SECULERT'S ELASTIC SANDBOX ENVIRONMENT

Advanced threats demand a new class of defenses. Precisely because they are persistent and ever-changing, it is essential to study their behavior over time – and not just at the moment of entry into the organization. And as threats become more sophisticated and dangerous, the most effective and efficient way to fight is to join forces and share information.

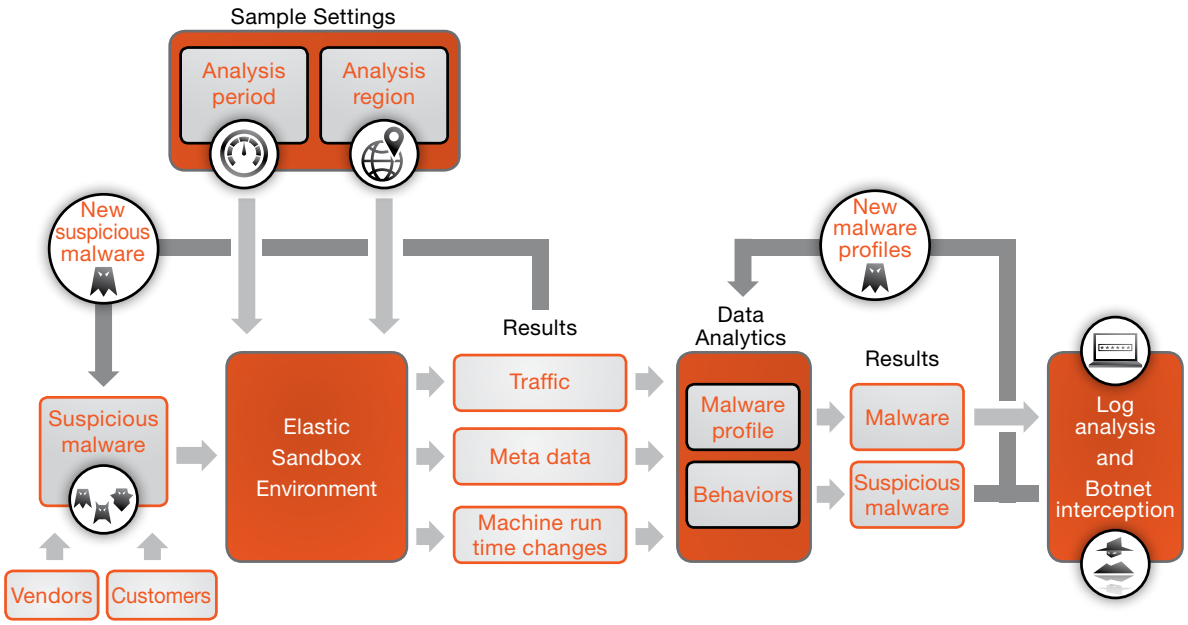
Today, Seculert is leveraging the capabilities of the cloud to turn this vision into reality. Seculert's Elastic Sandbox environment is an essential tool for studying and profiling malware over time for as long as necessary, and for sharing results with the community. It works together with the core technologies in the Seculert solution to identify and block malware as soon as it strikes.

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 Automated Traffic Log Analysis - in one simple solution that proactively identifies new threats as they emerge.

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 modules in the Seculert Solution: Botnet Interception, Big Data Analytics, Protection API, and Automated Traffic Log Analysis. 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 executables 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.

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

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'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 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.

MONITORED BEHAVIORS

When a suspicious file is uploaded and run in the Elastic Sandbox, Seculert looks for hundreds of different behaviors which, taken together, can indicate malware. Some examples include:

- **Network traffic:** All malware communicates with a command and control server which may be indicated by a dynamic DNS domain. It may also download additional files, scan for security vulnerabilities or setup back doors.
- **Device changes:** Malware will often make changes to the host device including the registry, security settings, creating and changing files, auto-run settings and hooking.
- **Security detection measures:** Malware actively avoids detection by disabling security settings, avoiding running while being monitored and injecting into other processes.

THE ADVANTAGES OF THE SECULERT ELASTIC SANDBOX

Long-term analysis

Advanced malware is often quiet for long periods of time, and when it does act, it isn't always immediately apparent that something is wrong. It is also programmed to change, so that its behavior patterns don't become suspicious. As a result, it is essential to study malware over a period of time ranging from minutes to days. Sandboxes that run in-line on your network traffic can only run suspicious code for short periods ranging from a few seconds to a few minutes. Anything longer would be disruptive and too resource intensive. The Seculert Elastic Sandbox can execute code for as long as necessary – from a minute to an hour.

Target emulation

Since many botnets target a particular region, industry or organization, Seculert configures servers in a way that mimics different potential targets. The Seculert platform gives you the ability to set the region, time and additional factors that can help identify malware behavior.

Invisible to Malware

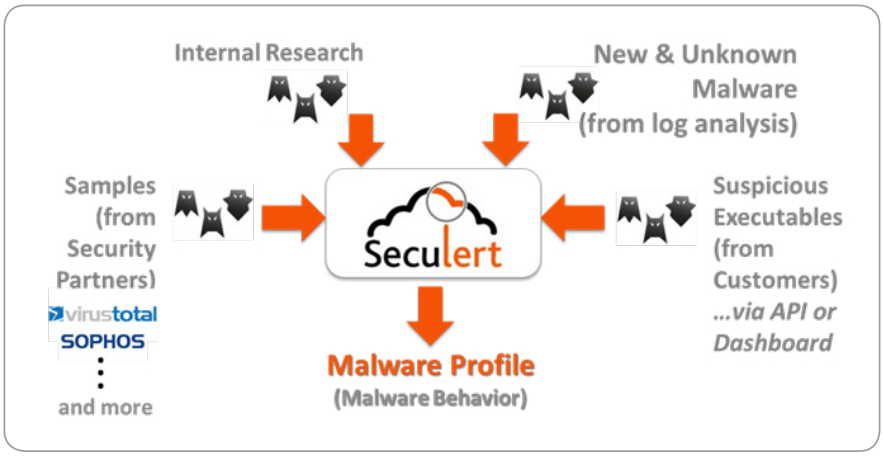
As malware becomes more and more sophisticated, it is able to identify sandboxing technology and will keep quiet until it thinks it is "safe." Seculert uses proprietary technology to make malware believe that it is not running inside a sanitized, virtual environment. To the malware, the Elastic Sandbox looks like a device with natural activity such as keyboard inputs and mouse movements.

Elastic, cloud environment

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 a sandbox environment.

40K samples daily, from all kinds of traffic and vendors

Today, the Seculert Elastic Sandbox analyzes over 40,000 new malware samples every day – and the number keeps growing. The samples come from customers who upload suspicious code through the API or dashboard, Seculert's automated traffic log analysis, the Botnet Interception module and partners.



BIG DATA ANALYTICS

Monitoring over 40,000 code samples a day generates a tremendous amount of data. Seculert's Big Data analytics engine uses machine learning algorithms and Elastic MapReduce to determine whether a code is malware or not. If it is malware, all Seculert customers are immediately protected via the API and dashboard alerts. But a single-pronged approach is not enough to stay ahead of emerging threats. Seculert also uses the new malware profile as a learning set for machine learning algorithms that detect unknown malware in customer traffic logs.

AUTOMATED PROTECTION API

To make the most of the Elastic Sandbox, 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:

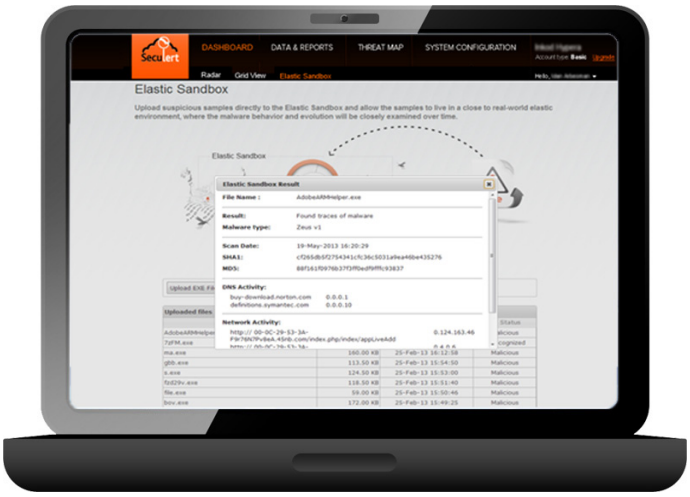
- A web request that uploads files via HTTP, followed by a response including the files' identification key
- A request that retrieves the results of the analysis using the identification key

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 AND ALERTS

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.



The dashboard automatically indicates whether malware was found and what activity should be blocked

SYNERGISTIC TECHNOLOGIES

Seculert's Elastic Sandbox environment is extremely powerful – but it is the combination of the Elastic Sandbox working together with all of Seculert's core technologies that provides the key to successful advanced threat protection. In addition to the Elastic Sandbox, Seculert features:

- Botnet interception to detect threats that are already attacking employees, partners and customers inside and outside your organization.
- Automated traffic log file analysis to identify unknown malware that is targeting your organization.
- 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

Basic Elastic Sandbox functionality is available for a total 5 samples running for 1 minute each for free. In order to upload more than 5 samples and get the ability to set the execution time and geographic region, 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