Seculert
Cloud-Based Malware Detection

WHITE PAPER

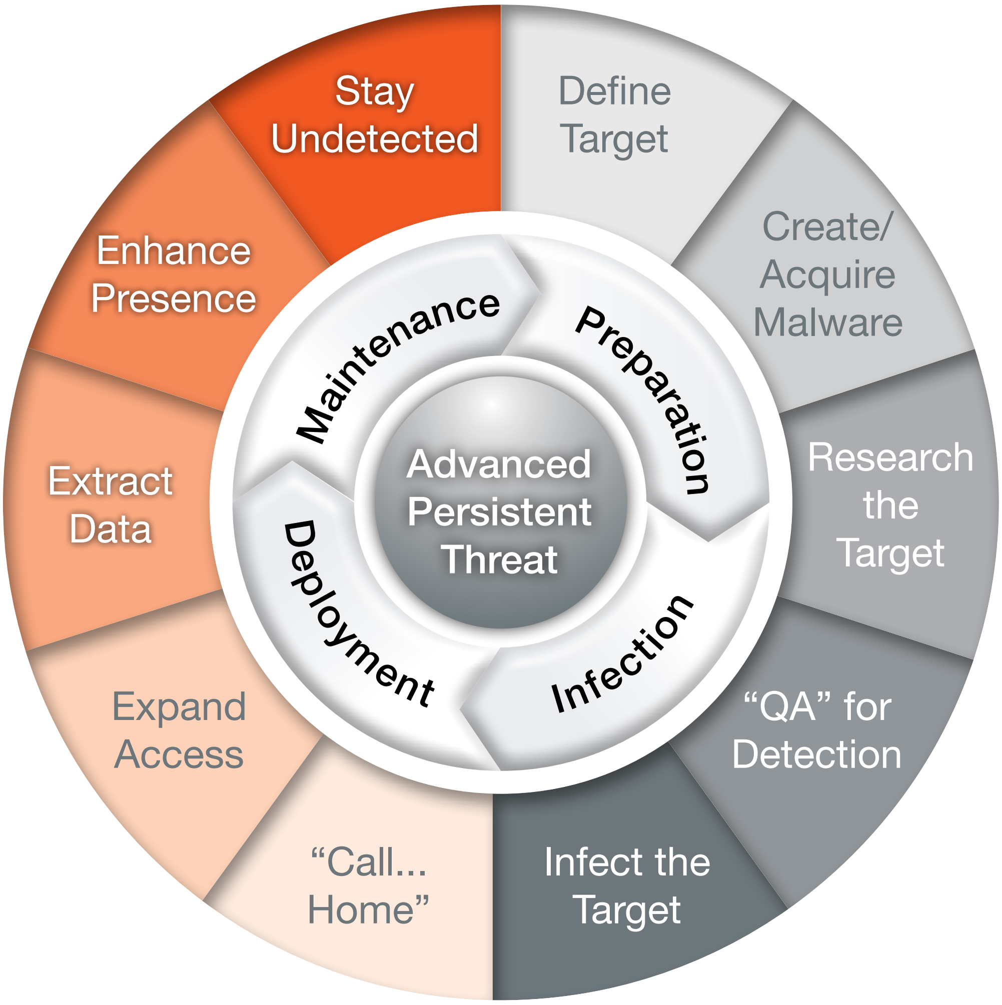
The 6 Key Factors to Consider When Choosing a Solution to Protect Your Network from APTs

TABLE OF CONTENTS

INTRODUCTION

Advanced Persistent Threats (APTs) are a growing danger to organizations. Rather than behaving in an opportunistic fashion like legacy malware, APTs focus on high-value targets and typically take a "low and slow" approach, and persist in the network for more than 400 days on average – while the adversaries behind them steal and manipulate valuable data, and carry out their insipid economic, political and social agendas.

There are four stages in the APT lifecycle: preparation; infection; deployment and maintenance.



It's the persistent and recurring nature of APTs that make them destructive, costly and a top concern for all organizations – not just military agencies, defense contractors and state-sponsored organizations. Indeed, today's adversaries have gone beyond these traditional targets, and are aiming for organizations across all sectors: technology, energy, media, news, manufacturing, education, telecom, and so on.

While the situation appears daunting, getting the protection you need isn't difficult – provided that you choose a solution that takes these 6 key factors into consideration:

1. THE SOLUTION MUST USE BIG DATA AND FOCUS ON DETECTION.

It's well established that preventing 100% of infections is impossible, because threat identification cannot entirely take place at the organization's perimeter, in real-time, or by policy. Plus, the inherent hardware boundaries and time limitations of on-premises appliances rule them out as a completely impenetrable framework. Yet, despite these facts, most vendors continue to focus on prevention -- and as a result, expose organizations to subtle, hidden and previously-unknown APTs.

Logically, APT detection decisions must be based on the ability to analyze data, which must be gathered from and analyzed over sustained time durations. And that's where Big Data analytics enters the picture. Therefore, when evaluating a solution, it's vital to look for a platform that can expand and adapt to meet the ever-increasing sophistication of new APTs. The solution must be flexible and scalable, with the ability to process immense amounts of multi-layered data over time.

As Executive Chairman Art Coviello announced at the 2013 RSA Conference: "The whole game here is to shift away from a prevention regime -- Big Data will allow you to detect and respond more quickly."

2. THE SOLUTION MUST ALLOW AUTOMATED ANALYSIS.

Detecting APTs isn't easy. With the sheer volume of new threats that emerge on a daily and even an hourly basis, most vendors oblige organizations to bring in an expensive army of data scientists, malware analysts and forensic specialists to manually locate and diagnose breaches.

Your organization can significantly decrease this costly scenario by choosing an APT detection solution that automates Big Data analytics on your behalf. The only task you should be required to perform is to simply upload your HTTP gateway traffic log files to a secure cloud-based platform.

From there, the solution should automatically analyze and correlate your data against unique malware behaviour profiles created by an automated and elastic malware analysis sandbox. It should also utilize different layers of machine learning algorithms to rapidly analyze historical network traffic data and uncover hidden, subtle and previously-unknown APTs that may have been flying "under the radar" on your network for months – or years.

3. THE SOLUTION MUST RELY ON A COMPREHENSIVE AND EVOLVING MALWARE DATASET.

In February 2012, Dr. Anton Chuvakin of the Gartner Group sent out an impassioned plea via social media that caught the attention of security experts the world over:

"It is truly maddening to see examples of bad guys sharing data, tricks, methods and good guys having NO good way of doing it. It is normal to sit on the 'hard-earned' knowledge of ways you used to detect that proverbial advanced attacker while your peers in other organizations are being owned by the same threat. And the cycle of suffering continues!!!"

While Dr. Chuvakin was directing his frustration at the adversaries behind today's sophisticated APT attacks, he was also taking aim at vendors who fail to "share data, tricks and methods."

However, not all vendors were implicated by Dr. Chuvakin astute criticism, because there are solutions that do exactly what he envisioned. That is, they cross-pollinate data intercepted from live botnets with crowd-sourced security logs shared by customers and partners. What's more, the datasets include HTTP gateway traffic logs from users of all leading perimeter security vendors, including Cisco, Juniper Networks, Fortinet, Check Point, F5, Palo Alto Networks, McAfee, Blue Coat, Websense and the list goes on. As a result, everyone within the community benefits from this sophisticated crowdsourced center of data.

4. THE SOLUTION MUST BE UP AND RUNNING IN MINUTES.

In the knowledge economy, ongoing training is essential. Yet, who has the time to complete a multi-day training or certification course before they can start using a network protection solution? Unfortunately, many vendors think that you do, and as a result they oblige your security staff to spend their limited time learning the ins-and-outs of (yet another) on-premises product installation, complete with tedious configuration requirements and confusing client-server architecture layouts.

Fortunately, there are cloud-based solutions that believe "up and running" should be measured in minutes, not days. There's no comprehensive training, and they feature a user friendly interface and dashboard that makes it easy for all users -- from the less-technical to the most professional personnel -- to play a role in keeping your organization safe.

5. THE SOLUTION MUST FEATURE AN ELASTIC DATA CENTER PLATFORM.

In order to analyze the vast amounts of data required for a true APT detection, you need a data center – and they aren't cheap. DataCenterKnowledge.com estimates that data center construction can typically cost $1,000 to $1,500 for each square foot of finished space. Plus, there are high costs associated with training and/or recruiting to get the required level of expertise with respect to virtualization, expandability, server management, rack design, and setting up remote access. And on top of this, there's powering the facility, which experts say comprises the bulk of the overall data center price tag.

The way to avoid this enormous expense is to choose a solution that, behind the scenes, already features a robust and elastic data center platform -- one that automatically processes petabytes of botnet traffic and gateway traffic logs every month, and analyzes tens of thousands of malware samples every day. And speaking of cost-effectiveness...

6. THE SOLUTION MUST BE COST-EFFECTIVE.

A comprehensive 18-month study by NSS Labs has concluded that installing yet another on-premises device -- such as a next generation firewall, IPS, or endpoint protection product -- doesn't help organizations prevent 100% of infections. This, however, doesn't seem to diminish the efforts of some vendors who continue to claim that adding "more boxes" is a sensible strategy.

Frankly, you've spent enough – and perhaps, more than enough – on creating your on-premises security framework, and implementing best-in-class products. Why spend on yet another box? That's a question you don't need to answer when you choose a cost-effective cloud-based solution, which offers unlimited elasticity and scalability as your organization grows, and low TCO with no hardware or software to purchase. Plus, these solutions are non-intrusive and have no impact on existing organizational network resources, which means you won't need to invest more on your IT infrastructure.

MOVING FORWARD WITH SECULERT

With the unprecedented velocity, complexity and breadth of APTs, organizations can no longer rely on a conventional prevention-based approach to stay 100% safe. Nor can they hope that cyber criminals, hacktivists, adversaries and nation states will pass them by. That may have been possible years ago, but these days, it's really not a question of whether an attack will occur -- but when, and how damaging.

To meet this challenge head-on, we've designed Seculert with all 6 of the above-noted key factors in mind:

- It uses uses Big Data and focuses on detection
- It allows for automated analysis
- It relies on a comprehensive and evolving malware dataset
- It's up and running within minutes
- It features an elastic data center platform
- It's cost effective

Ultimately, Seculert is designed to protect your organization from today and tomorrow's sophisticated malware and APTs, so that you can stay safe, achieve success, and move forward.

Share this white paper

Sign-up Now! It is FREE

http://www.seculert.com/signup