LOGPOINT

Nov 22, 2022 08:00 CET

5 ways MSSPs can transform daunting challenges into opportunities

Managed Security Service Providers (MSSPs) play an increasingly critical role in cybersecurity as more and more organizations turn to them for cybersecurity assistance. As threat actors continue to develop techniques and tactics, compliance requirements multiply, and the complexity of cybersecurity infrastructure increases, organizations scramble to protect business assets and processes from internal and external threats.

The MSSP market is estimated to reach a $53.2 billion revenue by the end of 2031, which is a 264 percent growth from the $14.6 billion reached in 2021. Despite the ample opportunities for MSSPs to scale, the MSSP market is not without friction. A recent Logpoint survey uncovered that MSSPs face a range

of challenges themselves. Through in-depth interviews with MSSPs across Europe and the US, we gained a deep understanding of these challenges and how MSSPs can overcome them and grow their business.

The challenges

The ability to productize and price cybersecurity services is an ongoing challenge. Especially since the main drivers for organizations outsourcing security operations to MSSPs are lowering costs and making them predictable. However, MSSPs struggle because they often use platforms with capacity-based licensing schemes that charge by volume.

Whether charged per message, gigabyte, or events per second, costs are unpredictable and potentially unaffordable, and without predictable pricing, MSSPs risk losing customers.

Another challenge MSSPs face is getting customer engagement just right. Customers who don't review status reports or have few interactions with the MSSP have higher churn rates. Customers who receive regular reports and frequently interact with the MSSP tend to renew service contracts and buy additional services.

While it's not difficult to deduct what's needed to maintain a strong customer relationship, the ability to engage requires personnel, and unfortunately, cybersecurity skills are in short supply. That's as true about customer success engineers as cybersecurity analysts.

Technological concerns

The issue with never having enough analysts is that although technological advances promise to increase efficiency, they can have quite the opposite effect. For MSSPs, introducing new technologies can result in increased customer expectations, including better SLAs, and keeping pace can be demanding.

Since MSSPs serve a wide variety of organizations in terms of size, sector, and outsourcing needs, they must be flexible regarding service packaging and deployment options. For example, operating exclusively in the cloud might be efficient, but many organizations either want or are required to keep their

security event data on-premises.

MSSPs face an overload of tools and solutions on the market, with hundreds of vendors who knock on their doors weekly to sell the latest technologies and systems. The challenge is to see through the hype to understand the actual capabilities of new platforms like SOAR and XDR.

As a rule of thumb, MSSPs must be confident that their customers want to buy the new capabilities before deploying them. MSSPs seek solutions that can drive business growth without necessarily increasing licensing costs.

Becoming the MSSP vanguard

The challenges reveal a paradigm shift for MSSPs, and the ones that figure out how to adapt to rising customer expectations, find a predictable pricing model, and build an appropriate cybersecurity technology stack will be the ones that reap the benefits of the growing market.

The 5 initiatives that will enable MSSPs to turn challenges into opportunities:

1. **Flexible deployment and delivery options:** MSSPs should bundle multiple cybersecurity functions into a single service package that can be deployed on-premises, in the cloud, or in a hybrid infrastructure. And with a security stack to integrate smoothly with itself and with a wide array of customer technologies, they can onboard, configure, and start delivering value to customers quickly.
2. **Flexible architectures that support business growth:** MSSPs should prioritize converged technologies such as SOAR and UEBA with existing SIEM platforms and make it easy to deliver a wide array of cybersecurity services under a converged and predictable licensing structure.
3. **Agile management of vendor and client relationships:** A close working relationship with solution vendors is essential to understanding the inner workings of their cybersecurity platform and being able to influence roadmap decisions to assure the continuity of affordable services and efficient operations to clients.
4. **Flexible implementation of SOAR:** Many MSSPs are not yet using

SOAR, but automation and orchestration will be necessary to remain competitive and grow the business. MSSPs can get started by looking for flexible licensing options and hands-on training on playbook design and use case implementation.

5. **Flexible reporting that shows value**: Customers want to know that their MSSP detects, manages, and responds quickly to security incidents and complies with regulations. MSSPs should look to implement a simple reporting dashboard that customers can easily understand.

While the MSSP market is faced with a handful of daunting challenges, there's also ample opportunity for them to overcome them by implementing technologies that simplify their processes and licensing models and enable them to create new offerings for their customers.

About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's SIEMand NDRtechnologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98