N1000 Network Security Appliance

## For Visibility into Malware and Unknown Threats in Email, Web & File Transfers

The N1000 performs comprehensive inspection and classification of files in email, web and file transfer network traffic. It extracts and stores information on files in near real-time. The N1000 accelerates breach response with analysis of all unknown and malicious payloads as well as provides historical visibility with network context. The system enables customers to define and deploy custom detection rules to identify new threats based on new threat intelligence to counter malware attacks before damage occurs.

Key Benefits

- **Exceptional scale and coverage** of analyzed content at millisecond speed.

- **Provides visibility across unknown threats** in files from HTTP, SMTP and FTP traffic.

- **Identifies more than 3500 file formats** while classifying files "in flight" before they execute.

- **Performs "retro-detection"** by continually checking reputation on past files and alerting on status changes.

- **Enables hunting** with ReversingLabs or customer supplied YARA rules.

- **Integrates seamlessly with SIEM and analytics platforms** to supply rich file analysis data and reports.

- **Scales to high volume and deeper analysis** with TitaniumScale Enterprise Scale File Analysis for high-volume analysis, A1000 Malware Analysis Platform for deeper malware analysis & hunting, and T1000 File Reputation Appliance for on-premises privacy.

The N1000 utilizes unique ReversingLabs' File Decomposition technology to derive detailed internal threat indicators. File Decomposition enables deep file inspection at speeds that are orders of magnitude faster than sandbox products. This allows the N1000 to extract and classify all major file formats from the network stream in near real-time. File classification utilizes up-to-date intelligence from ReversingLabs' industry-leading File Reputation Service with a powerful rules engine to assign threat levels, names and types. The results are made available through an integrated GUI and/or customer SIEMs and analytics platforms such as Splunk and Elasticsearch for further action.

N1000 Network Threat Visualization

The N1000 enables users to view file events, access file summary and detail information, see file network context (e.g. source, destination), search by file attributes and customize threat detection with custom YARA rules.
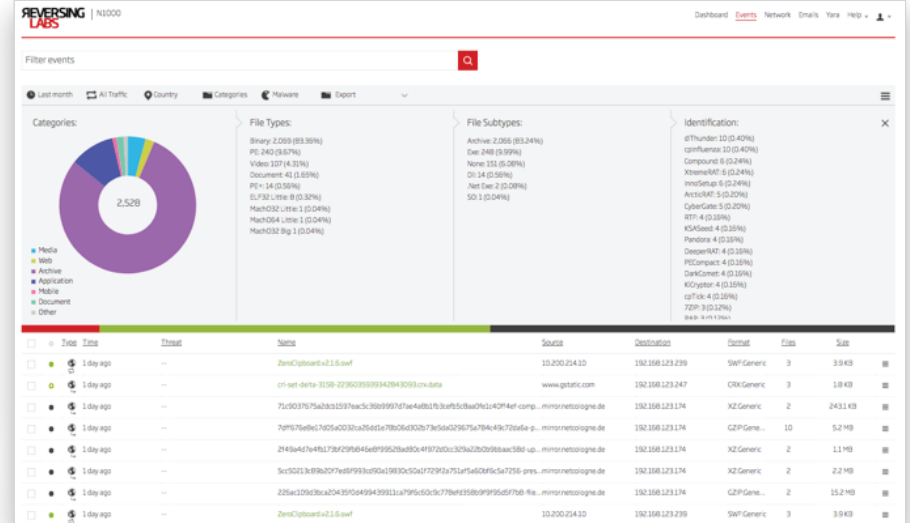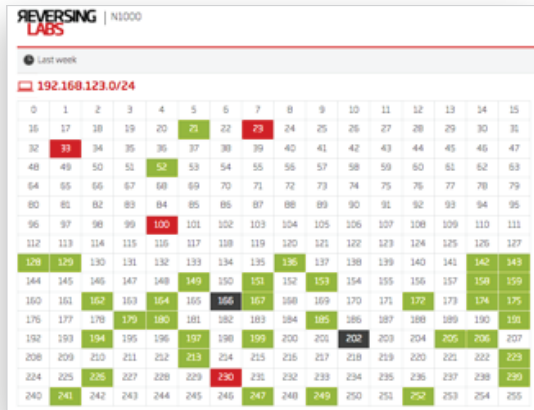
N1000
Network Threat Detection, Classification and Hunting

The N1000 performs real-time classification and analysis of files in network traffic. With the optional TitaniumScale, the N1000 can be configured for even higher throughput applications. The information derived by the N1000 from files of interest are used to generate reports to SIEM and analytics platforms and can be automatically fed to an A1000 Malware Analysis Platform for deeper analysis.
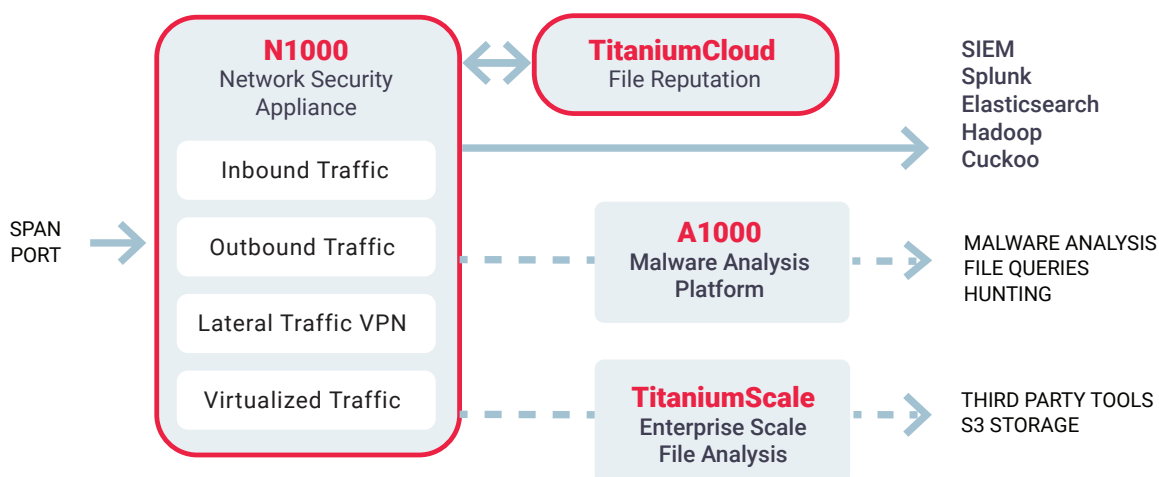
Key N1000 Features

Network File Reputation and Analysis

- Connects to SPAN port to monitor all files traversing the network
- Analyzes files from HTTP, FTP and SMTP traffic in near real-time
- Processes files up to 400MB (default)
- Exceeds sandbox file processing in coverage & volume

Threat Classification of Extracted Files

- Uses unique File Decomposition (FD) technology to assess and classify files in near real-time
- Inspects over 350 file types across platforms including Windows, Linux, Mac OS, Android, iOS, documents and media files
- Reports on file activity per source, destination or file type
- Checks TitaniumCloud file reputation service for whitelisted and blacklisted content

Delivered as

- Hardware based or virtual machine

Identification of Zero Day/Advanced Threats

- Recognizes polymorphic attacks by identifying functional similarity to known malware
- Applies your custom YARA rules to all files defined for threat calculation

Enterprise Data Integration

- Integrates file analysis logs and threat detections with SIEM or "Big Data" solutions
- Saves files of interest via TitaniumScale or T1000
- Includes Web GUI for monitoring, configuration and reporting

ReversingLabs Integration

- Integrates with TitaniumScale for high volume applications
- Provides input to the A1000 Malware Analysis Platform for deeper analysis and hunting
- Connects to the T1000 File Reputation Appliance for privacy and air-gapped environments

REVERSINGLABS

Worldwide Sales : +1.617.250.7518

sales@reversinglabs.com