Vulnerability Management: Simplifying the complexity

Introduction to Vulnerability Management

Vulnerabilities are weaknesses in software, which can be exploited by attackers to gain control over computer systems, steal sensitive information and cause disruption of services. Vulnerabilities can be in the operating system components or software applications. Every year thousands of new vulnerabilities are discovered.

Malware is a bad software program that has been created with malicious intent. The intention could be to steal sensitive information, cause damage or financial loss to organizations or individuals, cause disruption of services, steal or misrepresent digital identities, disclose sensitive information, etc.

When a user clicks a certain link on a website, opens an email attachment, downloads games or other software, malware can install itself on the user's computer. Malware is able to be installed by exploiting vulnerabilities that exist on the computer. Endpoint server and desktop systems are the main malware targets.

About 90% of malware attacks make use of vulnerabilities that exist in computer systems.

To protect against these types of attacks, endpoint computers are generally equipped with anti-malware products. Anti-malware products work based on a "detection and cure" method. They try to identify malicious software programs by scanning the system and looking for all known bad programs or by looking for known bad behavior.

About 60% of malware are undetected or go unnoticed by anti-malware products.

A good security system needs to identify and fix weaknesses before an attacker exploits the weaknesses. This analysis has to be done continuously to ensure computer systems are secure and not vulnerable. This preventive measure needs to be applied prior to the "detection-and-cure" method.

Vulnerability management is about identifying weaknesses regularly and remediating those weaknesses. Vulnerability management is an important first step that needs to be taken to safeguard computer assets.

Vulnerability Management Challenges

There are practical challenges to implementing an effective vulnerability management system. The challenges are,

1. Vulnerability management is complex, it takes days to identify vulnerabilities and it takes weeks or months to remediate weaknesses. During this timeframe, systems are vulnerable to exploitation by attackers.

2. Vulnerability management products generally only scan for vulnerabilities. Remediation or patching is a separate job. This then requires another product to remediate issues, creating an integration effort, maintenance effort and additional cost for the organization.

3. The industry today works based on weekly/monthly/quarterly/yearly scans to identify vulnerabilities, which are generally not remediated because of the complexity involved in running the "scan-and-remediate" job on a regular basis. But, the reality is vulnerabilities are discovered and published daily.

4. Reporting is not meaningful and sometimes runs into thousands of linearly listed items that are not action oriented. It is a huge effort to understand the report and to create an actionable list of items to secure systems.

5. Available products are overly complex to use, complex to deploy, consume great amounts of network bandwidth and result in general management issues.

These complexities have hindered organization's ability to implement vulnerability management, even though it is necessary to secure endpoint computers.

The Big Idea – How SecPod Saner simplifies vulnerability management

The objective of a vulnerability management solution should be to,

1. Simplify the vulnerability management cycle to a routine daily operation without affecting operations. The task of scanning and getting a complete organizational security posture should be less than five minutes.

2. Simplify remediation. Discovered vulnerabilities should be remediated with ease. The idea is to couple vulnerability scanning with the ability to remediate vulnerabilities with just a click of a button.

3. Simplify reporting. Quickly search through reports and extract what is needed at ease through intelligent search queries.

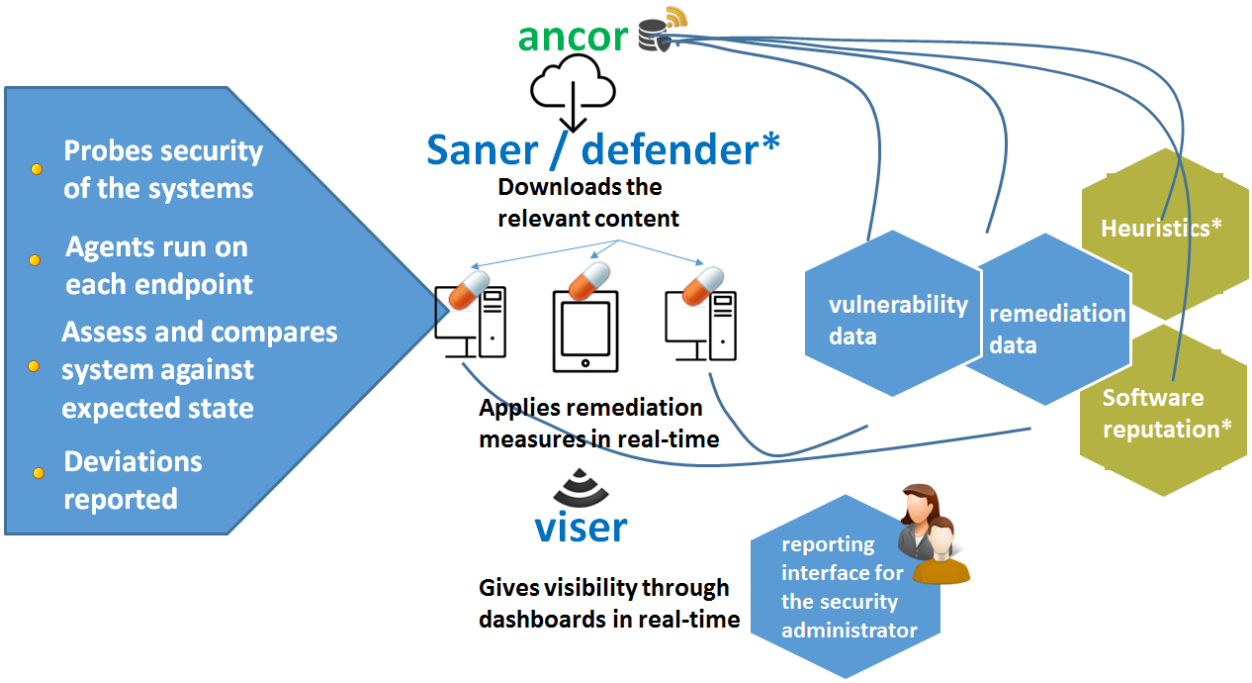
4. Reduce the Total Cost of Ownership (TCO) of a vulnerability management solution.

SecPod Saner incorporates these ideas.

SecPod Saner

SecPod Saner is a vulnerability management product that identifies security vulnerabilities and misconfigurations, and then remediates issues to ensure systems remain secure. It reduces the job of vulnerability management into a simple daily routine. It brings down the cost of the vulnerability management solution, is easy to deploy and easy to use.

SecPod Saner is an agent-based solution. Lightweight saner agents are installed on all endpoint systems. The agents scan the system for vulnerabilities and misconfigurations on a regular basis. The Saner agent consults SecPod Ancor for security intelligence and remediation data. Ancor ensures that the agent is constantly fed with new checks and patches. The solution includes SecPod Viser as an administrative console. Viser provides administrators with a consolidated view of the company's security posture. The Ancor server can be deployed in the cloud or on-premise.



Saner Features

Deep coverage
Addresses vulnerability and patch management, compliance and configuration errors.

Straightforward assessment
Provides comprehensive and easy-to-digest reports on all vulnerabilities.

Wide application support
Vulnerability remediation covering Microsoft products and vast number of non-Microsoft products including Java, SQL, Mozilla Firefox, Adobe®, Apple® iTunes, WinZip® and more.

Regulatory compliance
Ensures compliance with regulatory standards such as PCI, HIPAA, USGCB, NERC, NIST 800-53 and ISO27001.

Super-fast patching
Automatically identifies and installs security updates for every application.

Zero tolerance
Identifies and fixes policy violations automatically to bring the system to compliance state.

Send us an email today at
info@secpod.com

secpod