Endpoint Security Can Be Much More Effective and Less Costly

Here's How

Contents

Introduction

Organizations invest in many security products yet environments are subject to attacks and exploitation.

The footprint of most products expands with new releases and functionality, which increases complexity and training requirements. And a whole cottage industry has been created to provide user certifications to assert that a person is qualified to use a product.

Relying on more and more vendors increases the burden of procurement, installation and training. And yet, security and system management issues remain.

There has never been a scarier time to be a security professional than **right now.**

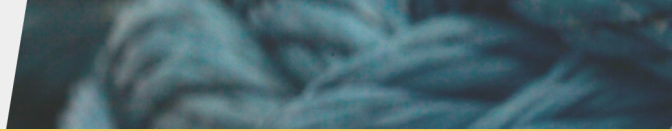
Why?

1 More is not always better

So many products: Organizations invest in multiple products, train employees, and manage activities, yet don't achieve security goals. IT environments and endpoints are still vulnerable to attacks and exploits.

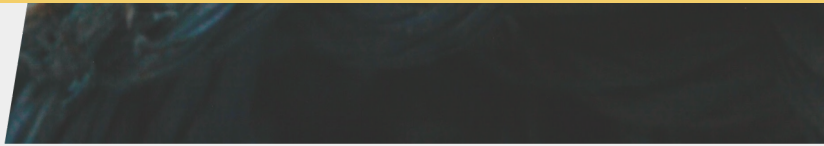
Unused feature-rich functionality: Most products have complicated or feature-rich functionality, but often only address a simple security challenge.

For each use case, a new product with overbearing capabilities is created. Though meant to simplify life and to secure the environment, the embedded complexity in many tools leads to their limited usefulness.



Companies invest in vulnerability management, patch management, compliance management, GRC solutions, endpoint management, EDR, asset management, and RMM.

Yet, so little security: Ransomware and other malware exploits are always in the news. Attackers exploit endpoints after penetrating perimeter and anti-virus protection. Unpatched endpoints are insecure and easily compromised. Current results illustrate a fundamental shortcoming in how security is being approached.



2 Escalating IT Security Budgets

So little value: Whether using a CapEx vs. OpEx model, purchasing multiple products with overlapping capabilities contributes to cost overruns. Generally, organizations are paying for unused functionality

Where is the money being spent

- Products
- Professional Services
- Maintenance and upgrades
- Training and certification
- Vendor and contract management

Investments are huge considering the cost of products, maintenance, professional services, training and vendor management.

Multiple vendors and multiple products contribute to unreasonable upfront and ongoing costs

3 Ineffective Management

- Attacks almost always use an unpatched vulnerability to exploit systems
- Patching is not a top priority
- Common belief is that patching is hard
- Endpoint users ignore or take several months to apply a patch
- Tools and processes are not simple and intuitive
- It takes weeks to deploy security solutions
- Security teams have to buy professional support, and pass certifications, but still get stuck in a ticketing rut

Today, some of the most critical IT issues deal with compromised endpoints. Ransomware and other malware attacks are continually in news headlines.

All too often, an organization doesn't have a clear view of their security posture and risk of being exploited. There is a general lack of visibility into and control of endpoints. 90% of successful attacks occur because of vulnerabilities and misconfigurations.

- **60% of malware is undetected, demonstrating the ineffectiveness of anti-malware solutions.**
- **Nearly all endpoints have critical vulnerabilities (frequently in the 100's) due to not having appropriate patches applied.**

Endpoint configurations frequently don't adhere to organizational guidelines and many businesses struggle to meet regulatory requirements.

Impact

Spiralling costs, untamed budgets, capital dollars wasted

CIOs & CISOs deal with many vendors, absorbing much of their time.

Need of the Hour

Building a computing infrastructure is now a speedy activity compared to a decade ago thanks to virtualization and cloud technology. But, IT management and security products haven’t kept pace. We can quickly provision a computing infrastructure, but struggle to secure it.

Just as a computing infrastructure can be provisioned, a similar approach is needed for IT management and security. A platform of tools, rather than many point products, will more effectively handle tasks. With task specific tools it would no longer be necessary to absorb the cost of product features that aren’t applicable or useful. Installation and training burden would pretty much go away. And with proper tools, security and system management concerns would be resolved.

System Management

Query, Monitor, Analyze, Respond

System Management

Typically, system management requires the functionality of ‘querying, monitoring, analyzing and responding,’ whether the system is simple or has multiple components that interact with each other.

The fundamental tasks of endpoint security management are:

Query the system to get visibility

Monitor for changes as they occur

Analyze the system for risks and threats

Respond to fix the issues

SecPod has built its SanerNow platform and toolset to address this need:

- Self-provision tools from the cloud
- Pay only for actual use of tools
- Keep things simple… no training classes or certifications required
- Provide tools for security and system management tasks

SanerNow

SanerNow is Software as a Service (SaaS). With no capital expenditure, a pay-as-you-go model allows payment for only used services based on the number of endpoints being serviced.

>> Automates the mundane

>> Is usable without the need to refer to user help documentation

>> Simplifies work using tools optimized to the task

SanerNow Platform: Ancor

Ancor is a scalable analytics and correlation engine. It works with the SanerNow agent that resides on endpoint devices to collect and transmit data to the Ancor server.

Ancor correlates the data from agents on endpoint devices with compliance standards, best practices, vulnerability and threat intelligence to provide real-time endpoint management and protection capabilities.

Key platform features include:

- ➔ Continuous monitoring: System controls
- ➔ “Principle of Self-Healing”,
  - ◆ Detect and fix vulnerabilities
  - ◆ Identify unwanted/unused assets and uninstall them
  - ◆ Monitor anti-virus program status, and start it if it is not running
  - ◆ Detect IoC/IoAs and respond to threats
- ➔ Speed: Deploy SanerNow in minutes, scan 1000s of endpoints in less than 5 minutes
- ➔ Scalability
- ➔ Multi-tenancy, multi-user and role-based access
- ➔ High-performance: Retrieve search results in less than a second
- ➔ Agents: Support for Windows, Linux and Mac OS X

SanerNow:
Business Cases

Vulnerability Management – Continuously assess risks, automated to a daily routine.

Patch Management – Apply operating system and third-party application patches for Windows, Linux and Mac OS X.

Compliance Management – Comply with regulatory standards benchmarks and achieve continuous compliance (PCI, HIPAA, NIST 800-53, NIST 800-171).

Endpoint Threat Detection & Response – Detect and Respond to Indicators of Attack (IoA) and Indicators of Compromise (IoC).

Asset Management – Discover and manage assets.

Endpoint Management – Manage endpoints and ensure their well-being.

Reduce up to 60% of the investment in endpoint security & management products

SanerNow: Benefits

Effective IT management and security

SanerNow is a platform with a variety of tools for managing and securing endpoints. It addresses security issues, whether it is fixing vulnerabilities, achieving configuration compliance, or killing a threat chain, etc. Most products merely report security issues, SanerNow fixes issues to provide real security.

Reduced Cost

Using tools from one platform rather than investing in multiple products can reduce overall endpoint management and security costs by up to 60%.

Ease of use; peace of mind

SanerNow is built for quick deployment and ease of use. Once agents are deployed most value is realized in less than 5 minutes irrespective of the number of deployed endpoints. Extensive training is not required to use SanerNow and its tools for managing and securing endpoints.

Where to from here

Please go to our **blog** that discusses this **ebook** and tell us what you think.

Tweeting about this eBook is fantastic and your comments are gems to us.

Thanks!