Endpoint Security: New Approach

secpod

Executive Summary

Large number of attacks ensue due to compromised endpoints. These endpoints form majority of computing devices in any organization. The definition of endpoints has been evolving over time with BYOD (Bring Your Own Device), cloud computing, virtualization and traveling employees. Traditional security measures are not always effective in tackling sophisticated and targeted attacks. 60% of the malware are undetected by anti-malware products. 90% of the attacks happen because of vulnerabilities or misconfigurations in the endpoints, even though organizations spend majority of their time performing the so-called vulnerability management. Attackers are easily able to bypass perimeter protection systems and network security measures. It takes only seconds to a few minutes for attackers to cause major damage. Defense in-depth is introducing multiple layers of disconnected security mechanisms and increased complexity, while not yielding the value that one would expect from high investment in information security tools.

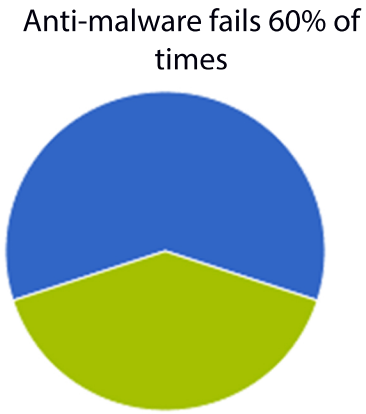
There is lack of visibility and control over endpoint activities. Stand-alone threat intelligence without actionable remedy increases the work of security analysts. Lack of automation causes delay in detection and response to attacks.

A new approach to endpoint security is indispensable. An approach that identifies risks in seconds (vulnerabilities and misconfigurations) and remediates within minutes, keeps track of all the security controls and fixes deviations immediately. An approach that provides visibility and control over endpoint activities, identifies Indicators of Compromise (IoC) through automated means and take responsive actions in seconds.

Endpoint Security Challenges

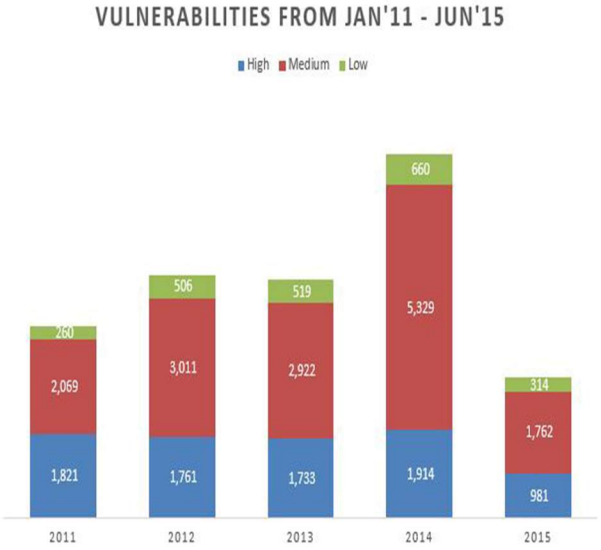
60% malware are not detected, ineffectiveness of Anti-malware

Advanced exploitation techniques - custom code, polymorphic and disappearing nature of malware, is making it increasingly difficult for signature based or blacklisting methods to detect malware. Attack duration is reduced to hours and minutes instead of days and weeks, by when signatures are either not authored or they are outdated. According to reports, Anti-malware products detect only 5% of the new malware.



While there are no alternatives to anti-malware products, they need to be complemented with additional capabilities that help in preventing the attacks in the first place, additionally providing visibility and control over what is happening on the endpoints and responding to IoCs.

90% of attacks happen because of vulnerabilities and misconfigurations



Source: NIST

In spite of spending enormous amount of time and money, vulnerabilities remain unresolved. It is reported that a typical organization spends 63% of the time on vulnerability and patch management as part of their security sustenance efforts. At the same time, majority of the organizations are not patching their systems. Vulnerability management products that exist are highly complex to use, consume lot of network bandwidth, hog system resources and they do not help fix the problem. Because of this, organizations do not run vulnerability scans on a daily basis. However, new vulnerabilities are being discovered on a daily basis at an average of 22 vulnerabilities per day. Typically, organizations run weekly, monthly or quarterly scan

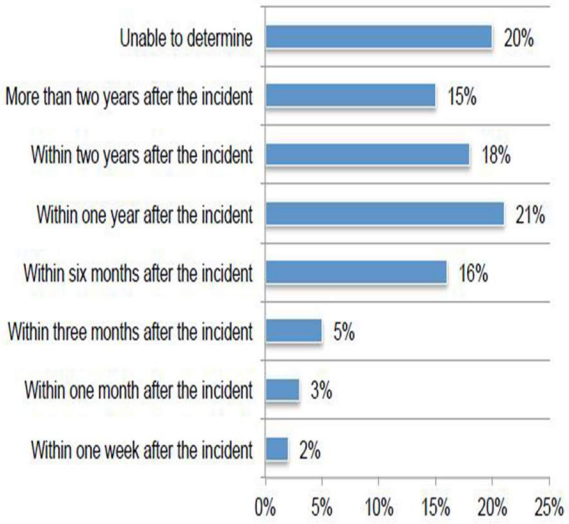
Even after performing a scan, they are not fully equipped to fix the vulnerabilities. It is discouraging to see thousands of pages of report and in almost all cases, a very important stage of vulnerability management, Patching, is ignored leaving the endpoints vulnerable to attacks. Even when they have processes to patch systems, typically it takes 30-90 days to roll out patches.

Vulnerability management needs to be simplified to a daily routine.

Lack of visibility and control

The definition of network perimeter has expanded considerably because of cloud, mobile workforce, BYOD and distributed networks. Firewalls, Advanced Firewalls, Intrusion Detection Systems (IDS), SIEM (Security Information and Event Management) and Advanced Malware detection tools offer no visibility over endpoint activities. Attack analysis require an in-depth look at the endpoint activities, to be able to identify and respond to attacks before the damage is done. Visibility is needed to vulnerabilities present in the system, patches that are missing, processes and services that are running, file modifications and deletions, security events, network connections being established, installed software, devices connected, privileged user accesses and rights, misconfigurations and hardening parameters etc

Time taken to discover attacks (in %)

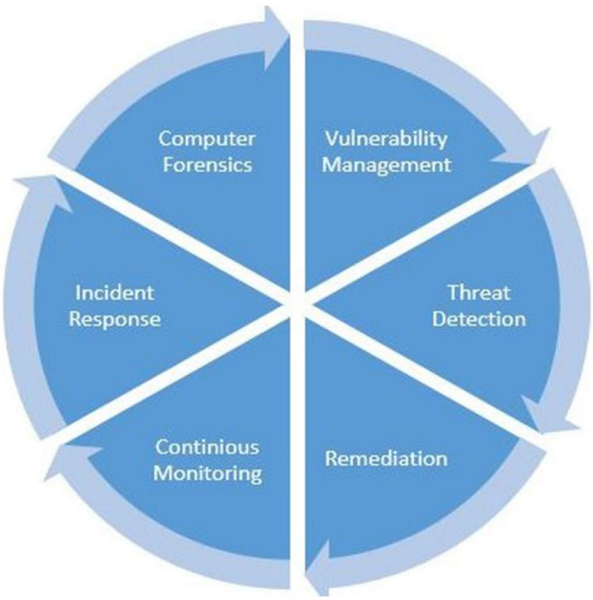


Source: Ponemon Institute Report 2014

As a preventive measure, it is also important to ensure all endpoints adhere to some guidelines, for example which applications are running, which devices are enabled under what conditions, device hardening measures, in general to stay compliant. Any deviations from the standard guidelines must be fixed and monitored at all times.

Knowing all security related information of each endpoint that connects to the organization and being able to control each device is critical to maintaining a secure environment.

Lack of automation



Over a period of time organizations acquire multiple tools to address different security problems. Tools so deployed do not easily talk to each other. It is essential to have all security management tools integrated, to have automated continuous monitoring capabilities. This would require products to store and communicate using structured data format protocol suites such as SCAP, STIX/TAXII. It is also important to automate the response/remediation capabilities to some of the routine alerts such as patching common applications vulnerabilities. Additionally, volume of threat intelligence is too high to manually sift through each and decide their applicability to the organization.

Automation is needed to integrate organizational security management practices into a single-window continuous monitoring system. Automation is needed to search through volumes of data and identify IoCs. Automation is also needed for faster response including patch management and configuration management.

Solutions built without remediation

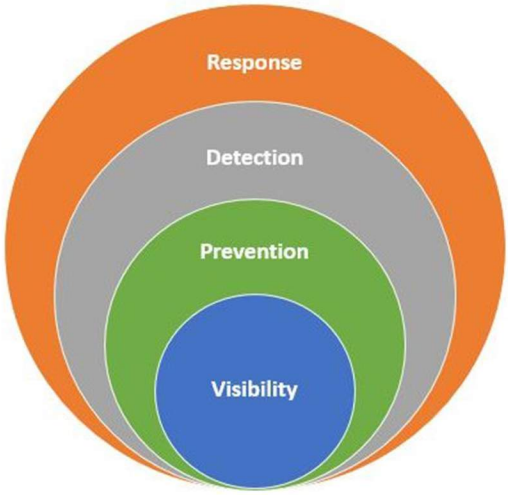
Detection takes weeks/months and remediation takes months/years while attacks continue to happen in minutes. It is important to have network and endpoint visibility. It is also important to have access to structured threat intelligence data, which can be fed into these systems to ensure speedy detection of IoC. But, if an ongoing attack is detected and if there is no strategy to respond to that attack or remediate, it is almost useless to know that an attack is taking place.

An incident response or remediation process must be in place and is a multi-layered strategy. It would require ability to block an ongoing attack and ensuring that it does not recur. An attack could be exploiting a vulnerability that is unpatched. It is important to identify the vulnerability quickly, identify how many systems are affected by that vulnerability and roll out a patch.

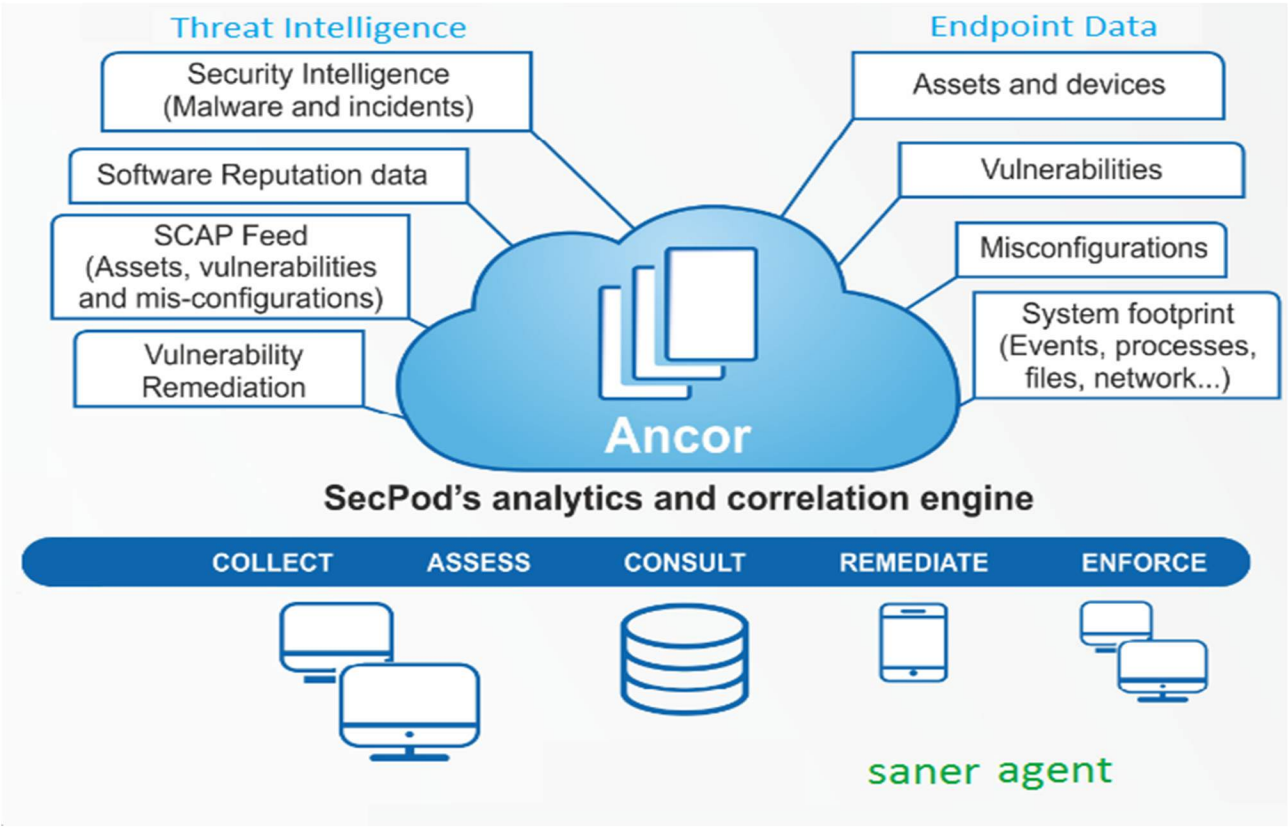
SecPod brings new approach to endpoint security

A complete endpoint security solution will necessarily have the following:

- Proactive management of vulnerabilities and adherence to security policies.
- Visibility and control to endpoint activities.
- Infrastructure to detect an on-going attack within the network.
- Ability to receive threat intelligence from trusted sources and check its relevance
- Comprehensive response to an on-going attack (this may include quarantine, removal from network and most importantly removing the root cause of the incident)

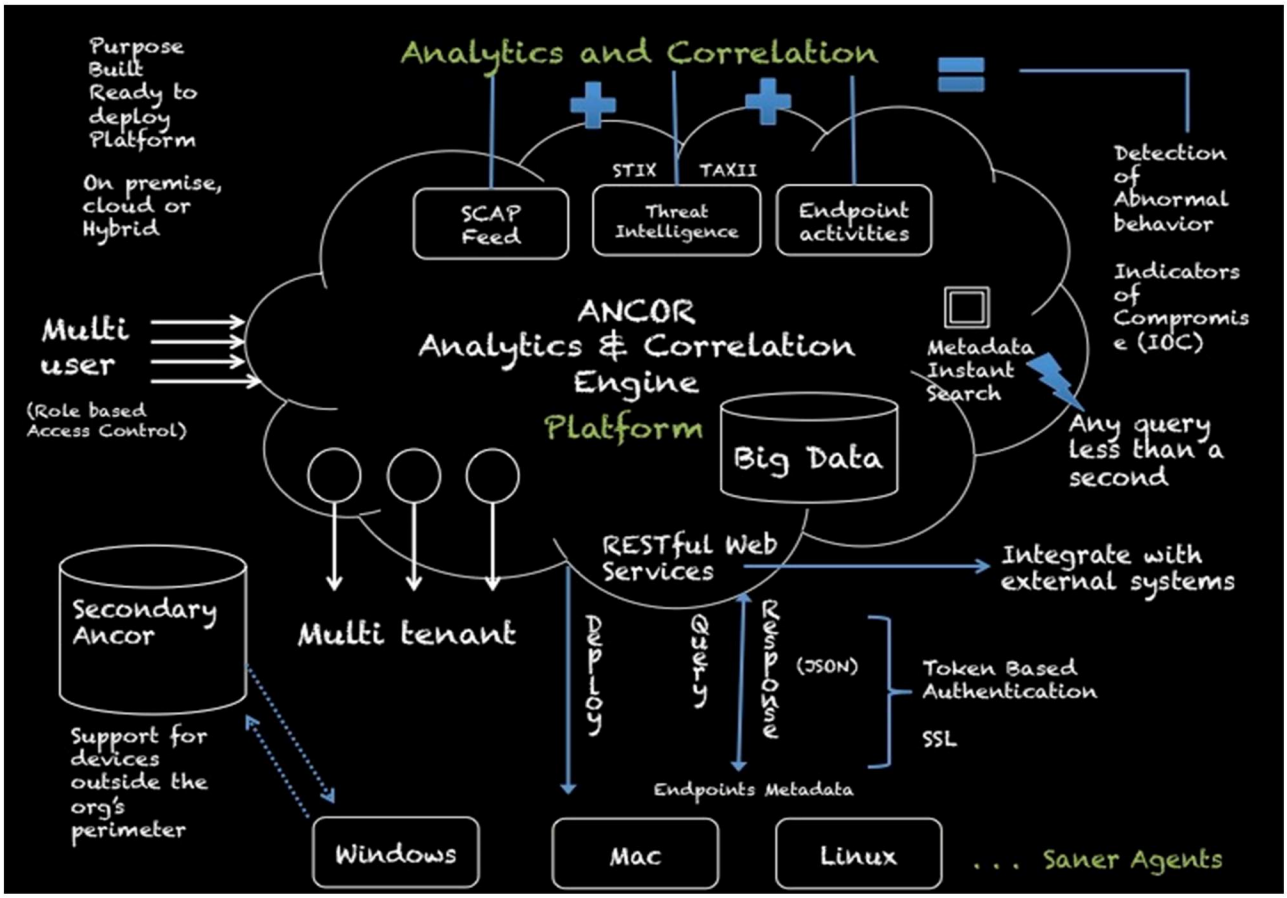


The solution must work across hybrid network of endpoints, offer speed and scalability, not hog network or system resources, and be extremely simple to deploy and use, and be resilient given the new definition of always-moving endpoints. SecPod Saner offers these capabilities like never before and helps automate the entire process lifecycle.



SecPod Ancor, our platform that makes it all possible

Ancor is a scalable analytics and correlation engine. SecPod's Ancor works with an agent residing on endpoint devices. Requisite data is collected and transmitted to the Ancor server located in the cloud or on premise. Ancor combines data from agents on endpoint devices, standards and best practices, vulnerability and threat intelligence, to provide real-time endpoint protection capabilities.



Analytics and correlation

Ancor operates on multiple sets of data to perform analytics. The data set include vulnerability and risk information, endpoint footprint that consists of various events data, vulnerability and risk indicators, and threat intelligence. Ancor correlates these data to uncover abnormal behavior and indicators of compromise.

Scalability

The platform is highly scalable to support large number of endpoints without having to rely on hierarchical server infrastructure. Based on a scalable BigData architecture, multiples of 10,000's of devices can be easily supported by a single server without performance degradation. Ancor is extremely light on network load consuming a very minimal network bandwidth.

Search-ability

Ancor searches through large set of structured data in micro seconds. The innovative metadata model makes it possible to search using unstructured natural language based queries with ease. Ancor is the only platform that is fully standards compliant to well-established standards such as SCAP, STIX/TAXII. The real-time endpoint data collected makes the solution scan-less. You never have to press scan button and you never have to search and wait for responses.

Multi-tenant, segregated data

A single server can manage multiple customer's endpoint data each compartmentalized neatly. Multiple segments of a corporate network can be managed by different users. Multiple managed accounts can be created with different accesses based on their role.

Beyond organization's boundary, perimeter less

Ancor ensures transient, perimeter-less devices that are part of organization's infrastructure are always protected and up-to-date. Ancor allows seamless support for such endpoints allowing migration of these devices from corporate Ancor server to the external facing zone server or the cloud deployed server, back and forth with ease.

Integration, Inter-Operability

The flexible architecture of Ancor allows integration with other systems. The REST APIs expose access to all the data points collected on the endpoints, threat and vulnerability information, IoCs including allowing search queries through these APIs.

Summary

An endpoint security story delivered through SecPod Saner provides,

- Proactive management of vulnerabilities and adherence to organizational security policies
- Visibility and control to endpoint activities
- Infrastructure to detect an on-going attack within the network
- Ability to receive threat intelligence from trusted sources and check its relevance
- Comprehensive response to an on-going attack

About Us

Founded in 2008 and headquartered in Bangalore with operations in USA, SecPod Technologies creates cutting edge products to ensure endpoint security. We strongly believe in the principle 'Strong Defense, Not a Weak Cure' and our product Saner Business reflects this ideology by proactively detecting and eliminating vulnerabilities before they can be exploited. We have been entrusted by Enterprise and mid level organizations in various verticals including Government, Healthcare and IT/ITES .

Contact Us

Web: www.secpod.com Tel: +91-80-4121 4020

Email: info@secpod.com +1-918-625-3023