# SECURING YOUR DATA

Using the cloud to protect your organization from Advanced Persistent Threats (APTs) is the smartest way to stay Safe in today's challenging and constantly changing malware threat environment. However, while you want to reap the benefits of cloud-based APT protection, you don't want to compromise the security of your data. And that's why it's essential to choose a Service Provider that has 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. That partner is Seculert.

## THE NATURE OF APTS AND THE NEED FOR DATA TRANSMISSION

Advanced Persistent Threats (APTs) are targeted attacks specifically designed to breach conventional Network Security systems - which are typically comprised of firewalls, IDS and Secure Web Gateways - and remain undetected. Once inside, the malware goes to work stealing and manipulating data over a period of months or even years, before launching into a full-blown attack against a shocked and often helpless victim.

## HOW SECULERT COUNTERACTS APTS

How does Seculert counteract this malicious tactic and keep your organization safe? By empowering you to easily upload logs of your actual organizational HTTP traffic, which is then analyzed using Big Data analytics and correlated with Seculert malware expertise from both the botnet interception (Echo) and elastic sandbox (Swamp) over time.

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.

## 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 "Seculert Sense" 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.

Please feel free to contact us with any questions, suggestions or issues about any of the above, including our security policies, support@seculert.com.

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