noCore | Criminal | Computer | 3030:33...30:3030 | — | 4.1 K |

## Subscriber Dashboard

- Provides detailed threat information on individual subscribers and views on trends over time

**Figure 3**

Cyber Threat – Subscribers



46700000000011 - Last updated at 14 Mar 17:25 IST

Subscriber

Subscriber: 46700000000011
Plan: SERVICE_PLAN_50M_BRONZE

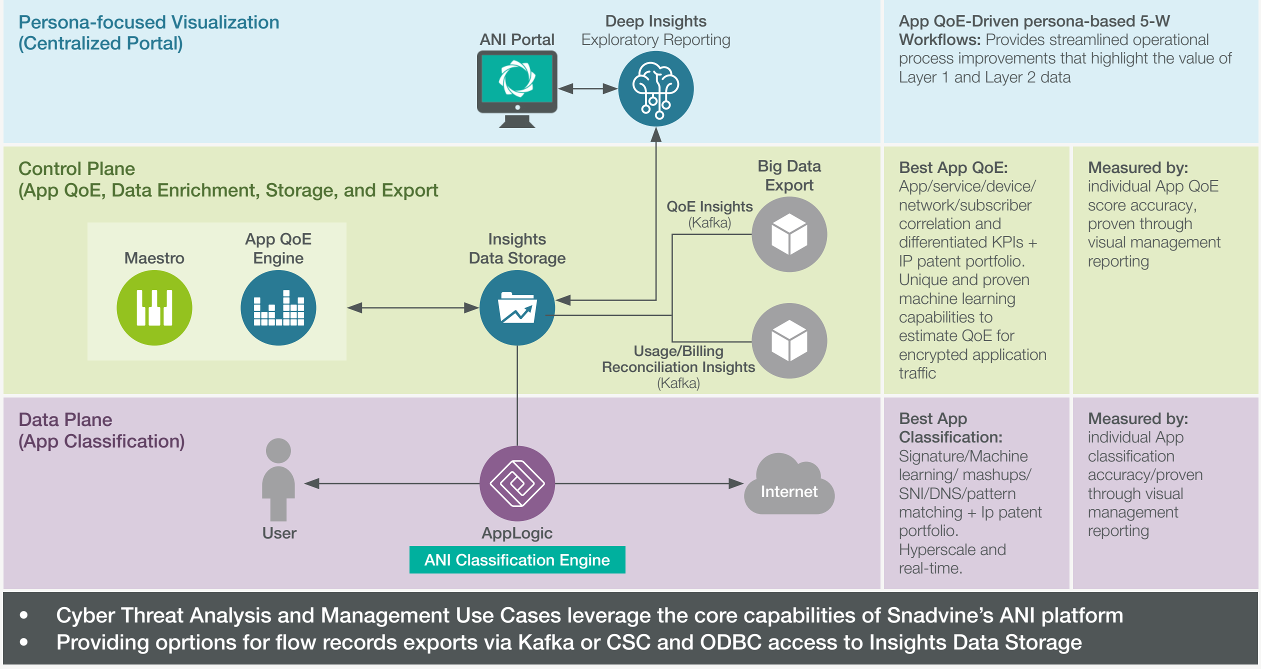
| Threat type | # Total threats | # Mitigated threats |
|---|---|---|
| Malware | → 1.05 K | → 1.05 K |
| Botnet | → 848 | → 848 |
| Phishing | → 811 | → 811 |
| ClickFraud | → 634 | → 634 |
| Adware | → 480 | → 480 |

Top threats

| Malware family | Threat type | Confidence level | Location | Rule name | Rule action | # Mitigated threats | # Threat count |
|---|---|---|---|---|---|---|---|
| Virus | Malware | threat_...dence-1 | Greenhill Farm | block-malware | Allow | 325 | 325 |
| Bots;Ra...e;Virus | MobileM...hishing | threat_...dence-3 | Depende...r 29803 | block-malware | Reset | 322 | 322 |
| Adware | Botnet | threat_...dence-3 | Former...ma Site | block-malware | Redirect | 318 | 318 |
| Virus | ClickFraud | threat_...dence-3 | Mount F...on Yv10 | Policy_Name-3 | Block | 312 | 312 |
| Bots;Ra...somware | Botnet | threat_...dence-2 | Depende...r 51535 | Policy_Name-3 | Allow | 308 | 308 |
| Adware;...Trojans | Extorti...;Adware | threat_...dence-2 | Staplet...223835 | block-malware | Redirect | 306 | 306 |
| Ransomware-2 | Malware | threat_...dence-2 | Depende...r 91620 | block-malware | Allow | 298 | 298 |
| Ransomware | Phishing | threat_...dence-3 | Depende...r 91299 | block-malware |  | 263 | 263 |

Figure 4

Cyber Threat – Architecture



**App QoE-Driven persona-based 5-W Workflows:** Provides streamlined operational process improvements that highlight the value of Layer 1 and Layer 2 data

**Best App QoE:** App/service/device/ network/subscriber correlation and differentiated KPIs + IP patent portfolio. Unique and proven machine learning capabilities to estimate QoE for encrypted application traffic

**Measured by:** individual App QoE score accuracy, proven through visual management reporting

**Best App Classification:** Signature/Machine learning/ mashups/ SNI/DNS/pattern matching + Ip patent portfolio. Hyperscale and real-time.

**Measured by:** individual App classification accuracy/proven through visual management reporting

- Cyber Threat Analysis and Management Use Cases leverage the core capabilities of Snadvine's ANI platform
- Providing oprtions for flow records exports via Kafka or CSC and ODBC access to Insights Data Storage

## REQUIRED SOLUTION COMPONENTS

- ActiveLogic
- ContentLogic
- Maestro Policy Engine
- Deep Insights
- Elements

## ABOUT SANDVINE

Sandvine's cloud-based Application and Network Intelligence portfolio helps customers deliver high quality, optimized experiences to consumers and enterprises. Customers use our solutions to analyze, optimize, and monetize application experiences using contextual machine learning-based insights and real-time actions. Market-leading classification of more than 95% of traffic across mobile and fixed networks by user, application, device, and location creates uniquely rich, real-time data that significantly enhances interactions between users and applications and drives revenues. For more information visit **http://www.sandvine.com** or follow Sandvine on Twitter **@Sandvine**.

SANDVINE

The App QoE Company

**USA**
5800 Granite Parkway
Suite 170
Plano, TX 75024
USA

**EUROPE**
Neptunigatan 1
211 20, Malmö
Skåne
Sweden
T. +46 340.48 38 00

**CANADA**
410 Albert Street,
Suite 201, Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

**ASIA**
Arliga Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333

This documentation, including all documentation incorporated by reference herein such as documentation provided or made available on the Sandvine website, are provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Sandvine Corporation and its affiliated companies ("Sandvine"), and Sandvine assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect Sandvine proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of Sandvine technology in generalized terms. Sandvine reserves the right to periodically change information that is contained in this documentation; however, Sandvine makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.