SANDVINE

Cyber Threat Analysis and Management

Identify, quantify, and protect subscriber QoE from cyber threats

KEY BENEFITS

- Creates an additional layer on top of basic device protection offered by OS/applications
- Detects evolving behavior of complex malware through known communication pattern/protocol between devices and abnormal traffic patterns
- Monitors and observes the infectious communication where attacks involve multiple devices
- Perform actions (block) on infected traffic, and can apply rules on in-line traffic upon detection of malicious activity

MARKET OVERVIEW

Cyber threats continue to evolve and rise in frequency, making it increasingly challenging for service providers to protect the network from malicious and organized cyber criminals. With the proliferation of smart devices (including IoT), the globalization and cloudification of business critical applications create more network entry points to exploit.

Public service providers are prime targets for cyber-attacks, as they provide the backbone of information exchange for businesses and consumers. Bandwidth and session targeted attacks are growing exponentially, directly impacting network quality of experience (QoE). The threat originators or actors, who are involved in distributing malware through various websites, or phishing for personal information from unsuspecting victims, are taking advantage of blurred physical distances on the internet, which makes cybersecurity a game of hide-and-seek.

In most cases, cybersecurity teams are aware of these attacks due to increased activity, but don't specifically know which hosts and locations are involved in the attack. However, most security solutions used for identifying and quantifying cyber activity lack the necessary network visibility and contextual awareness, which is arguably the biggest challenge facing security professionals.

With applications moving into the cloud and virtualization on the rise, security perimeter devices like Firewall and IDS/IPS are not enough to protect data center infrastructure. IoT is not just another attack vector. The number of devices involved, and lack of any built-in security stack make them highly vulnerable and their exposure to network threats is much higher than other devices.

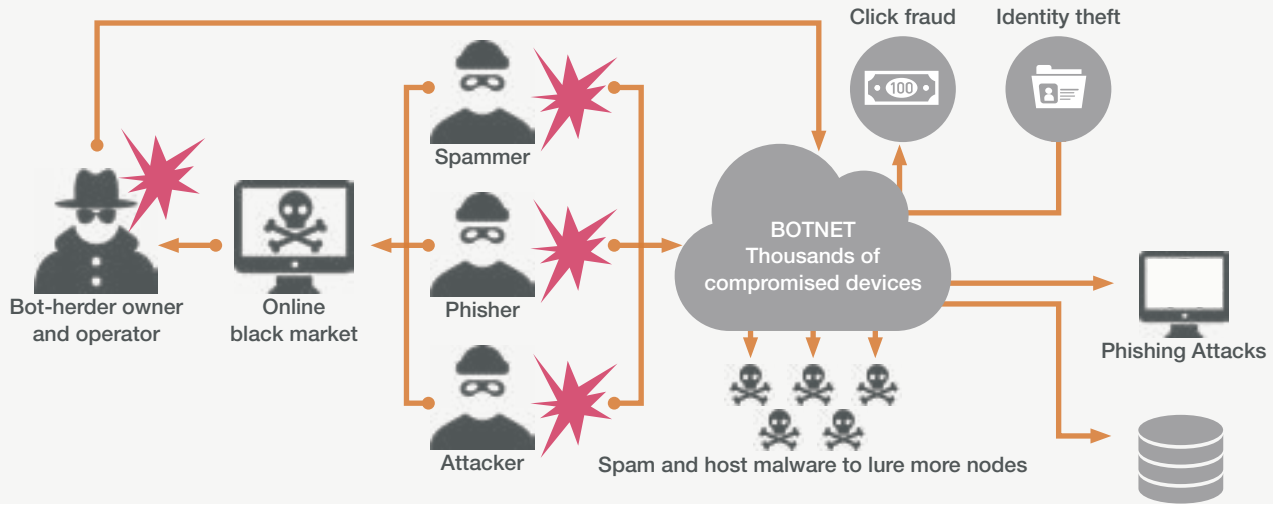
Service providers leave themselves vulnerable to cyberattacks by not addressing the day to day threats and infected devices. The infected devices also act as agents to launch attacks unbeknownst to the end user, as shown (**Figure 1**).

Major cyberattacks have a two-sided cost, direct and indirect. Studies suggest that indirect costs such as public reputation, far outweigh the monetary cost of outages. Service providers need a solution that allows them to proactively detect and mitigate potential attacks and manage ongoing threats to maintain a safe and high network quality of experience (QoE).

Cyber Threat Analysis and Management

Figure 1

Cyber Threat Challenges: an army of infected user devices with internet connectivity (PCs, Phones, Tablets, Machines, Sensors), used by criminals to conduct malicious activities



USE CASE OVERVIEW

Sandvine Security and Cyber Threat use case allows service providers to manage the security challenges and maintain high network QoE. It consists of two use cases: The Cyber Threat Analysis use case and the Cyber Threat Management use case providing comprehensive analytics and real-time protection to cyber threats respectively.

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. Using Sandvine's real-time data and analytics reporting interfaces, security teams can monitor and analyze malicious traffic, and the sources threatening network users and resources, such as botnet traffic, and active connections related to phishing scams and malware infections.

Positioned in the network protection domain, the Cyber Threat Management use case adds to these capabilities the ability to execute real time mitigation policies to block malicious threats, and therefore protect subscribers from a range of network threats and malicious traffic that can compromise equipment and data. The Cyber Threat Management use case analyzes and solves security challenges on fixed and mobile network environments. Sandvine's Application and Network Intelligence solution identifies and acts on malicious activity, applying network policies in real time to protect subscribers and networks.

Cyber Threat Analysis and Cyber Threat Management key capabilities

Both use cases are built on Sandvine's industry-leading application identification, inspecting all network traffic regardless of the network scale, and augmenting it with a third-party database for security-specific categorization of malicious traffic. The use case is further enriched by the industry's most trusted IP geolocation database so that service providers can correlate local users with the source of malicious attacks to feed mitigation decisions.

Detection and Classification of Threats

Using the ContentLogic Cyber Threat Intelligence Database for detection of more than 40 threat types and enrichment with classification metadata for:

- Real-time matching of flow performed against multiple parameters including: URL, hostname, TCP/UDP port, protocol type and subnet

Cyber Threat Analysis and Management

- Historical usage, measurements, and dimensions, including threat category, devices involved, location, and QoE
- Real-time activity monitoring
- Asymmetric traffic threat detection

Malware Classification

Categorization and grouping are available in both use cases, providing visibility to the phases of an adversary attack lifecycle (cyber kill chain, MiTRE Attack) and adapting the responses accordingly.

Malware metadata available includes:

- Threat Type
- Threat Name
- Threat Confidence
- Threat Target
- Threat actors
- Threat Kill chain
- Threat MiTRE Attack

Location properties for each flow, indicate the location (i.e., country, region, city, ISP, ASN, and latitude/longitude) of the remote hosts communicating with users (GeoLogic).

Reporting and Visualization

The Cyber Threat Analysis and Cyber Threat Management use cases are visualized from the rich data collected by ActiveLogic and stored within Insights Data Storage. Service providers can see actions preceding the attacks, what happened in the network during the attack, where the attacks are coming from, and how policy changes were able to mitigate the impact of the attack traffic. They can then measure the impact of malicious traffic on QoE, and detail which devices were involved or impacted by the attack. This intelligence is critical to detecting the correct mitigation strategy and selecting the most surgical policies.

Both use cases are also integrated with the ANI Portal and visualized via dedicated dashboards providing Information specific to the top threats detected. The overview panel (**Figure 2**) presents statistics on any Low, Medium and High subscriber threats detected. When the Cyber Threat Management license is active, information also includes data related to protected subscribers.

Figure 2

Cyber Threat Overview Panel

Cyber Threat Analysis and Management

Threat location map

The threat location map panel displays a global map with threat locations identified by city, region, and country (**Figure 2**). The map panel allows users to zoom in and out on specific locations to display the total number of threats in a cluster.

Cluster size may differ on various locations as the size depends on the total number of threats. The map cluster supports a tooltip feature, which displays a total threat count for the single or multiple locations present in that cluster.

Top threats

The top threats data grid panel displays:

- Threat count
- Malware family
- Threat type
- Device category
- Country
- Region
- City

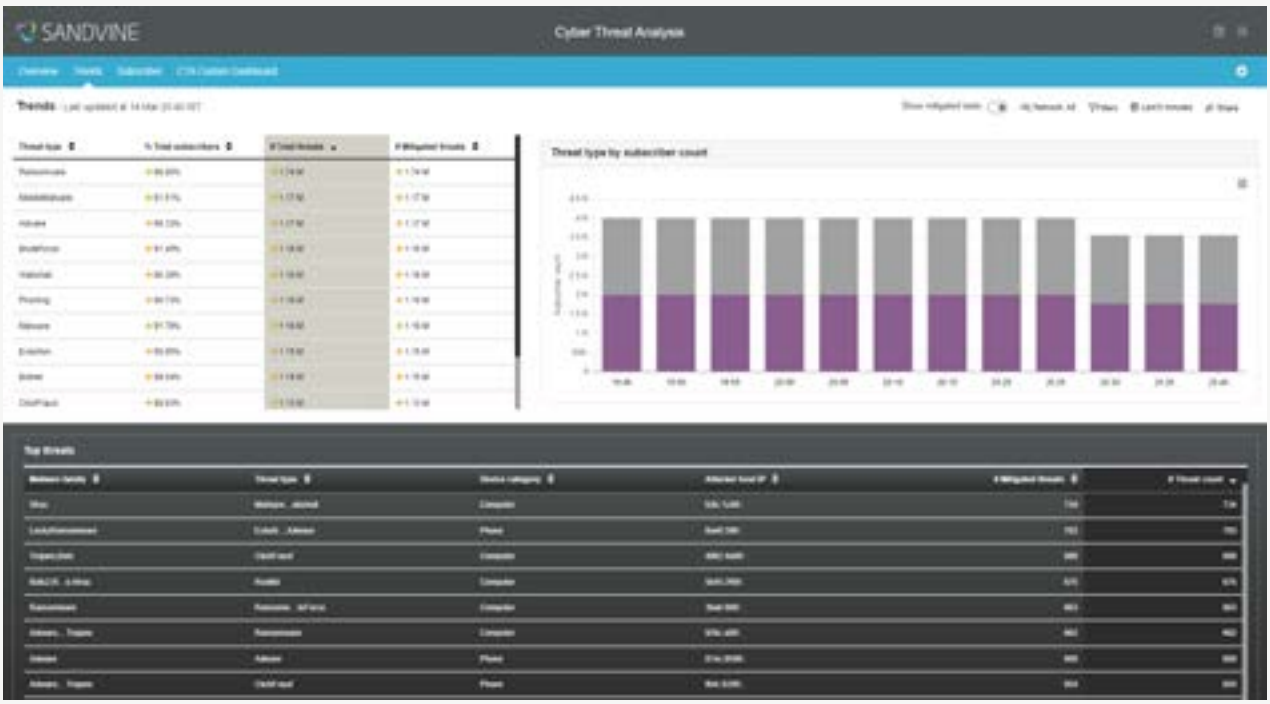
Trends Dashboard

The Trends dashboard provides visualization of trends of different threat types. The user can change network, global, and time filters or select filtering capability by access technologies (e.g., slice, slice type, device connectivity, and access connectivity)

With the Cyber Threat Management use case, a supplementary field provides users information on the number of mitigated threats (**Figure 3**).

Figure 3

Cyber Threat Management - Trends Dashboard



Cyber Threat Analysis and Management

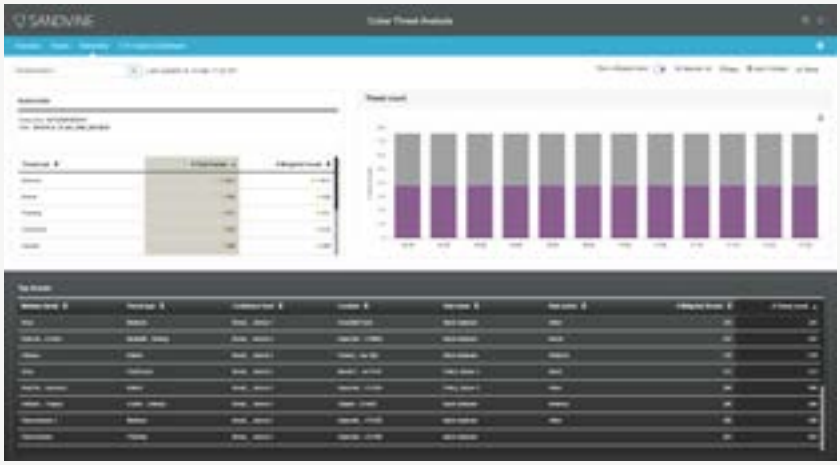
Subscriber Dashboard

The Subscriber dashboard provides detailed information on threats impacting individual subscribers with trends over a selectable period of time.

With the Cyber Threat Management use case, a supplementary field provides users information on the number of mitigated threats for the subscriber (**Figure 4**).

Figure 4

Cyber Threat Management - Subscriber Dashboard



Service providers that implement Sandvine's Security and Cyber Threat use case can benefit from reduced operational costs associated with user-based security issues. Specifically, by reducing user infection rates, service providers experience fewer support calls and reduced network impact from malware. Service providers can protect themselves from major attacks by identifying infections earlier, blocking them, spotting infected devices, and taking proactive steps such as contacting users whose devices are affected and assisting them with a remediation process.

Ultimately, this use case provides users with peace of mind and allows service providers to maintain a good network QoE, preventing future security-related costs and customer churn.

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