STOP MALWARE FOREVER

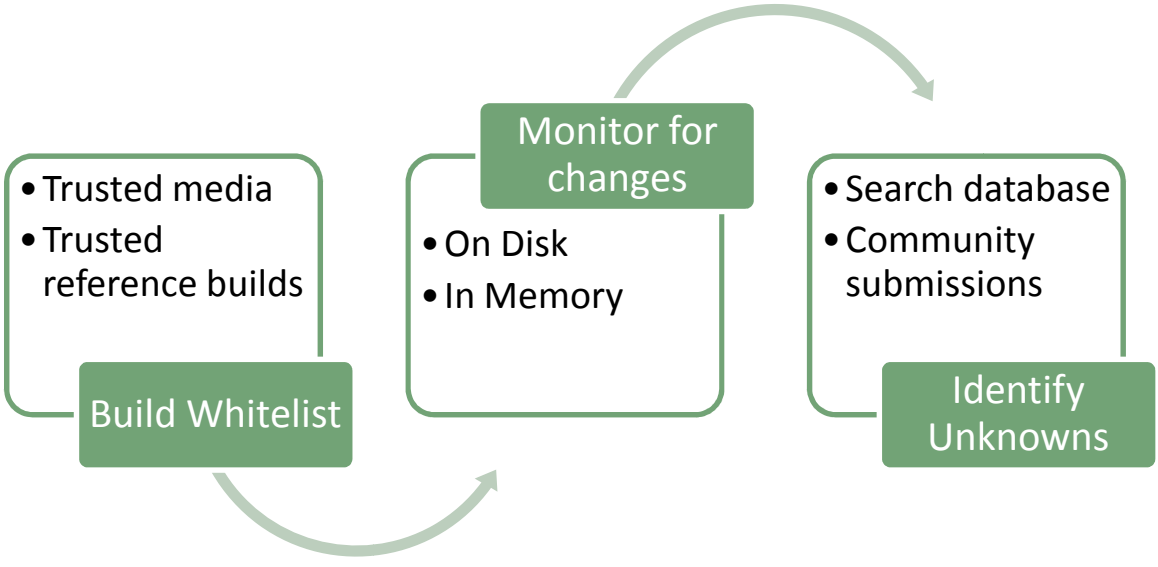
IDENTIFICATION IS THE KEY

Security Objectives takes endpoint security beyond reactively searching for known malware with unreliable signatures and behavioral methods. Enterprises can achieve software sovereignty and stay ahead of the threat curve by auditing systems for the presence of any unauthorized software. Our Pass The Hash solution reliably identifies what code is running, verifying that programs have not been modified in any way. The capability to precisely identify what's on your systems gives you the ability to locate, capture, analyze and eliminate everything from inappropriate software installed by your own personnel, to targeted viruses controlled by sophisticated attackers (i.e. organized crime participating in e-commerce fraud, hostile foreign governments, etc.) and everything in between.

TAKE CONTROL OF YOUR SECURITY

Conventional anti-virus companies attempt to thwart malware by selling you a subscription to an exhaustive signature list. It contains patterns or methods for detecting pieces of software your vendor arbitrarily deems malicious. It is compiled in secret and you are not allowed to examine it. Malware authors are receiving the same signature list as you and are constantly modifying their code to evade detection. This cat and mouse game has been going on so long that signature lists contain more entries than the number of legitimate software packages ever released. Some organizations are targeted by sophisticated adversaries able to create custom malware specifically for the current job. Signature lists don't help in such cases because of their reactive nature.

Pass The Hash is completely open, but malware authors can't know what you're looking for. It keeps no secrets from you because you supply it with all the information needed to maintain integrity. It doesn't matter if malware is written to specifically target your organization. You know what software makes up your infrastructure because you built it, therefore if you don't authorize software to be running then it shouldn't be. When unauthorized code is found it is not arbitrarily classified as malicious. The fact that unauthorized code was present is a policy violation all by itself. You can search our software database to identify code you don't know about internally without revealing that code to us. PTH never requires you to relinquish any of your trade secrets or internal data.



LESS SOFTWARE MEANS MORE SECURE SYSTEMS

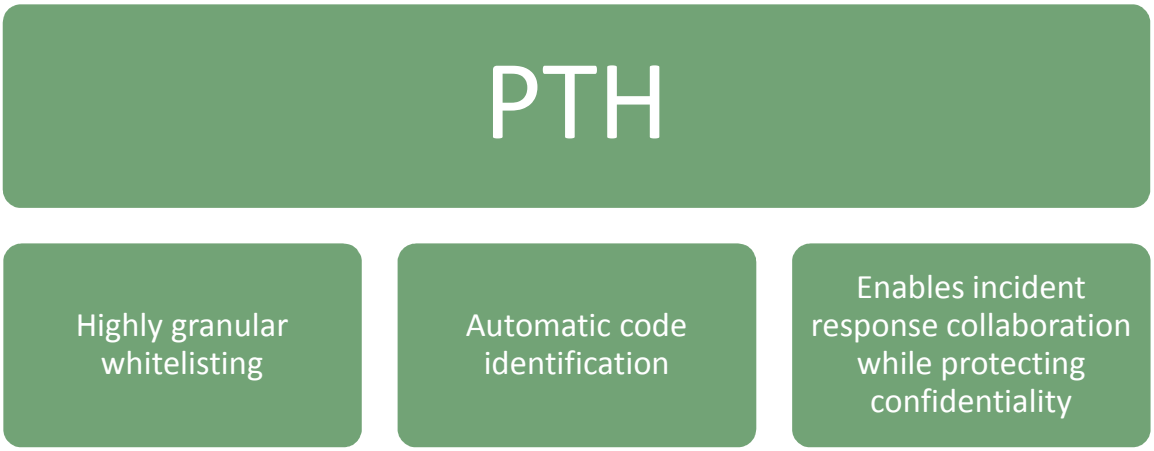
Traditional anti-virus engines must unpack/decrypt/disassemble and then scan a growing multitude of disparate file formats in order to perform the conventional signature matching scheme. This ever-increasing legion of data analysis functionality exposes systems to additional risks and expands attack surface area. A complex system with more moving parts is more likely to fail than a system that is elegant in its simplicity. As a result, the number of reported vulnerabilities in anti-virus software has dramatically increased in the past several years.

Pass The Hash simply calculates hash values that correspond to data so there's no need to parse a myriad complex file formats. It does this in a modular top-down fashion as opposed to basing a signature on the file in its entirety so if a virus mutates for example, it would still be recognized. PTH also has a facility for computing the integrity of applications or processes that are already executing on the system thus extending its verification utility to any type of in-memory data object.

WHITELISTING IS PROVEN TO SUCCEED AND BLACKLISTING IS PROVEN TO FAIL

Whitelisting is superior to blacklisting as the technique for identifying malicious software. Whitelists are also generally safer than blacklists as they are less prone to faulty encoding and pattern matching. Blacklisting is not only problematic and unsuited for the software integrity problem; it's also shown very limited practical success in other areas of information security. A case in point is that default-deny firewalls are clearly better at preventing unauthorized traffic when compared to default-permit firewalls.

Whitelisting known safe characters is effective at stopping dangerous meta-character vulnerabilities, while relying on blacklists of known dangerous characters is not. Once a malicious string becomes blacklisted, a natural counterattack occurs with polymorphous strings that can be re-encoded/compressed while still evaluating to some form of the original malicious string itself. Blacklisting may be easier to implement, but over and over it has been shown to be ineffective due to the practical impossibility of building a list of not only everything that is bad, but all possible representations of everything that is bad.



As part of their usage and security policies, many organizations do not permit the installation of software that is not included in a pre-approved inventory. Unapproved software leads to more severe security incidents and becomes an infrastructure management problem. Instead of constantly creating more signatures for new malware, a battle that is clearly unwinnable, Pass The Hash creates signatures for trusted software and then searches for unknown software. This approach greatly reduces the amount of work (human and computer) required to respond to the existence of unapproved software.