Seculert
Advanced Threat Protection

AUTOMATIC TRAFFIC LOG ANALYSIS

APTs, advanced malware and zero-day attacks are designed to evade conventional perimeter security defenses. Today, there is wide agreement that even with the best signature-based security solutions available, advanced malware is still getting through the door. In response, IT organizations are transitioning from prevention to detection. They are using a combination of technology and professional services to identify attacks in progress by analyzing traffic logs. While traffic log analysis does reveal malware activity, the manual, on-premises approach is slow, incomplete, and expensive.

Today, Seculert is leveraging the capabilities of the cloud to perform accurate Traffic Log Analysis quickly and cost-effectively. Using Big Data analytics and advanced machine learning algorithms, Seculert automatically analyzes traffic logs and identifies malware attacks – even malware that was previously unknown to any authority. Working in synergy with the Elastic Sandbox Environment and Botnet Interception, and leveraging crowd-sourced information from customers and vendors all over the world, Seculert Traffic Log analysis discovers even the most devious malware.

Seculert is a comprehensive cloud-based solution for protecting organizations from advanced malware, APTs and zero-day attacks. Seculert combines several key detection and protection technologies – an Elastic Sandbox environment, Botnet Interception, and Traffic Log Analysis - in one simple solution that proactively identifies new threats as they emerge.

ANALYZING HTTP/HTTPS TRAFFIC LOGS COLLECTED OVER TIME

Because of the persistent nature of advanced threats, it is essential to study HTTP/HTTPS traffic logs collected over an extended period of time and Seculert offers this capability by enabling customers to upload their HTTP/HTTPS traffic logs to the Seculert cloud. The logs can be uploaded either via the web dashboard or by the RESTful API

Since the threats are networked, it is important to process logs at the level of the user, the department, the organization, the industry and the region. Performing this type of analysis requires a great deal of memory and CPU as well as access to logs from other companies and security vendors. It simply isn't feasible for inline security solutions such as proxies, IPS, IDS and firewalls. They do not have the memory or processing power, and they do not have access to the requisite variety of external information sources.

HARNESSING THE POWER OF BIG DATA ANALYTICS

Traffic log analysis is only as effective as the expertise that it embodies. Seculert's malware experts work together with experts in statistical analysis and Big Data analytics to create the malware profiles and adopt machine learning algorithms that power Seculert's traffic log analysis. Even in the cloud, the requisite statistical analysis of big data is very challenging. Today's statistical packages generally assume that the data set can fit in the memory of one computer. Seculert has developed proprietary techniques for performing scalable machine learning using Hadoop and Amazon's elastic map reduce.

IDENTIFYING MALWARE PROFILES

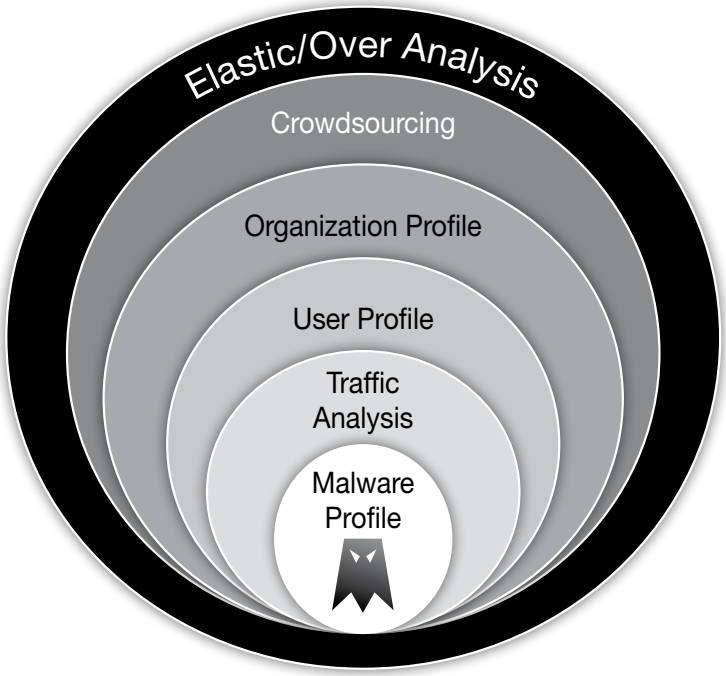
A critical stage in traffic log analysis is defining a malware profile. A profile is a vector derived from a "learning set" of behaviors. Seculert's Elastic Sandbox and Botnet Interception modules provide unique learning sets that include many features (some of which are statistical moments) that represent a thorough picture of how a particular malware behaves in a wide variety of situations such as uploading data, performing remote access and sending email. From the learning set, Seculert classifies malware behavior and create a profile that is used by the machine learning algorithms during traffic log analysis.

THE POWER OF MACHINE LEARNING

Malware profiles are a critical input for log analysis but they are not enough to identify malware. Because malware is evolving and new malware is appearing all the time, Seculert uses very sophisticated Machine Learning algorithms to examine statistical features, classify the traffic and determine whether it is similar to any of the known malware profiles.

MACHINE LEARNING DATA LAYER CORRELATION

Sometimes, Traffic Log Analysis can identify malware conclusively based on existing profiles. But due to the evolving nature of malware, it is not always enough. Seculert's machine learning algorithm processes additional data such as domain and IP reputation, Domain Generation Algorithm detection and botnet traffic correlation. It then isolates the suspicious activity into a channel and correlates it with additional data layers.



User and Organizational Data Layers

To confirm the presence of malware, Seculert automatically correlates the suspicious channel with a larger data set of user activity to classify features such as location, working hours, and websites visited. If the correlation is low, it is a feature that can indicate an activity with a malicious intent.

Next, the platform looks at the channel in the context of the behavior of the entire organization. If there is a high probability that the channel is an outlier in comparison to the organization, that is another factor that can indicate a malicious intent. For example, usually the organization communicates with Europe and North America, so communication with China is an outlier.

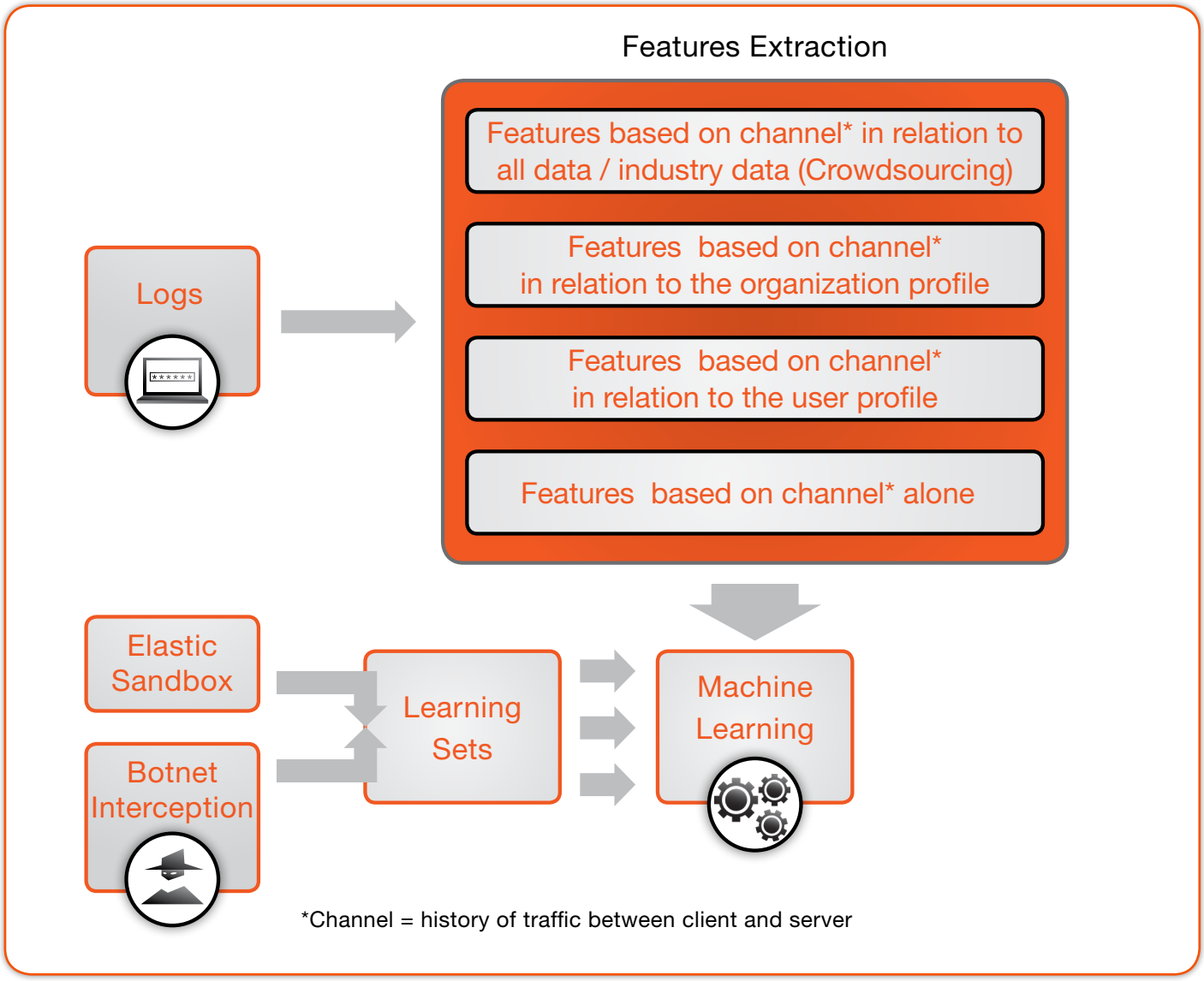
Both of these calculations are very heavy and involve processing a large amount of user and organizational data collected over a significant period of time. The Seculert platform is capable of handling the calculation because it is running in an elastic cloud environment.

Crowdsourcing and the Community Data Layer

Last but not least, Seculert correlates the channel with usage data from organizations around the world. A high correlation between the industry and the channel indicates a higher probability of malware. This is essential for identifying targeted attacks. For example, if a mildly suspicious server is accessed only from the energy industry, that is a significant factor.

Seculert is able to perform this crucial step because it is an independent platform with access to terabytes of botnet traffic and customer logs each month. Our customer logs come from the full range of security devices and vendors, giving Seculert a uniquely broad perspective on the threat landscape.

HOW TRAFFIC LOG ANALYSIS WORKS



1. Customers upload log files to the Seculert Traffic Log analysis module using the dashboard or API.
2. Machine learning algorithms process the traffic logs. If they identify suspicious traffic, they isolate it into a channel.
3. The features of the channel are analyzed in relation to the user's activity profile, the organization's activity profile, and the industry/regional activity profile.
4. All of the channel's features are processed in the context of unique learning sets (malware profiles) derived from the Elastic Sandbox and Botnet Interception modules.
5. If malware is conclusively detected, Seculert updates you immediately via the dashboard and the Protection API, which communicates directly with proxies and firewalls to block known threats.
6. Seculert also analyzes historical traffic log files to identify the initial point of infection and downloads the original malware to the Elastic Sandbox Environment for further analysis and profiling.
7. If the malware is determined to be a botnet, the data is also passed on to the Botnet Interception module, which monitors traffic and identifies infected users and IP addresses. All Seculert customers and partners are also notified via the dashboard and API.

ASSURING THE PRIVACY OF YOUR DATA

While the cloud offers the elastic processing power and storage capacity necessary for effective log analysis, it is essential to protect your data in the cloud. Seculert relies on the world class standards and processes provided by Amazon S3 to ensure that your confidential log data is protected while it's in transit, and while it's being stored for analysis.

What Data is Transmitted?

To optimize your security, your organization would upload the following log data to Seculert either manually or automatically:

- Timestamp (Date + Time) of the request
- Machine identifier - Client IP
- HTTP Request Method (GET/POST/etc.)
- HTTP Request URI Host
- HTTP Request URI Path
- HTTP Request URI Query string
- HTTP User-Agent
- HTTP Request Referrer (optional)

Seculert immediately begins the Big Data analysis process as soon as your logs are uploaded, and stores them for a week. This is done to look beyond real time or close to real time, and allow Seculert to correlate the different events into one threat.

Amazon S3 Standards and Processes

Seculert relies on the world class standards and processes provided by Amazon S3 to ensure that your confidential log data is protected while it's in transit, and while it's being stored for analysis. With Amazon S3's data protection features, your data is protected from both logical and physical failures, and from data loss as a result of unintended user actions, application errors, and infrastructure failures.

Amazon has S3 data centers both in the US and in EU (Ireland). You can also upload your data to a particular region via a specific FTP domain name that will be provided to you upon request (e.g. eu.ftp.sense.seculert.com).

Industry-Standard Compliance & Certifications

Seculert adheres to industry-standard compliance requirements, and has earned an array of certifications that verify our competence and professionalism. These standards and certifications include:

- PCI
- HIPPA
- ISO27001
- SAS70
- FISMA

Securing Your Data in Transit

Your organization's logs are uploaded to the "Log Analysis" secure environment via Secure FTP (FTPS), SFTP or Syslog to ensure strong encryption (AES-256). Seculert employees do not have access to your data at any time.

Securing Your Data in Storage

Your data is stored on Amazon S3, and features multiple access control mechanisms and security layers, including:

- physical security
- access security to define and grant granular access permissions
- multiple options for encrypting data, either via Amazon's server-side encryption or manage your own encryption using client-side

Only you and the Seculert system will have access to your resources.

Securely Removing Your Data

After storing your logs for one week to detect any advanced threats, your data is securely and completely removed.

Access to Your Data

Access to your data is strictly limited to you, and to select and authorized Seculert employees. In addition, your explicit authorization will be required before any Seculert employee accesses your UI screens in order to provide requested technical support. At all times, data access is securely handled and fully tracked.

Seculert: Security is our Only Focus

At Seculert, we don't juggle multiple products that achieve different business goals. We focus on one thing, and only one thing: our customers' security.

And so it should come as no surprise that to learn that Seculert has the proven data protection systems, technologies, processes and resources in place to keep your data secure at all times – whether in transit or while being stored.

After all, keeping you safe in an increasingly complex and challenging malware threat environment isn't just our mission and our specialization. It's the essence of who we are and what we do – without compromise.

AUTOMATED PROTECTION API

To make the most of Traffic Log Analysis, you can integrate it with your existing security infrastructure using the Seculert Protection API. The API features two simple interfaces for accessing and retrieving data:

- A web request that uploads files via HTTP, followed by a response including the files' identification key.
- A request that retrieves the results of the analysis using the identification key.

When malware is detected by the Elastic Sandbox, Seculert customers are notified immediately. The API can communicate directly with corporate firewalls and proxies to block traffic. To support complete forensics, threat detection data can also be sent to SIEM systems for correlation. Some additional examples of integration include:

- A mail server plug-in that automatically uploads suspicious attachments to the Elastic Sandbox.
- An anti-virus integration that inspects quarantined files to determine their severity in order to prioritize remediation activities.

SECULERT DASHBOARD

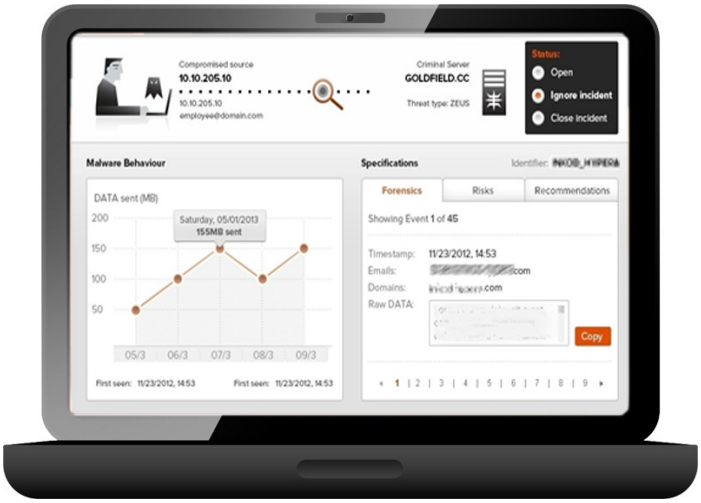
The Seculert Dashboard gives you a complete picture of all of the users and IP addresses that are infected by malware.

After any attack is detected, customers receive a detailed report so that customers can understand and mitigate their exposure and modify their security policies as needed. The compromised computer will be identified by source IP, threat type, crime server, raw data of the logs and the time and date of the transmission. All relevant transmissions from the source to the crime server will be grouped together.

The dashboard automatically indicates all infected users and endpoints detected through Traffic Log Analysis

The malware behavior is displayed in a graph and shows the daily number of transmissions or the size of the uploaded data.

Separate tabs are available that offer information on the risks and recommendations for remediation.



Seculert's Detailed Incident Dashboard Report

SYNERGISTIC TECHNOLOGIES

Seculert's Traffic Log Analysis is extremely powerful – but it is the combination of the Big Data analytics and machine learning working together with all of Seculert's core technologies that provides the key to successful advanced Threat Protection. In addition to the Traffic Log Analysis, Seculert features:

- Botnet interception to detect threats that are already attacking employees, partners and customers inside and outside your organization.
- Elastic sandbox environment to execute and study suspicious code for as long as necessary in order to profile it.
- Protection API to automatically stop identified threats through integration with perimeter defenses.
- Big Data analytics analyzes tens of thousands of malware profiles daily as well as petabytes of traffic logs in order to detect APTs.
- Machine learning technology identifies unknown malware based on an understanding of malware behavior in order to keep up with the volume and rate of change.
- Intuitive dashboard puts instant information about all advanced threats at your fingertips.
- Full coverage of remote and mobile users on all endpoints including BYOD - without installing a single appliance or endpoint solution.
- Cost-effective cloud service means no installation, instant results, and low total cost of ownership

LICENSING

Traffic Log Analysis is free however full detailed reports are limited. In order to learn more about pricing please contact us.

SECULERT
6 Efal Street, Petach Tikva, Israel.
Tel: +972-3-9193366
Tel (US): +1-718-305-7067
Tel (UK): +44 (0) 203-468-1234
info@seculert.com

Seculert
Advanced Threat Protection

Follow us