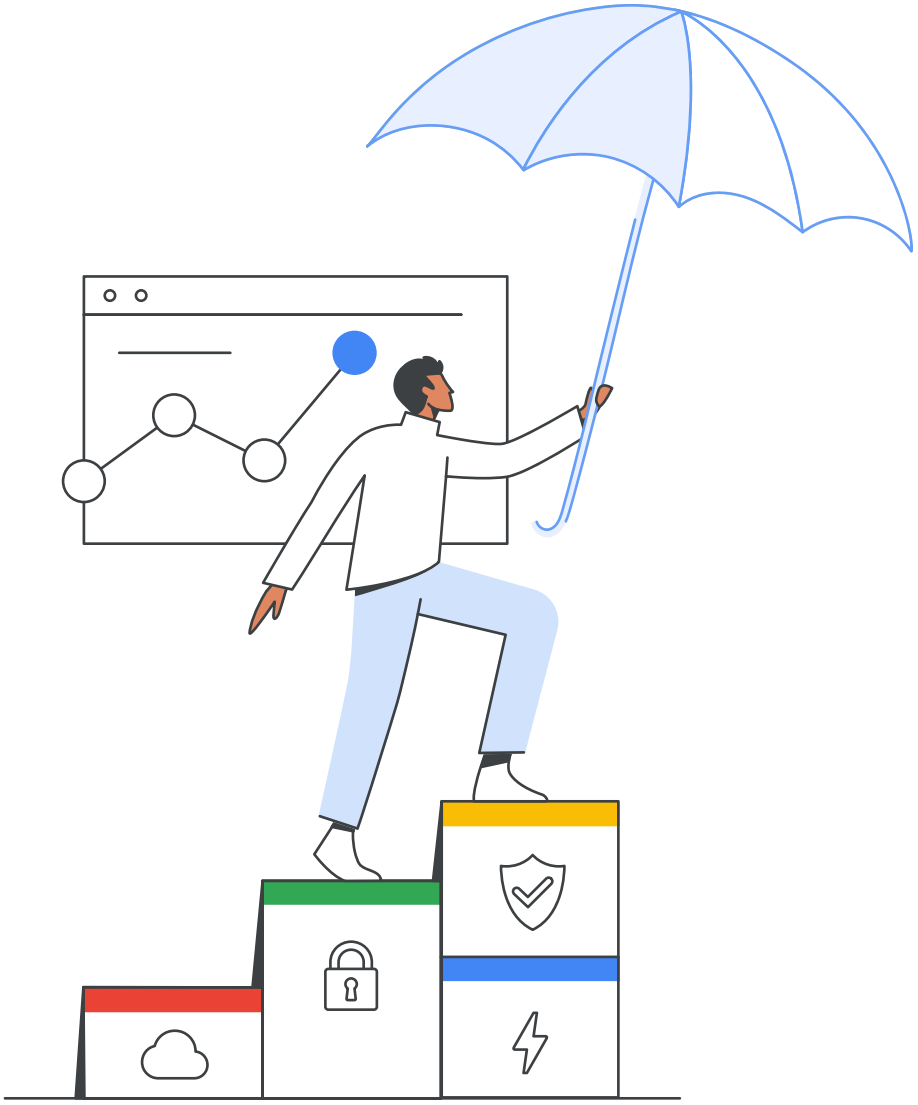
Google Cloud

White paper



The All-in-One Guide to Maturing Your MSSP

How managed security services providers can stand out from the competition and drive revenue growth

Google Cloud

Introduction

Cybercriminals are relentless, professional, and organized, and will stop at nothing to attack organizations. Meanwhile, many of their targets are becoming more attractive by the day as organizations welcomely embrace digital transformation through mobile, IoT and cloud adoption, all leading to greater risk exposure, blind spots and potential security incidents like sensitive data loss.

One of the results of this perfect storm: Managed security services providers (MSSPs), sometimes referenced as managed detection and response (MDR) providers, are being greeted with more opportunity than ever to grow their business. In addition, more and more managed service providers (MSPs) are transitioning to MSSPs in hope of capitalizing on the rising demand for cybersecurity solutions worldwide.

The global maanged security services market was valued at $22.5 billion in 2020 and is expected to grow to $77 billion by 2030.[1] MSSPs are quickly realizing, however, that differentiation is becoming exceedingly difficult in a fast-paced, rapidly evolving market.

In this white paper, we examine MSSPs, reasons why MSPs become MSSPs and challenges that MSSPs face. We also provide actionable insights and recommendations to help MSSPs differentiate themselves from rivals as compeition grows. This includes ensuring they are conditioning staff to more efficiently handle security incidents and incorporating the right security solutions into their portfolios. Finally, we close with a discussion of technologies that help MSSP security operations

[1] ResearchAndMarkets.com, "Managed Security Services Market by Deployment Mode, Enteprise Size, Application, and Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2021-2030," March 2022.

60% of security professionals believe their organization is at moderate or extreme risk due to a lack of security staff.

Why do organizations partner with MSSPs?

When it comes to data breaches, no organization wants to become the next major headline — i.e. a globally recognized brand that sustains revenue losses and brand reputation damage due to its inability to secure customer data. Yet few organizations possess the appropriate skills, time and budget to prioritize security.

Enter MSSPs — in many cases considered one-stop shops for all things security. Here are five reasons why global organizations partner with MSSPs:

Comprehensive protection

Let's face it — cybercriminals have many opportunities to launch attacks, and they use advanced hacking methods and tools to penetrate IT systems. Conversely, organizations are tasked with protecting their endpoints and networks against a wide range of attacks.

Failure to account for attack vectors can cause long-lasting problems for an organization, its employees and its customers. Fortunately, MSSPs understand the threat landscape, and they provide organizations with comprehensive protection and visibility of cyber risks. Plus, MSSPs frequently update their portfolios to ensure that organizations can secure their systems and data against emerging threats.

Expertise

A recent IT security workforce survey indicated that the global cybersecurity workforce must grow 65% to effectively protect the critical assets of organizations.[2] In addition, the survey revealed that approximately 60% of security professionals believe their organization is at moderate or extreme risk due to a lack of security staff.

[2] (ISC)², "2021 Cybersecurity Workforce Study," May 2021.

Today's organizations are competing for top talent, yet aptitude alone offers no guarantees. In fact, organizations must provide security training to keep staff and customers up to date on new cyber threats and how to swiftly detect and deter them — or risk falling victim to sophisticated attacks. Organizations must comply with local, federal and international data security laws and teach staff and customers about these mandates as well. And if an organization experiences a data breach or even a potential breach, it must notify all affected stakeholders and revamp its security training programs and protocols accordingly.

MSSPs hire security experts who understand what it takes to protect an organization, with many offering around-the-clock guidance and monitoring. Also, MSSPs typically provide in-depth training to keep employees up to date on threats.

Cybercriminals will only grow more sophisticated as exemplified by their use of advanced technology like artificial intelligence, evasive techniques that are difficult to detect, new data exfiltration features and attack methods involving multiple phases and platforms.

Through breach investigations, threat intelligence feeds, telemetry captured from their security technologies and potentially in-house research, MSSPs are privy to exponentially more information than their clients would have without them. Specifically, they have a greater and more nuanced understanding of the attack landscape because they are exposed, in some cases, to thousands of different customer networks and engage with all of their security incidents.

State-of-the-art technology

Every organization is different, and there is no one-size-fits-all technology stack to accommodate their security requirements. Meanwhile, not all technology is created equal, and identifying the right strategy for an organization can be challenging.

Differentiating one service or solution from another is rarely simple, and buyers lacking internal capabilities can sometimes find themselves in a situation in which a purchase quickly becomes so-called shelfware because they are unable to successfully deploy it. Thanks to MSSPs, organizations can adopt best-in-class security technologies to protect their systems and meet compliance requirements.

An MSSP can perform an audit to identify an organization's cybersecurity gaps and offer personalized technology recommendations. Then, an MSSP can deliver services that work seamlessly in conjunction with an organization's existing security tools.

Cost savings

The average security professional in North America earns an annual salary of about $91,000.[3] But a global shortage of practitioners often makes it difficult for a small organization to generate interest from top talent — or, the organization may need to reallocate funds from its limited operating budget to meet the salary requirements of top cybersecurity talent.

Let's not forget about the costs of office space, training and benefits for in-house security professionals, either. These costs add up quickly, and they sometimes prevent small organizations from getting the help they need to combat cyberattacks.

MSSPs enable organizations — regardless of size — to implement and manage security solutions without having to worry about the costs associated with finding, hiring and retaining in-house security personnel. In doing so, MSSPs not only tailor a security program for the needs of individual clients, they also can deliver a return on investment.

Time savings

Security can be cumbersome, particularly for an organization with limited time at its disposal. For instance, an organization must find the right technologies based on its budget and IT requirements. The organization must also implement these technologies and teach employees how to use them. After the process is complete, an organization may still experience a data breach or some other security incident if it does not maintain and update its security solutions.

The time it takes to recruit, hire and train security personnel can be significant, too. It may take many weeks or months to identify top talent and onboard new personnel. Furthermore, an organization will need to educate this incoming staff about how its program functions and provide access to various systems and data.

MSSPs help offset this time-consuming responsibility by working within an organization's specifications and timeline. It can even reduce or eliminate the time that an organization requires to recruit, hire and train in-house security staff.

Flexibility

A notable draw of MSSPs is they do not have to handle all of an organization's security. So-called hybrid models permit a company to contract with an MSSP and still retain its own team of infosec professionals. Perhaps a business wants to offload its mundane and tedious security tasks (for example, logging and firewall management) to a third-party so it can instead concentrate on more strategic, revenue-generating security projects. On the flip side, maybe an organization lacks the requisite in-house talent. In that case, they may turn to MSSPs to help address the more complex disciplines they desire, such as threat hunting and incident response. Or an organization may call in an MSSP simply for part-time work, such as off-hours threat monitoring.

3 (ISC)², "2021 Cybersecurity Workforce Study," May 2021.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus ultricies convallis nibh, non eleifend arcu ornare quis. [C3]

Why do organizations partner with MSSPs?

Clearly, there is a lot to like about the MSSP business model, especially in an era where every single business is at risk of an attack, bolstered by emerging cloud threats, and needs to take a proactive stance. Thus, it is easy to understand why many MSPs are transitioning into the managed security services market.

MSPs help organizations bridge technology gaps and perform routine IT tasks related to networks, servers and applications. If they venture into the world of security, it is to perform basic duties like installing firewalls or anti-virus. But as more companies embrace digital transformation, the number of MSPs has increased globally. At the same time, these providers have explored new opportunities to enhance their portfolios, driven by the demand for more advanced security amid an ever-widening security skills chasm.

The number of MSPs transitioning to MSSPs is growing, and they are doing it for three big reasons:

Gain a new revenue stream

MSPs generally help organizations keep their IT systems running at peak levels, but they are limited in applying that same proactive attention to a client's security stance. Or in the event of a cyberattack, MSPs are often not equipped to address the causes of the incident and respond to the ramifications, thus missing out on opportunities to support organizations that require protection.

MSSPs, on the other hand, can capitalize on these opportunities. They can offer a variety of security solutions — everything from the basics such as anti-malware to disciplines requiring more advanced skills, like penetration testing and incident response — to generate newfound revenue.

Grow customer loyalty

Businesses sometimes partner with MSPs that provide IT operations support but cannot handle their cybersecurity requests. They may also work with MSPs and MSSPs to get the right combination of IT operations and security support.

MSPs focus solely IT operations — or can become MSSPs that deliver IT operations and security support. MSSPs can make it simple for organizations to manage their digital environments and safeguard systems and data against attacks.

"Stickiness" often plays a key role in an MSP's decision to become an MSSP, too. Once the transition occurs, its value immediately increases, as it can provide a large collection of services to a customer. Since it is much easier to work with a single provider of security and other services, it is more likely that a customer will "stick" with an MSSP over time.

Respond to market needs

Managed security services are popular — and for good reason. They help organizations combat threats, as well as quickly identify and address breaches.

MSSPs can become the experts, if they dedicate the time and resources to perfect their craft. Because if MSSPs understand the ins and outs of cybersecurity, they can impart that knowledge to clients. MSSPs can then identify IT infrastructure and security challenges simultaneously and deliver positive outcomes that far exceed those provided exclusively by an MSP.

Google Cloud

What obstacles do MSSPs face?

Operating in the managed security services marketplace may seem overwhelming — if an MSSP makes even a single mistake in its efforts to deliver security services, it risks brand reputation damage, revenue losses and compliance penalties. But these impediments can be overcome if an MSSP understands the challenges from the onset. Some of the most common impediments that MSSPs face include:

Talent recruitment and retention

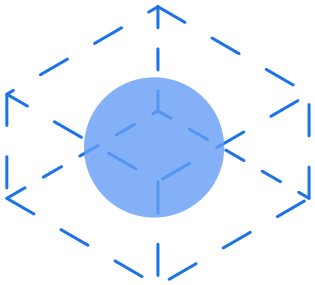
Global organizations are struggling to recruit and retain top security talent, and MSSPs are dealing with the same issue. To address this problem, MSSPs should prioritize internal cyber training. MSSPs can develop training programs to teach employees about different technologies. With a training program in place, certain MSSPs may be better equipped than their industry rivals to attract and retain talent too. Later on in this white paper, a section is devoted to the type of industry certifications MSSP security analysts should consider obtaining, making them more attractive for prospective clients.Look for gaps in your detection use cases, especially gaps that exist due to inability to collect and retain telemetry data.

Increasing customer acquisition costs

With the proliferation of security technology options, customers' security stacks are more diverse than ever before. In addition, the rise of cloud adoption —and its ensuing risks — is creating new requirements and capabiltiies from providers. To compete, MSSPs must be willing and able to sufficiently support a broad set of technology that often results in higher acquisition costs, as well as increased training requirements for security analysts.

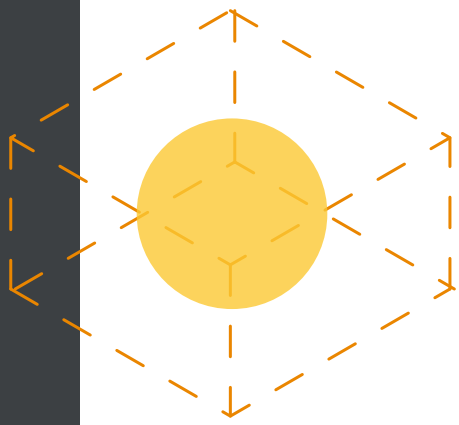
Lack of centralized visibility

Analyst teams who manage and monitor a large customer base often lack visibility into the allocation of resources, which hinders their ability to balance productivity and risk. This visibility void often extends to the customer as well. Clients are yearning for greater visibility into their expanding network (which has grown to be increasingly cloud based), more transparency around what is happening within it, and, most of all, the ability for an outsider provider to do more than simply notify them about a threat. Customers care more than ever about positive outcomes from their providers, which means finding, disrupting and eradicating adversaries and helping get their affected business back on its feet as quickly as possible.



Multiple delivery models

The range of MSSP delivery models is increasingly diverse and includes: 24/7 outsourced SOC, managed SIEM, MDR, staff augmentation, as well as numerous hybrid models. These various models are converging – a single MSSP may provide multiple models in various configurations, adding cost and complexity to operations.



Increasing Competition

Once upon a time managed security was merely an emerging trend, and there were limited options for organizations that wanted to outsource their security. Today, managed security services are in high demand, and organizations have many options as they search for outsourced support.

MSSPs must assess the security landscape and identify their target audience. Even if an MSSP offers multiple services, expert staff and top-notch technology, it must always put the customer first. This can help an MSSP generate sales leads, accelerate its revenue growth and differentiate from rivals.

An MSSP Checklist

Differentiating one MSSP from another is often challenging, due in part to the fact that many such vendors deliver the same outsourced monitoring and management of security devices and systems to global organizations. If an MSSP can differentiate itself from rivals, however, it can boost the likelihood of long-lasting market success.

Here are some baseline reccomendations for how MSSPs can set themselves up to stand apart from the crowd:

Earn Industry Certifications

- ☐ Encourage certain staff to obtain the following industry certifications, which will help demonstrate domain-level expertise and elevate customer confidence
  - ○ ISO27001: Information security management system (ISMS) specification that focuses on the legal, physical and technical controls of an organization's information risk management program
  - ○ SOC 2: Customer data management certification that emphasizes availability, confidentiality, privacy, processing integrity and security
  - ○ CISSP: Certification for security executives, managers and practitioners that covers the following domains: asset security, communication and network security, identity and access management (IAM), security assessment and testing, software development security, security operations and security and risk management
  - ○ GIAC: Collection of more than 30 security Certifications that highlight an individual's expertise with security administration, management, legal, audit, forensics and software security
- ☐ Bonus points if the team includes industry-recognized individuals who regularly blog and participate in conferences.

Train Employees at Every Level

- ☐ Provide security training to employees across all departments
- ☐ Focus training on developing skills for detection and response to reduce attacker "dwell time" within client enviornments.
- ☐ Perform security testing to evaluate an employees' skills
- ☐ Establish a training schedule
- ☐ Update the training program at regular intervals throughout the year

Invest in Customer Service

- ☐ Establish a designated point of contact who understands customers' business and technical requirements
- ☐ Find out when and how customers want to be contacted for alerts
- ☐ Create a customer portal that allows customers to view alerts and reports on demand
- ☐ Provide customer service training to all employees
- ☐ Enable customers to reach out via email, phone and other contact methods 24x7
- ☐ Encourage employees to listen to customers and empathize with their concerns
- ☐ Follow up on customer requests via email or phone
- ☐ Request customer service feedback
- ☐ Track customer service requests and complaints
- ☐ Generate customer service reports and use them to identify areas in need of improvement

Be Transparent and Accessible When Selling

- ☐ Avoid jargon and complex language when explaining security technologies and contract terms to prospects and customers
- ☐ Create a website that is easy to follow and makes it simple for prospects and customers to reach out as needed

Condition the Customers Well

- ☐ Craft a personalized security training program for each customer
- ☐ Perform on-site training sessions that offer insights into different types of attacks and their potential impact on an organization
- ☐ Provide tests to assess security awareness
- ☐ Schedule regular training sessions
- ☐ Evaluate the effectiveness of the training program at different times throughout the year
- ☐ Update the training program at least twice a year

Learn About a Customer's Business

- ☐ Meet with a customer (preferably on site) to learn about their business and the security challenges they face
- ☐ Perform a full-scale audit to identify security gaps within a customer's IT environment
- ☐ Offer an automated vulnerability scan to identify potential security and compliance gaps
- ☐ Listen to their challenges before speaking or making suggestions. This cannot be emphasized enough.
- ☐ Offer personalized recommendations

Develop and Maintain Service-Level Agreements (SLAs)

- ☐ Create a well-written SLA that defines and documents the managed security services being provided. (Note: SLAs can act as a competitive differentiator, and applying automation can make the process more seamless and help your customers keep up with changes and help you quickly identify potential breaches of contract.)
- ☐ Include the following service availability provisions:
  - ○ Definition of service availability
  - ○ Time period used to measure availability
  - ○ How availability is calculated
  - ○ Percentage of availability promised
  - ○ Ramifications of availability failures
- ☐ Provide details that define MSSP responsibilities and where those responsibilities end

Provide References

- ☐ Ask past customers to serve as references
- ☐ Verify customer reference contact information and the best way to reach them
- ☐ Create a customer reference list and offer the list to prospects
- ☐ Update the reference list regularly

Establish a Seamless Customer Onboarding Process

- ☐ Assess a customer's existing security tools
- ☐ Evaluate a customer's security requirements
- ☐ Provide a managed security services quote
- ☐ Establish an agreement that includes a managed security services quote and deployment timeline
- ☐ Implement managed security services and document all relevant customer activities
- ☐ Perform a final assessment and provide a customer with documentation to verify that all required tasks have been completed
- ☐ Set up contact points within a customer's organization

Provide Security Reports

- ☐ Offer daily activity, maintenance and incident reports, as well as monthly summary security reports
- ☐ Follow a standard report format that includes an overview, sequential outline and short- and long-term security recommendations
- ☐ Use clear, concise language in each report that is transferable to executives
- ☐ Proofread and edit each report

Leverage Best-in-Class Security Technologies

- ☐ Determine which managed security services to provide and what technologies are necessary to support them
- ☐ Evaluate multiple security technologies and the vendors that provide them
- ☐ Request security technology vendor references and reach out to them for additional insights
- ☐ License best-of-breed security technologies that align with an MSSP's mission and goals
- ☐ Consider developing and providing homegrown security technologies, including solutions that can support detecting and responding to both on-premises and cloud-based threats. Are you cloud-native? That will help.

Prioritize Threat Intelligence

- ☐ Collect and analyze threat data across client IT environments
- ☐ Identify threat trends and patterns
- ☐ Produce custom threat intelligence reports for customers
- ☐ Provide data-driven recommendations to help customers guard against threats
- ☐ Deliver Round-the-Clock Monitoring and Visibility

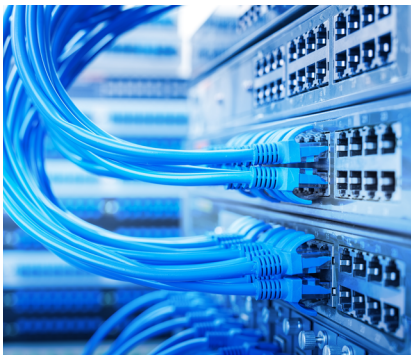
Deliver Round-the-Clock Monitoring and Visibility

- ☐ Deploy systems to track customer network and endpoint activity 24/7
- ☐ Perform ongoing security vulnerability scans and software patching
- ☐ Automate customer data backups and store and secure critical information in the cloud
- ☐ Remediate vulnerabilities as soon as they are detected

Offer Advanced Capabilities

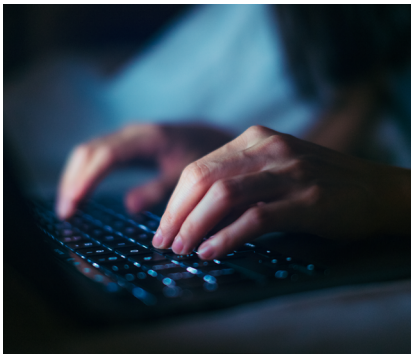
- ☐ Provide actionable incident response and remediation. if an incident occurs, offer detailed remediation recommendations
- ☐ Investigate incidents to determine their exact cause and best practices to prevent them from becoming recurring problems
- ☐ Deliver brand and dark web monitoring
- ☐ Offer active defense and threat hunting tools and/or perform proactive threat hunting to identify issues before they lead to a data breach
- ☐ Help clients develop security policies that fall in line with industry- and/or government-mandated requirements.
- ☐ Set your customers up for success when engaging with their stakeholders by providing details and observations around threats and risks. This is especially relevant for cloud.

What security services should MSSPs integrate into their portfolios?



to protect organizations against new and emerging threats, address the shortage of skilled security professionals and manage growing attack surfaces. Multiple security services are available, and deciding which ones to provide is pivotal for an MSSP to make headway in the global market. Here is a look at some of the top services that MSSPs should seriously consider integrating into their portfolios:

Network Security



Network security services protect an organization's computer networks and data. They leverage hardware and software technologies, including firewalls and intrusion prevention systems, to stop threats from penetrating or spreading across networks and manage network access. Today's networks extend beyond the traditional perimeter and into the cloud, so you will need technlogies that can address and respond to these threats.

Benefits of network security for MSSPs

- *Extensive Protection:* MSSPs can protect data and files shared between computers on a network, provide multiple levels of network access and deliver application protection and other network security services.
- *Threat Targeting:* Networks are protected against malware, social engineering attacks and other advanced cyber threats.

Network security market demand

The global network security market is projected to grow from $22.6 billion in 2022 to $53.1 billion by 2029.[4]

[4] Fortune Business Insights, "Network Security Market Size, Share and COVID-19 Impact Analysis," April 2022.

Log management and SIEM

Log management tools generate text-based security audit records and event logs. They perform log functions, such as collection, aggregation, storage and reporting.

SIEM tools, meanwhile, collect and aggregate log data across an organization's IT infrastructure, then identify, categorize and analyze this information to provide security alerts and reports.

Log management and SIEM tools may sound similar, but there are notable differences between the two. With log management, log files are collected and stored from applications and systems across different hosts and systems. SIEM goes a step further than log management because it includes all security products and software across an organization. So, an organization can use SIEM as a single tool to view and analyze all activity across its security products and software — that is, if the organization deploys and manages its SIEM correctly.

With support from an MSSP, an organization can leverage a security expert to automate SIEM processes. The MSSP can help the organization use SIEM to identify and thwart malicious activity, stay informed about threats and review security logs and alerts in real time.

Benefits of SIEM and Log Management for MSSPs

- *Security Analytics: MSSPs can capture threat intelligence feeds and traditional log data to evaluate network and user behaviors.*
- *Various Deployment Models: SIEM can be deployed via hardware, software and cloud models.*
- *No Data Silos: Security data can be collected across a customer's IT environment, so threats can be identified and resolved across all departments.*

Network security services protect an organization's computer networks and data. They leverage hardware and software technologies, including firewalls and intrusion prevention systems, to stop threats from penetrating or spreading across networks and manage network access. Today's networks extend beyond the traditional perimeter and into the cloud, so you will need technlogies that can address and respond to these threats.

SIEM Market Demand

The SIEM market is expected to reach $6.6 billion by 2028.[5]

Chronicle SIEM

Chronicle is Google's cloud-native SIEM platform built on the power of Google infrastructure combined with Google's threat intelligence insights. Chronicle delivers modern threat detection, investigation, and response at unprecedented speed and scale, and at a disruptive and predictable price point. The recently announced Chronicle MSSP Program offers MSSPs around the world the ability to provide scalable, differentiated, and effective detection and response capabilities with Chronicle SIEM.

Scalable and effective threat detection

Correlate petabytes of your telemetry with Google's threat intelligence to detect and identify threats that other tools cannot surface.

Search and investigate threats faster

Search at Google speed to hunt for threats 90% faster than traditional SOC tools.

Disruptive pricing and total cost of ownership

Full-security telemetry retention, analysis at an industry-leading price. Drive compliance and security initiatives with full 1-year telemetry retention at no additional cost.

[5] Brandessence Market Reserach, "Security Information and Event Management Market Size," February 2022.

Endpoint Detection and Response (EDR)

EDR services protect networks accessed via laptops and other wireless and mobile devices. They secure each network endpoint created by these devices.

Benefits of EDR for MSSPs

- Limited Downtime: MSSPs can prevent server outages caused by cyber attacks.
- Proactive Security: Protection extends beyond firewalls and anti-virus software to limit data breaches.

EDR Market Demand

The global EDR market is projected to expand at a compound annual growth rate of 23 percent between 2020 and 2025 and could be worth more than $4.5 billion by 2025.[6]

Penetration Testing and Threat Hunting

Penetration testing, traditionally a manual process executed by humans (as opposed to vulnerability scanning), simulates cyberattacks against computer systems. It checks for exploitable vulnerabilities, misconfigurations, and other weaknesses that can leave a customer's applications, databases and networks open to attack. It also provides insights to help an organization fine-tune its security policies and patch detected flaws.

Threat hunting, meanwhile, allow an MSSP to search customer networks and endpoints to detect indicators of compromise (IoCs) and threats that evade existing security systems.

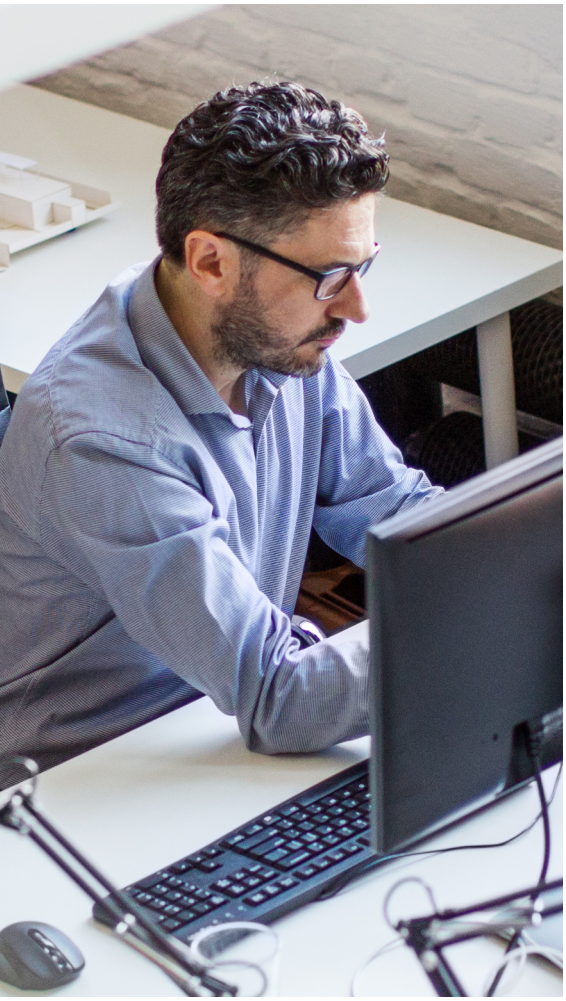
[6]Mordor Intelligence, "Endpoint Detection and Response Market - Growth, Trends, and Forecast (2020 - 2025)." December 2019.

Security orchestration, automation and response (SOAR)

Security orchestration, automation and response (SOAR) tools help an MSSP define, prioritize and standardize security operations across different client tools, while advancing the improvement of key SOC metrics like mean time to detection (MTTD), mean time to response (MTTR) and attacker "dwell time." SOAR provides a single platform that an MSSP can use to manage and orchestrate activities across SIEM, MDR, EDR and other security tools. It includes built-in integrations with different client tools so it can quickly and affordably develop and offer new services.

The challenge of too many alerts, an explosion in security tools that rarely work together, a dependence on manual processes and an existential in-house talent shortage is helping to drive robust growth for SOAR. And these challenges are only exacerbated within MSSPs, compared to enterprise end-users, leading to higher customer acquisition cost and lower margins.

With a SOAR integrated into your security architecture, alerts will flow automatically into a process where they can be analyzed and actioned upon with little to no human intervention. An appropriately deployed SOAR solution will also speed the process once a full investigation begins. By building workflows into the SOAR, also known as playbooks or runbooks, analysts tasked with performing the full investigations will have all the data they need at their fingertips with minimal effort.



Chronicle SOAR

The cloud-native Chronicle SOAR enables modern, fast, and effective response to cyber threats by combining playbook automation, case management and integrated threat intelligence in one cloud-native, intuitive experience.

Interpret and resolve threats faster

Shift the paradigm by uniting context with a threat-centric approach, empowering analysts to quickly focus on what's truly important instead of drowning in analysis and data.

Deploy, maintain and scale with ease

Designed for fast time-to-value and ease of scaling with pre-packaged use cases, an intuitive playbook builder, and powerful playbook lifecycle management.

Capture security operations insights

Empower teams to consolidate and easily see the scope of activities, generate insights that drive improvement, and measure progress over time.

For more information on how your MSSP can deliver high-value security services at scale while keeping your customers delighted and your margins healthy, visit chronicle.security.

Google Cloud