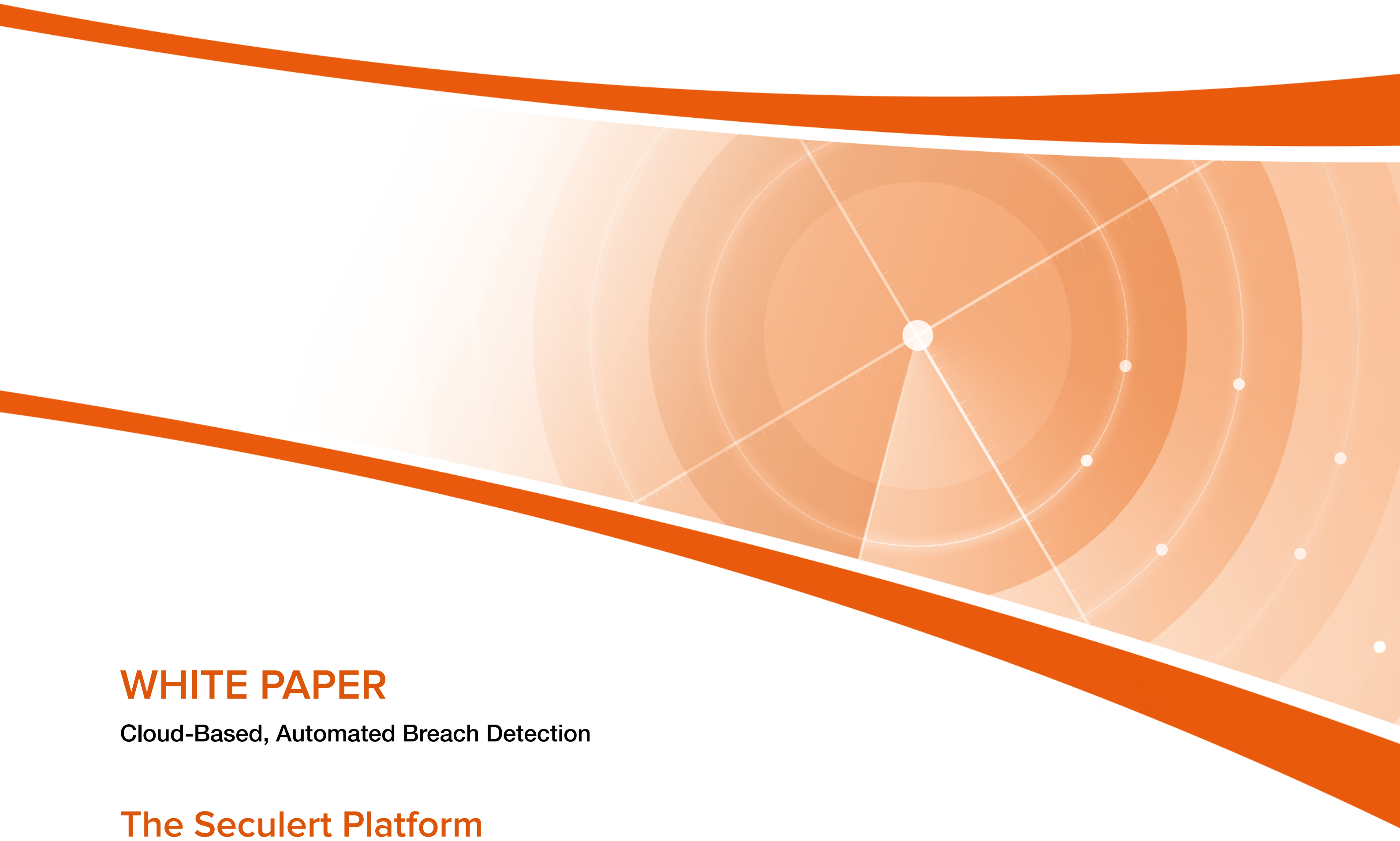
Seculert



WHITE PAPER

Cloud-Based, Automated Breach Detection

The Seculert Platform

Table of Contents

Introduction

Hackers have increased the effectiveness of their persistent malware and their attacks on major corporations. In 2014, their success rate has created unwanted headlines about data breaches on a weekly basis. Seculert provides an automated breach detection platform that finds infected devices that have gone undetected by other means. The results are both verified precisely and within 24 hours of examining a corporation's outbound connections to the Internet. This significantly reduces the time taken to identify malware-infected devices and remove these compromised assets from an organization's environment, thereby reducing the risk of a breach as well as stopping the exfiltration of key corporate data to the hackers.

Comprehensive Technologies

The Seculert Platform detects persistent and unknown malware by focusing on outbound malicious traffic over time, providing superior visibility, speed, and accuracy of incidents. The Seculert Platform achieves this at a materially lower cost by enhancing the productivity of SOC/IR teams, automating the event/log analysis process (for detection), AND without installing any new hardware or software.

Using a combination of technologies, Seculert identifies with certainty new threats as they appear and provides SOC and Incident Response teams actionable data to drive remediation. To prevent subsequent re-infection, Seculert communicates the new threat data to the legacy perimeter defenses and Breach Detections Systems through a RESTful API.

Seculert's core technologies that provide the key to successful breach detection are:

- **Automated Traffic Log Analysis** to identify unknown malware that is targeting your organization
- **Elastic Sandbox** to execute and study suspicious code for as long as necessary in order to profile it
- **Botnet Interception** to detect threats that are already attacking employees, partners, and customers inside and outside your organization
- **Big Data Analytics** to collect and analyze terabytes of data
- **Machine Learning** to examine statistical features, classify the traffic, and determine whether it is similar to any of the known malware profiles
- **SIEM Integration** to enhance existing alert and SOC workflows with Seculert's unique malware perspective
- **Protection API** to automatically stop identified threats through integration with perimeter defenses

The Power of the Cloud

Having scalable resources is critical because in order to understand advanced malware, you must let it run over an extended period of time, and often you must execute it on multiple servers with different properties. The elastic, distributed nature of the cloud is ideal for this.

As a pure cloud service, Seculert is able to digest huge amounts of data over-time in order to identify persistent attacks that have gone undetected by other on-premises security solutions for days, weeks, months, or even years. And without requiring new hardware or software or changes to the corporate network, the cloud offers the elastic processing power and storage capacity necessary for effective malware detection. Furthermore, by preforming all data processing in the cloud there is no drain on local network resources and the solution can be scaled to meet the needs of a corporation today and in the future.

Seculert in Numbers

- 40,000 malware samples automatically analyzed daily
- 1,000s of active botnets under surveillance
- 7 million new infected unique IP addresses detected every day
- 10s of 1,000s of compromised enterprises discovered worldwide
- Petabytes of traffic analyzed monthly

Automatic Traffic Log Analysis

APTs, advanced malware, and 0-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 on larger data sets covering much longer periods of activity than was previously possible. 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 crowdsourced information from customers and vendors all over the world, Seculert Traffic Log analysis discovers even the most devious malware.

What is Traffic Log Analysis?

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.

> In early 2014, Russian banking Trojan Corkow started making headlines. As a lesser known cousin to Carberp, Corkow was originally seen in 2011. It focuses mainly on corporate banking users and has managed to infect thousands of machines undetected.

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

How Traffic Log Analysis Works

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 creates a profile that is used by the machine learning algorithms during traffic log analysis.

1. Customers upload log files to the Seculert Platform using the online 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 runs 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 botnet traffic and identifies infected users and IP addresses. All Seculert customers and partners are also notified via the dashboard and API.

Want to learn more about detecting breaches and advanced persistent threats? Click here.

Elastic Sandbox

Seculert's Elastic Sandbox environment is an essential tool for studying and profiling malware over time for as long as necessary, and for sharing results with the community. It works together with the other core technologies of the Seculert Platform to identify and block malware as soon as it strikes.

> Seculert's Elastic Sandbox uncovered some infamous malware including Ramnit, Kelihos.B, Mahdi, Shamoon, and Dexter.

What is a sandbox?

In IT security, a sandbox is an experimental environment where suspicious code can be executed and studied safely, without risk of infecting a production environment. Today, many security solutions feature sandboxing technology. But not all sandboxes are created equal. Seculert's Elastic Sandbox is unique because of a combination of leading-edge technologies and synergistic interaction with the other technologies in the Seculert Platform: Automated Traffic Log Analysis Botnet Interception, Big Data Analytics, Machine Learning, and a Protection API. And unlike other single-vendor environments, Seculert's Elastic Sandbox sees a complete picture consisting of samples from the full range of on-premises security device vendors.

How the Sandbox Works

1. Customers, partners, vendors, and the malware experts at Seculert upload suspicious executable files to the Elastic Sandbox using the online platform or API.
2. In the Elastic Sandbox, Seculert studies the behavior of the code including network communications, meta-data in the network traffic, and host runtime changes.
3. You can tune the sandbox by setting the execution time and region to approximate geographically targeted attacks.
4. If additional suspicious code is found during execution, it too is downloaded and sent to the Elastic Sandbox for analysis.
5. Seculert uses Big Data analytics to process all of the information collected and determine whether or not the code is malicious. If the solution recognizes a known malware profile, it updates customers and partners immediately via the online dashboard and the Seculert API, which communicates directly with customer's proxies and firewalls to block known threats.
6. If the executable file's behavior is not known, but is conclusively identified as malware, a profile is defined. Seculert immediately notifies customers and partners via the dashboard and API. In addition, the new malware profile becomes an important learning set for Seculert's Machine Learning algorithms and Automated Traffic Log Analysis.
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.

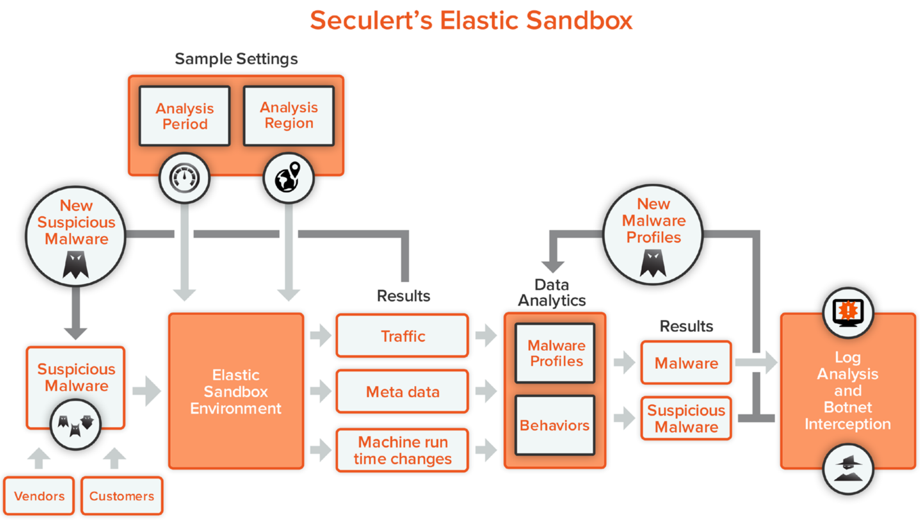


Figure 1: Seculert's Elastic Sandbox

Click here to learn more about the advantages of the Seculert Elastic Sandbox.

Botnet Interception

A large percentage of today's advanced threats operate as a botnet – a network of malware-infected devices run by a series of command and control servers. These botnet infections gradually spread throughout the users and endpoints in your organization until they can do significant damage. Remote employees and employees using personal mobile devices (BYOD) are a prime target for botnets because they are beyond the protection provided by perimeter security defenses.

Seculert Botnet Interception analyzes botnet traffic to identify all infected users and endpoints – whether they are inside or outside of the corporate network The Seculert Platform quickly detects malware infections that are already affecting your organization – and that your current security defenses have not detected.

What is a Botnet?

Like all advanced malware, botnets evolve. That is why it is essential to analyze them over a significant period of time. A typical botnet may undergo three stages:

- **Opportunistic:** Criminals attack the general population, usually for monetary gain. The risk is usually greater to the individual rather than to the organization.
- **Semi-opportunistic:** This category is programmed to infect specific targets in a search for vulnerable entry points and key employees in a specific industry or country, and is often performed with the goal of selling the information onward.
- **Targeted:** Once vulnerable targets have been found, a targeted attack with well-defined goals may be launched by the original hacker or by a second criminal organization with more focused goals.

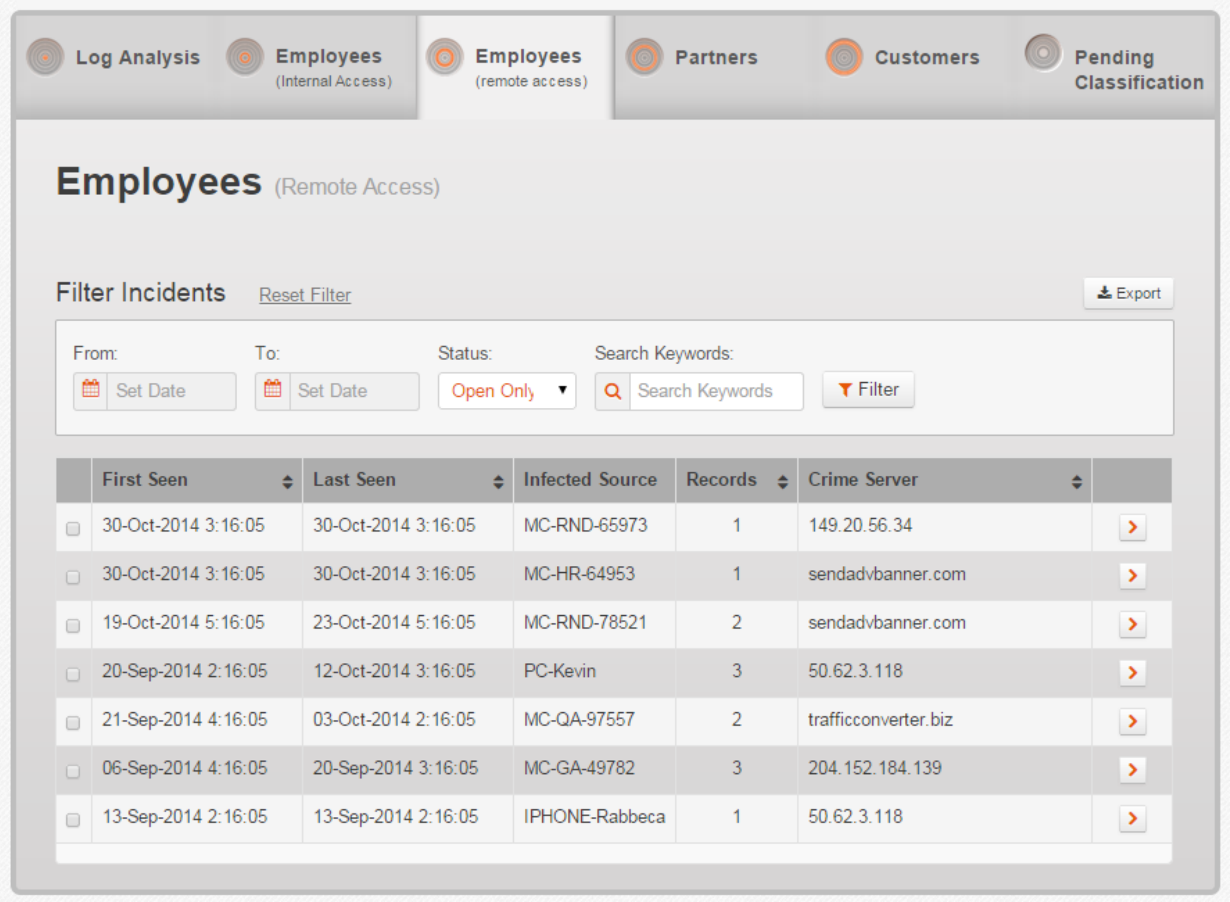
> Since 2007, infamous botnet Gameover ZeuS has infected more than 500,000 machines and stolen over $100 million from banks, businesses, and consumers. A new variant of Gameover ZeuS, introduced in July 2014, allowed it to go from generating 1,000 domains per week to 1,000 domains per day.

Seculert Botnet Interception is effective with all three types. It uses a number of recognized techniques along with proprietary, patent-pending methods that work together to collect information that no other method can deliver.

How it Works

Standard botnet monitoring services provide a list of known command and control servers so you can block them. Seculert goes one step further and actually identifies the users and endpoints that are infected. As soon as we identify a botnet, we infect our own servers and join the network. Seculert Botnet Interception collects millions of global bot transmissions as they communicate with command and control servers (C&C) every day. Using a wide range of techniques, the Botnet Interception module silently intercepts the traffic, analyzes it, and determines if our customers are infected.

Since it is part of our cloud-based platform, Seculert Botnet Interception is entirely zero-touch for your organization: no need to change your security architecture, install software, deploy a new appliance, or redirect Internet traffic. You can set it up easily by simply defining a range of IP addresses or outward facing web domains (e.g. sslvpn.mycompanydomain.com or owa.mycompanydomain.com), and detection begins immediately.



Employees (Remote Access)

Filter Incidents

From: Set Date To: Set Date Status: Open Only Search Keywords: Search Keywords

	First Seen	Last Seen	Infected Source	Records	Crime Server	
□	30-Oct-2014 3:16:05	30-Oct-2014 3:16:05	MC-RND-65973	1	149.20.56.34	>
□	30-Oct-2014 3:16:05	30-Oct-2014 3:16:05	MC-HR-64953	1	sendadvbanner.com	>
□	19-Oct-2014 5:16:05	23-Oct-2014 5:16:05	MC-RND-78521	2	sendadvbanner.com	>
□	20-Sep-2014 2:16:05	12-Oct-2014 3:16:05	PC-Kevin	3	50.62.3.118	>
□	21-Sep-2014 4:16:05	03-Oct-2014 2:16:05	MC-QA-97557	2	trafficconverter.biz	>
□	06-Sep-2014 4:16:05	20-Sep-2014 3:16:05	MC-GA-49782	3	204.152.184.139	>
□	13-Sep-2014 2:16:05	13-Sep-2014 2:16:05	IPHONE-Rabbeca	1	50.62.3.118	>

Figure 2: Seculert Dashboard- Grid View

Immediately see the users and devices infected – both inside and outside the corporate network

Seculert is designed to protect remote users - no matter where they are located, and regardless of the computer, mobile device or operating system they use.

Click here to learn more about protecting remote users and BYOD.

Speed and Precision

Big Data Analytics

Breach detection 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 Platform. 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.

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 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.

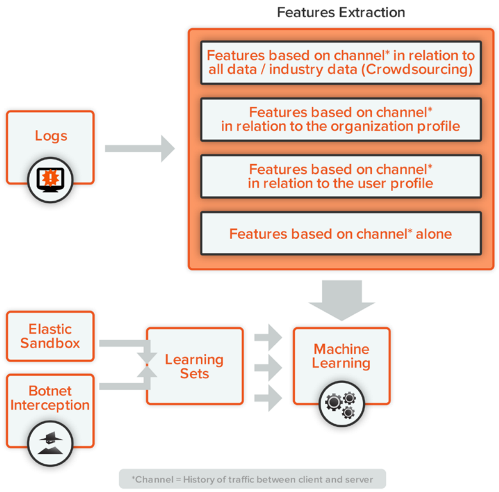

Features Extraction
Features based on channel* in relation to all data / industry data (Crowdsourcing)
Features based on channel* in relation to the organization profile
Features based on channel* in relation to the user profile
Features based on channel* alone
Logs
Elastic Sandbox
Botnet Interception
Learning Sets
Machine Learning
*Channel = History of traffic between client and server

Figure 3: Seculert's Machine Learning Process

To confirm the presence of malware, Seculert automatically correlates the suspicious channel (history of traffic between client and server) with a larger data set of 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. Click here to learn more about how Seculert analyzes data layers to pinpoint suspicious activity.

A Comprehensive Platform

Seculert Dashboard and Alerts

After any attack is detected, the dashboard (Figure 4) supplies you with an alert so that you can understand and mitigate your exposure and modify your security policies as needed. You will see the compromised computer by IP, machine name, employees' email, threat type, and crime server.

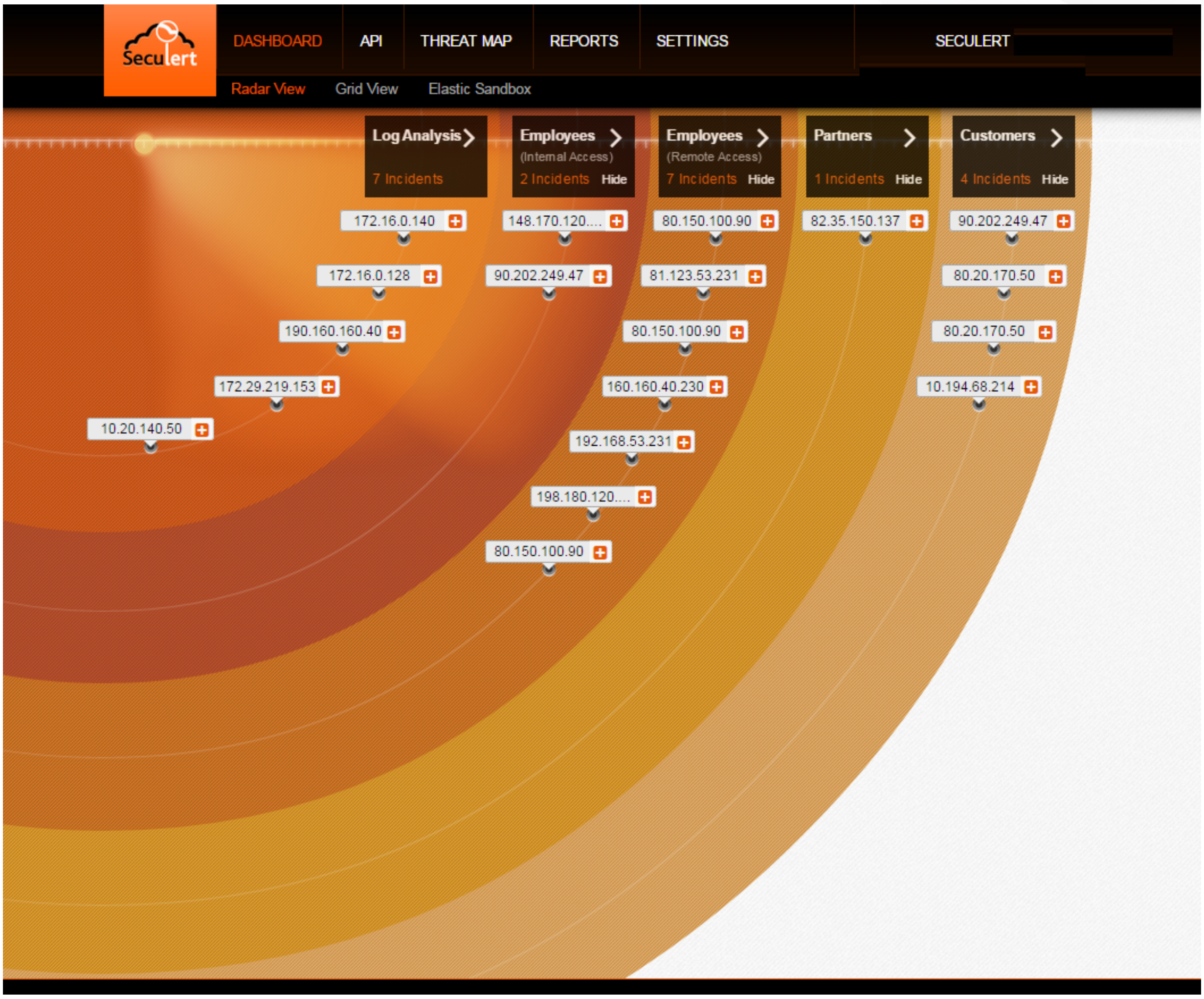
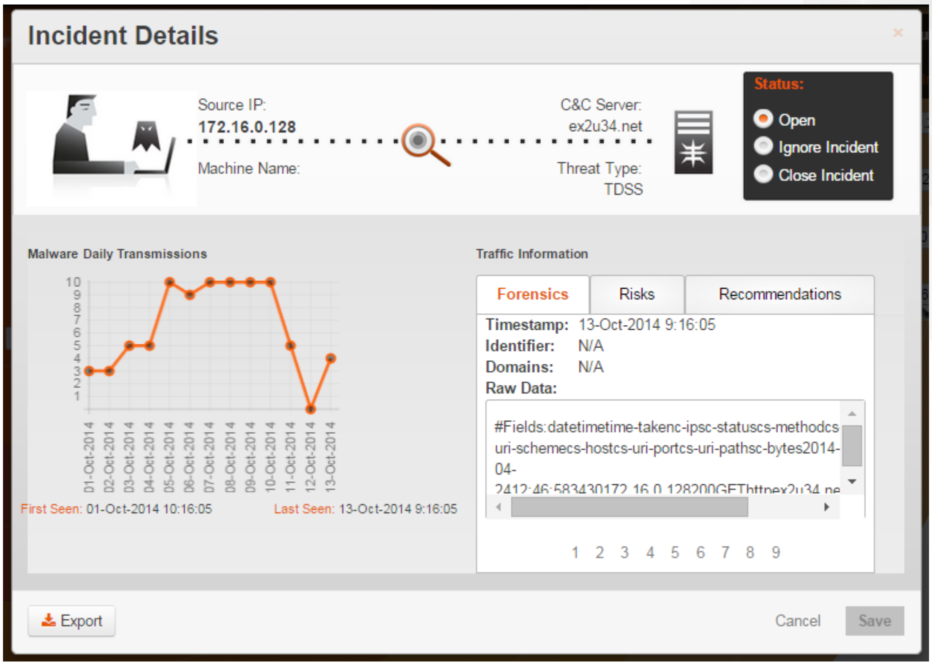


Figure 4: Seculert Dashboard- Radar View

The incident details (Figure 5) include the raw data of the transmission from the infected endpoint to the crime server, which can sometimes contain the confidential information that was leaked- e.g. credentials to access critical web services, plus the time and date of the transmission is reported. To help you further understand the threat, a chart depicting the daily number of transmissions and the malware behavior is also included. All the relevant transmissions from the source to the crime server are grouped together and we provide separate tabs for risks and remediation recommendations.



Incident Details

Source IP: 172.16.0.128

Machine Name:

C&C Server: ex2u34.net

Threat Type: TDSS

Status:
● Open
○ Ignore Incident
○ Close Incident

Malware Daily Transmissions

First Seen: 01-Oct-2014 10:16:05

Last Seen: 13-Oct-2014 9:16:05

Traffic Information

Timestamp: 13-Oct-2014 9:16:05
Identifier: N/A
Domains: N/A
Raw Data:

```
#Fields:datetimetime-takenc-ipsc-statuscs-methodcs-
uri-schemecs-hostcs-uri-portcs-uri-pathsc-bytes2014-
04-
2412:46:583430172.16.0.128200GETthttpex2u34.ne
```

Figure 5: Seculert Dashboard- Incident Details

Additionally, you can upload samples to the Elastic Sandbox at any time using the dashboard as well as the API. It's easy to configure runtime settings such as region and time. As soon as the analysis is completed, you are alerted by email and receive a detailed report. Malware reports include information about suspicious behavior observed, domains visited, registry, and other host changes so that you can understand and mitigate your exposure and modify your security policies as needed.

Automated Protection API

Today, SOC teams face the daunting challenge of sifting through immense amounts of potential breach data generated by perimeter defense systems. It is difficult to identify the few incidents with malicious potential out of the large number of generated most prevention systems. To prioritize incidents and to address the more complex and evasive breaches, most advanced organizations have a Security Incident and Event Management system in place (SIEM).

This infrastructure requires resources for expert analysts in data science and security and a tremendous amount of dedicated compute power. In order to empower SOC teams to use Seculert incident data into this existing infrastructure, Seculert can be integrated via the RESTful API or in some cases applications that have been designed specifically to present Seculert data in these other environments.

To make the most of the Seculert Platform, you can integrate it with your existing security infrastructure using the Seculert Protection API. The API's simple interface for accessing and retrieving data is done via a web request that uploads files via HTTP, followed by a response including the files' identification key.

When malware is detected, 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.

For more information about integrating Seculert data with your existing solutions, via application or API, click here.

Prevention is Not Enough

The Seculert cloud-based, automated breach detection platform fills the gap left by legacy perimeter defense and breach prevention solutions. Seculert protects distributed enterprises from advanced threats by focusing on the malicious outbound network traffic generated by advanced malware. By combining Big Data analytics, machine learning technology, and behavioral analysis, Seculert provides unique visibility of malware that has evaded prevention solutions and established presence on enterprise networks.

Using a combination of Automated Traffic Log Analysis, an Elastic Sandbox environment, and Proactive Botnet Interception, Seculert identifies with certainty new threats as they appear and provides SOC and incident response teams actionable data to drive remediation. Seculert communicates the new threat data, using a RESTful API, to the legacy perimeter defenses and breach detection systems to prevent subsequent re-infection. AND, the Seculert Platform achieves all of this without the need to install on-premises hardware or software.

Today's headlines prove that all prevention solutions eventually fail. Protect your company, your reputation, and your profits with a comprehensive post-breach detection solution.

Seculert

Cloud-based, Automated Breach Detection

Seculert fills the gaps in existing advanced threat defenses by focusing on the blind spots found in breach prevention systems. In an era when infection is inevitable and adequate resources to find and remediate threats are limited, the Seculert Platform identifies new threats with unprecedented speed and precision. Leveraging its Big Data analytics as a service, botnet interception, and elastic sandbox functionality, Seculert provides superior detection while driving down the cost and time it takes to remediate. For more information on Seculert, visit www.seculert.com.

Contact Us

Toll Free: (US/Canada): +1-855-732-8537
Tel (UK): +44-203-355-6444
Tel (other): +972-3-919-3366
Email: info@seculet.com
www.seculert.com