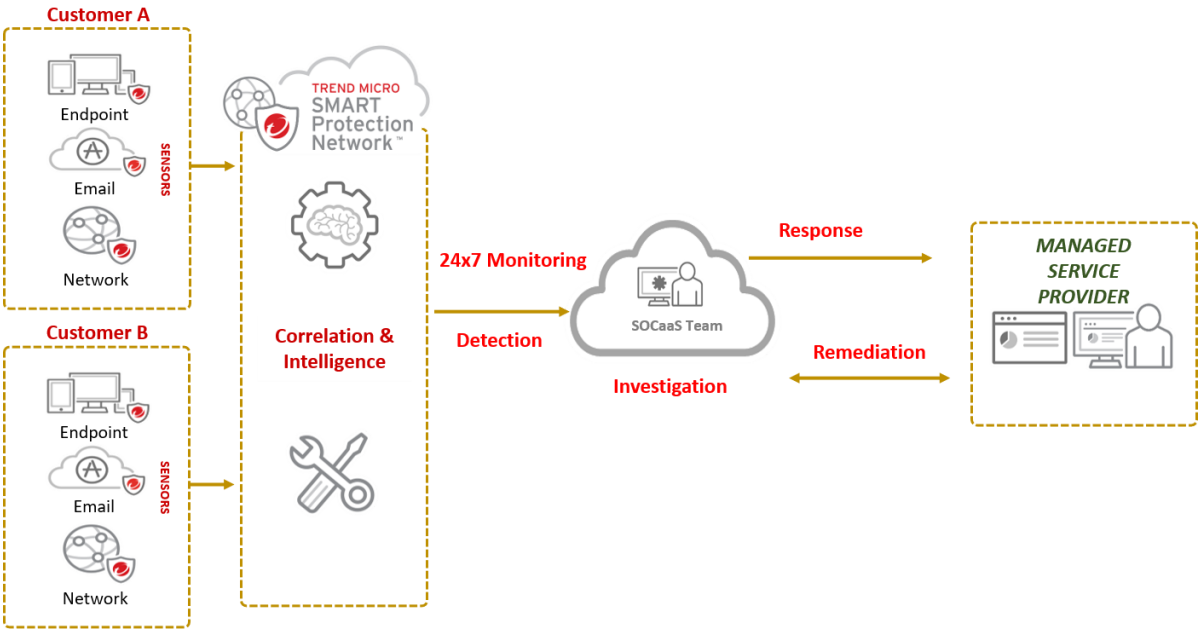
MSP's Guide to **SOC-as-a-Service**

TREND MICRO™

SOCaaS: An Outsourced Security Approach for MSPs



SOCaaS, or Security Operations Center as a Service, is essentially an outsourced security approach, and this approach combines technologies such as endpoint detection and response (EDR), machine learning, automatic data correlation, and IoC sweeping along with a team of security experts.

The key element to this approach being the people element, and more specifically, access to security experts and analysts. The idea of SOCaaS is to incorporate all the benefits of a fully built SOC without the high investment -- whether that's investment in time, people, or money to build one.

The reality for many MSPs is that building out a SOC to deliver scalable and profitable managed detection and response services is not practical.

The term "co-managed" and how it relates to SOCaaS

This is a co-working model where both the SOCaaS provider and the MSP collaborate with a shared responsibility to secure clients. In this model, the SOC team becomes an extension of the existing IT staff where the security services being delivered to the client are transparent.

The SOCaaS provider does all the security heavy-lifting at various stages of the cybersecurity framework – whether that's in the detection, investigation, or response phase.

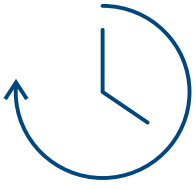
Meanwhile, the MSP manages all of the client communications and relations.

This working model ensures that the MSP always stays in the value stream with their clients.

An Elevated Level of Protection

The challenge many MSPs experience today is that detection and response requires a significant amount of time and resources for investigating threats. This guide explains the concept of SOCaaS, how it can help solve detection and response obstacles, and what to consider when evaluating vendors.

A security breach is inevitable even with the best and broadest preventative technologies in place. The reality is not all malicious activity can be stopped, and as recent and well publicized breaches have demonstrated, the longer it takes an organization to detect and respond to an incident, the more severe the consequences. This reality has made SOCaaS offerings attractive to both clients and MSPs.



Most organizations are spending hundreds of hours a week investigating suspicious alerts. Despite hundreds of hours devoted to alert investigation, 17% are not investigated at all.
– IDC

The sophistication and commonality of these attacks are a top concern from all types businesses across the world, including SMBs. Clients, regardless of size, are expecting an elevated level of protection. The good thing for MSPs is that their clients are willing to pay for it, so this brings forth a lot of opportunity as SMBs continually turn to MSPs to close security gaps.

The client's viewpoint on cybersecurity has also shifted, so they no longer view their security posture as a checkbox. Businesses recognize that traditional and defensive approaches only go so far, and a more offensive posture must be incorporated.

MSPs are in the business of assuming client risk, and SOCaaS is a solution that many are evaluating as a way to diversify the risk.

Business outcomes MSPs can expect from a SOCaaS solution

There are many business outcomes you can expect from leveraging a SOCaaS solution, some more tangible than others, but don't disregard the intangibles - they're just as important.

Team Augmentation

MSPs feel the pressure as a result of the IT personnel shortage, and SOCaaS offerings enable them to better focus their existing IT resources on mission critical initiatives. It's also an uncomplicated way to augment their team by bringing in security expertise without the associated expense and extend their security operations to 24x7.

Operational Efficiency

SOCaaS offerings help improve overall cybersecurity operational efficiency. For example, it ensures MSPs can respond to, and contain, client security incidents more quickly as well as create an opportunity to centralize and connect information across security layers and clients.

New MRR Streams

These services help MSPs tap into new opportunities by extending their managed security services portfolio and creating new MRR streams. It essentially acts as a gateway into larger accounts that may have more demanding security requirements.

Peace of Mind & Customer Retention

It's hard to put a dollar amount on an intangible like peace of mind, but it allows MSPs and their clients to rest more easily knowing that a team of skilled experts are constantly monitoring their security posture. Additionally, these high value services are a lot stickier and make it less enticing for clients to switch providers.

Considerations for MSPs when evaluating vendors

There are a lot of new players in the market, and cutting through the noise can be very difficult, but these are some of the questions an MSP should be asking:

01

Is the service a co-managed solution?

From a client perspective, the service should be viewed as an extension of your service delivery team.

02

Is the service multi-tenant?

As multiple clients are underneath your company's management, cross-customer threat detection and response capabilities become necessary, and without them, visibility and the ability to respond across multiple clients is very limited and operationally inefficient.

03

Which technologies does the service utilize? EDR? XDR?

Make sure the technology is flexible and capable enough to grow with your business and meet your requirements.

04

Are those technologies included in the price or must they be purchased separately?

Some services tack on an extra cost for more advanced technologies.

05

Does the service include threat hunting, incident response, and investigation?

Some of those services are really a "monitor and notify-only" type of service.

06

What are the procurement terms?

Are there lengthy contracts involved? Ask whether upfront capital is required, and consider whether the procurement terms for this service align with how you and your customers expect to be billed.

Partnering with Trend Micro

Trend Micro's solution is truly co-managed so MSPs maintain control over the interactions with their customers. As part of the incident response service, Trend Micro's 24/7 threat experts can provide customized recommendations or remediation actions if authorized by you.

This service provides proactive threat assessments across the MSP's entire customer base and protects multiple customers at once. Additionally, our threat analysts review similar threats across partners, especially those in the same industry, to provide proactive response.

Trend Micro views the MSP partnership as more than just product and economics. It's about closing security gaps, open communication, and long-term focus on people and partnerships. We're an expert in security and an advocate for MSPs so your focus can be on supporting your customers and running your business.

Contact Us

www.trendmicro.com/msp

msp@trendmicro.com

888.977.4200

Threat detection and response across multiple attack vectors by Trend Micro. **Created with real data by artist Brendan Dawes.**