Enhance the MSSP Experience

secpod

Overview

In the modern enterprise, a proliferation of devices and the apps they can run has exposed the enterprise to an increasing number of vulnerabilities and threats. Controlling these ever-increasing endpoints and minimizing the risks they pose has become crucial to reducing enterprise IT risk. Managing this security in-house takes time and resources away from the core competency of the enterprise. A Managed Security Service Provider (MSSP) is therefore, an increasingly attractive alternative.

An MSSP provides outsourced services to monitor and manage the security of devices and systems in the enterprise.

This white paper discusses how the right technological solution can help MSSPs achieve efficiency while providing an effective and differentiated security solution to their customers.

The definitive goal of every MSSP is to deliver the utmost quality of service possible with the best solution.

MSSP Goals

The definitive goal of every MSSP is to deliver the utmost quality of service possible with the best solution. An MSSP should be able to use minimal resources to achieve maximum impact.

Offer Compelling Security Service

Address high-profile, critical market needs. Benefit from vast SMB and Enterprise service potential.
MSSPs do not have an easy task in the modern enterprise; their charter is to ensure the highest levels of protection so that organizations can focus on business-critical goals such as improving service availability and ensuring business continuity for their customers. Enterprise security is no longer perimeter-bound; an MSSP has to protect customer information and organizational data from unauthorized access while allowing users the flexibility of their devices, apps, and locations. This requires robust endpoint security solutions that can identify and eradicate threats before they reach the network. Lapses in security may lead to adverse high-profile publicity for their customers.

Increase Profit Margins

Maximize client value. Minimize technical resource cost.
Enterprises today are scalable, cross-platform, integrated, and agile. MSSPs therefore need solutions that are scalable, reliable, cost effective, high-performing, and support multi-tenant environments. Solutions that can help MSSPs monitor and control endpoints helps MSSPs increase client value and revenue, reduce costs, and maximize the profit margin.

Can I go back to my customer and say, I'll keep your systems vulnerability free on a day-to-day basis? Can I automate most of this activity?

Endpoint Security Challenges

The statement "it's a dangerous world out there" has never been more true. Enterprises face both unstructured and structured threats; cloud computing, numerous devices and apps, ingenuity of hackers, increasingly sophisticated security threats, and weaknesses in technology, configuration, and security policies. All this makes the MSSP task onerous. Retaining existing customers while acquiring new customers demands a high-level of automation in security management.

1. 90% of attacks stem from known vulnerabilities and mis-configurations in endpoint systems. It typically takes an enterprise 30-90 days to apply available patches. This provides a window of opportunity allowing attackers to exploit vulnerabilities. An MSSP needs to keep systems vulnerability-free on a day-to-day basis without disrupting business operations. Automating security solutions is the only viable means of achieving this.

2. Risk assessment and mitigation is not a onetime activity. As vulnerabilities become public and new attacks are introduced, an MSSP needs to provide solutions to defend against them. Assessment through vulnerability scanners and then a remediation exercise through other IT endpoint management/patch management software is not easy, adequate or effective. Investing in multiple tools to keep the enterprise safe is not viable; an integrated solution is essential.

3. Regulatory compliance requirements are designed to provide a safe environment for businesses. However, IT staff is overworked during audits and systems generally don't meet compliance benchmarks. The MSSP challenge is to always ensure compliance, making sure that the moment an endpoint device slips out of compliance, it is identified and rectified.

4. New attacks are discovered almost every day. Using threat intelligence, MSSPs need to prevent previously unknown attacks. Availability of a platform to inject threat intelligence and use it effectively in the customer environment can be a crucial differentiator. Additionally, MSSPs should be able to detect a threat within their customer environment by analyzing indicators of compromise.

5. An MSSP requires visibility to control and secure endpoint devices in an enterprise. Information on the OS of each device, applications installed, processes running, suspicious processes and the ability to block access to specific applications are crucial to providing a safe IT environment. Additionally, the ability to query endpoint systems can be a differentiator, especially in a vast organization with many endpoints.

Saner allows users to enter natural language-based queries. With over 80,000 built-in queries to detect the system state.

Unlocking Customer Problems with Saner

The Saner Business endpoint security solution with its features of real-time visibility, risk mitigation, regulatory compliance, and threat detection and response provides an ideal platform for MSSPs to provide best in class security solutions. The Saner Platform helps MSSPs maximize client value while minimizing resources they deploy.

Proactively Secure Endpoints

More than 90% of security breaches take advantage of known vulnerabilities present in systems. Saner proactively detects vulnerabilities and automatically remediates them. Misconfigured systems provide another avenue for attacks. Saner can be deployed to detect deviations from strict enterprise configuration norms and bring systems back into compliance. With its ability to inject Threat Intelligence, Saner provides a comprehensive platform for quickly responding to ongoing attacks and detecting and responding to compromises.

Automate Compliance

Saner collects vulnerability and compliance status in real-time. This makes it possible to ensure endpoints always remain compliant. With this information it is possible to ensure organizational guidelines, such as, prohibited applications and hardening measures are enforced on all devices. Compliance to regulatory requirements can also be easily automated using Saner.

Ensure Real-Time Visibility and Control

With Saner, it's easy to know the security posture of all endpoints within seconds from one convenient dashboard. SecPod Saner provides continuous visibility and control of endpoint systems. Real time information on vulnerabilities, missing patches, running processes, active services on endpoints, file information, security events, network connections, installed software, and devices are available on the dashboard. Saner proactively remediates risks by correcting deviations almost instantaneously. Using available threat information, Saner detects and responds to threats by instantaneously containing or blocking an attack.

Use Natural Language Queries to Identify and Respond

Saner allows users to enter natural language-based queries. With over 80,000 built-in queries to detect the system state, Saner responds to queries in seconds. Queries can be run based on an attack symptom to detect abnormal behavior or an on-going attack. Threat intelligence can also be fed from trusted sources to check the relevance of an attack in the form of STIX/TAXII, OpenIOC, and Yara. Complex queries can be created, or multiple queries can be defined with AND and OR combinations.

Saner Business endpoint security solution is a platform that offers remarkable speed and scalability to support a number of customer accounts with one server.

Saner Advantages

Saner Business is designed for MSSP growth. MSSPs can easily meet customer needs with the following:

Product Branding

MSSPs can brand Saner with their logo.

Multi-tenant Support

Saner Business enables MSSPs to manage multiple clients from one dashboard and support many clients on one server.

MSSP Service Reports

The MSSP Service Reports illustrate the client endpoint security posture, and also the actions taken by the MSSP to patch/ harden systems and to respond to threats.

Cloud Deployment

Saner's offering with Amazon, Google, Azure and other virtualization software helps to deploy applications on the cloud.

Quick and Easy Installation

Customer evaluations take place in minutes and the server installation is completed in two hours.

Licensing/ Price

Monthly subscription is available with no up-front costs. Subscriptions are based on managed and deployed endpoints across all clients. Technical support, security intelligence, and upgrades can also be delivered. The cost per endpoint is minimal.

Summary

Managed Security Service Providers face multiple challenges today – The number of endpoint devices is growing fast; attacks are on the increase; new attacks are being launched at an alarming pace; visibility and control of endpoint devices is imperative for a successful security solution. As the needs of managed security service providers continue to change, the Saner Business solution helps MSSPs enhance their productivity and provide customers a reliable, successful security service. SecPod's advanced MSSP solutions help managed service providers attract new clients by providing a compelling security service at lower cost. MSSPs have a competitive advantage with the Saner Business solution. Saner Business helps MSSPs increase their client base, retain existing customers and increase profit.

Learn more about the SecPod MSSP Partner Program.

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