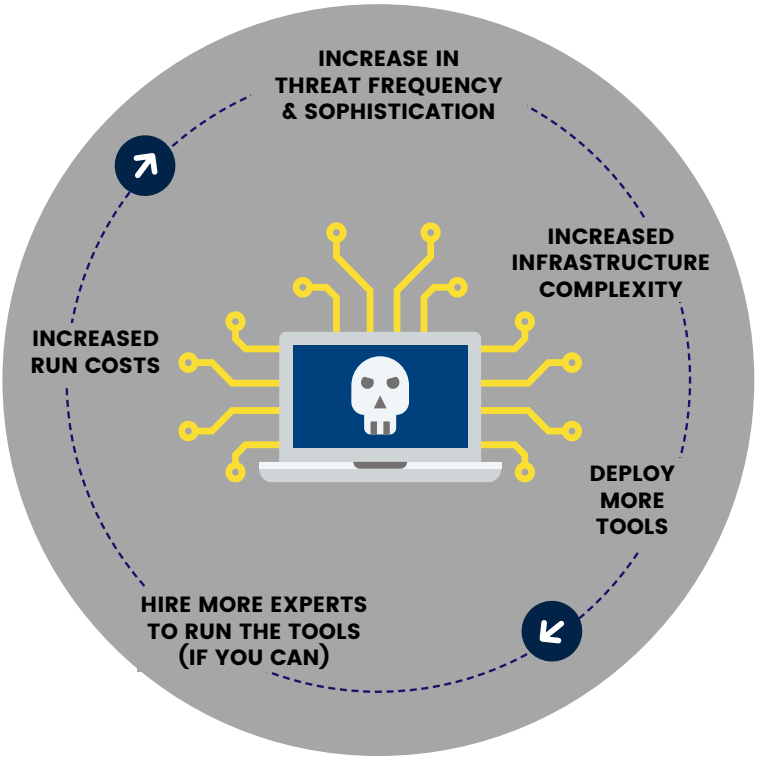
NETENRICH

Technology: What MSSPs Should Look for Now and Next

MSSPs have their work cut out for them. Demand is up. Infrastructures are increasingly complex, and cyberattacks are growing in frequency and sophistication. Like all service providers, MSSPs have to keep an eye on their margins and make technology investments that deliver fast ROI as well as continued value over the long term.

Far more enterprises – of all sizes – are outsourcing to MSSPs, according to the 2022 Cyberthreat Defense Report from CyberEdge Group. The report hypothesizes that the increase "is partly attributable to the fact that operations entails very labor-intensive activities…. MSSPs have achieved a high level of automation of these tasks, so they can provide these services very economically to their clients."[1]

To make the economics work you need to constantly improve your levels of automation while continuing to provide high-value services to your customers. Otherwise, you're caught in a vicious, margin-busting cycle.



Given where you are today:

What should you implement now or soon? And what should you be keeping your eye on for the future to ensure ongoing resilience, relevance, and margins?

1 CyberEdge Group, 2022 Cyberthreat Defense Report, p. 47

We've worked with a lot of MSSPs for years, and they've shared with us that their biggest problems today include:

1. Too many siloed tools. They juggle too many low-level tools that don't talk to each other. Each tool may do what it does well, but there's a cost to integrating technologies, managing vendors, and finding employees with the right expertise to run them. Each new tool introduces new benefits but also new risks.

2. Data ingestion and storage is expensive. Maintaining security requires data, and it's expensive. You need a lot of data so you can determine when and if something could be going wrong that indicates an attack or breach. You want to collect all that data and sift through it, but ingestion and anything close to real-time analysis is expensive – often prohibitively so.

3. It's hard to get and keep talent. Well-trained security analysts who understand the tools and environments you work with aren't easy to find or to keep. The 2022 Cyberthreat Defense Report says, "The gating factor in providing better security is finding personnel with security skills, not budget."[2] (But isn't budget nearly always a concern?)

4. Mapping threats against assets is hard. It's harder to know where to focus when you don't have asset information integrated with your security data. Maintaining asset data is extremely challenging in a world where assets come on and offline frequently.

5. Far too many alerts and false positives. You need to find signals in the noise, but when your tools are low level, you won't see patterns above them. When you don't have the data you need to find patterns – in real time and over time – you'll miss trends.

Here's what to look for in new technologies that can address each of these five issues.

---

2 CyberEdge Group, 2022 Cyberthreat Defense Report, p. 32

1.Too many siloed tools

Having siloed tools is not itself a problem until you have a lot of them. Having a lot of tools isn't a problem unless they don't work together without a lot of extra work. However, ripping out the tools you have and replacing them with a smaller number of other tools won't solve the problem long term.

If you already have or anticipate this challenge of too many siloed tools, look for solutions that leverage your current investments and that integrate into a multi-tool world. As Gartner®, Inc. points out, "IT leaders must integrate security tools into a cooperative ecosystem using a composable and scalable cybersecurity mesh architecture approach." [3]

> ***"By 2024, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of security incidents by an average of 90%."*** [4]

Advantages of a cybersecurity mesh architecture include flexibility, adaptability, and continuous improvement. There is no one product that provides it – it's an architecture, after all. But some technologies are better suited to an open, agile architecture approach than others.

There's another major issue: Too many siloed and low-level tools can inhibit your ability to perform behavioral detection analytics. Behavioral analytics identify potentially malicious activity within a system or network that may not rely on prior knowledge of adversary tools and indicators. It is a way of leveraging how an adversary interacts with a specific platform to identify and link together suspicious activity that is agnostic or independent of specific tools that may be used. You can use the MITRE ATT&CK framework to construct and test behavioral analytics to detect adversarial behavior.

---

3 Gartner, Inc. Top Strategic Technology Trends for 2022: Cybersecurity Mesh. Published 18 October, 2021. By Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. https://www.gartner.com/en/doc/756665-cybersecurity-mesh

4 Gartner®, Inc. on https://www.gartner.com/en/doc/756665-cybersecurity-mesh

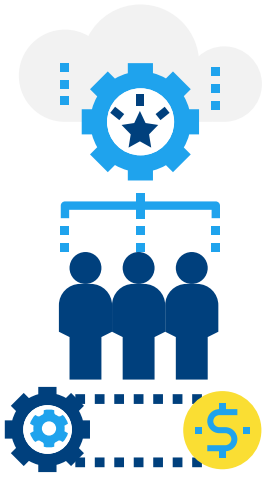
Look for technologies that offer:

- Secure APIs as well as prebuilt integrations.
- Scalability, ideally through native cloud platforms.
- Behavioral detection analytics.
- Mapping to a framework like MITRE ATT&CK.
- Support for Cybersecurity Mesh Architecture.

2. Data ingestion and storage is expensive.

Actually, data ingestion and storage no longer has to be expensive. There are new options out there well worth your consideration. Look for data ingestion and storage technologies that offer:

- Ability to scale to capture the amount of data you need for your customers now and in the near future – even if you "open the aperture" and filter less.
- Fast search speed for your current and near-term data volumes.
- Real-time (or close) data analytics.
- Ability to use your current security telemetry sources.
- Ability to ingest data from all sources: on premise, cloud, etc.



3. It's hard to get and keep talent.

Getting and keeping talent is an ongoing and growing problem. Many employees are burned out from the grind. Automation can relieve your people of tedious L1 and L2 tasks. Technology products that use data analytics and machine learning can provide extensive context, identify trends and anomalies, add data enrichment, and other functions that speed resolution while reducing tedium.

Use technology to dramatically improve how you run security ops, not just to automate current processes to make them more efficient. For example,

look beyond threat detection and response to proactive “peacetime” activities that shore up resiliency in advance of attacks. Consider effectiveness as opposed to “efficiency” against specific metrics that the new technology may make obsolete. For example, enabling your team to manage more customers is a better metric than the number of tickets that they can close. (After all, the technology may also cause more tickets to be generated.)

If you have a good team, help them be happy and highly productive. Look for technologies that:

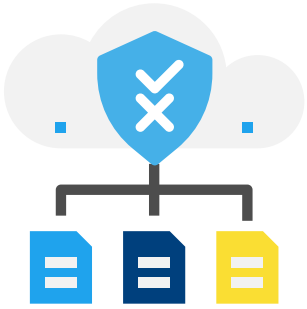
- Enable your current team to be more effective, not only through automation but also through data analytics, machine learning, etc.
- Support proactive “peacetime” activities that shore up resiliency in advance of attacks.
- Don’t require that you hire more experts.
- Reduce burnout and that your team is excited to use.

4. Mapping threats against assets is hard.

It’s harder to know where to focus when you don’t have asset information integrated with your security data. You can be dramatically more effective when you know whether an attack is targeting a high-value business resource (“the crown jewels”) or a more isolated, unimportant asset. Maintaining asset data is extremely challenging in a world where assets come on and offline frequently.

So, look for technologies that offer:

- Automatic asset discovery and the ability to tag assets depending on their business importance.
- Ability to map known threats against any customer’s assets to see where they may not have sufficient log coverage for early detection.



5. Far too many alerts and false positives.

Back to that vicious cycle we described above: more tools provide more data but at the same time produce even more noise that takes time to sort through – and it's the type of high-stress job of sorting through it that exhausts your team and sends them packing. This is an area ripe for data analytics, machine learning, and improved automation.

The goal is to make your people more effective, not more efficient at closing tickets for false positives.

Look for technology that provides realistic ways of reducing false positives while enhancing important signals – fast.

Think about the types of signals you need to detect:

- Across the entire infrastructure to find more complicated patterns of attack.
- Across time to find trends going back months or longer.

Think about how signals need to be enhanced

- Correlating related alerts from various sources with tickets, users, and asset.
- Prioritizing and scoring to assess which signals should be addressed first for maximum effectiveness.

Conclusion: it's all about security – and margins

To maintain your business and your margins, you continuously evaluate the technologies that enable your teams to ensure your customers' security. At the same time, you can't maintain margins with a more-tools-more-people approach. So, choose your tech wisely. Download our MSSP Technology Checklist for a one-page summary of what to look for in your new tech investments.

MSSP Technology Checklist

MSSPs have to keep an eye on their margins and make technology investments that deliver fast ROI and continued value over the long term. Use this checklist to ensure that new technology you consider addresses the five top challenges that MSSPs face today.

CHALLENGE		LOOK FOR TECHNOLOGIES THAT OFFER
Too many siloed tools	☐	Secure APIs as well as prebuilt integrations
	☐	Scalability, ideally through native cloud platforms
	☐	Behavioral detection analytics
	☐	Mapping to a framework like MITRE ATT&CK
	☐	Support for Cybersecurity Mesh Architecture (CSMA)
Data ingestion and storage is expensive	☐	Ability to scale to capture the amount of data you need for your customers now and in the near future – even if you "open the aperture" and filter less
	☐	Fast search speed for your current and near-term data volumes
	☐	Real-time (or close) data analytics
	☐	Ability to use your current security telemetry sources
	☐	Ability to ingest data from all sources: on premise, cloud, etc.
It's hard to get and keep talent	☐	Enable your current team to be more effective, not only through automation but also through data analytics, machine learning, etc.
	☐	Support proactive "peacetime" activities that shore up resiliency in advance of attacks
	☐	Doesn't require that you hire more experts
	☐	Reduces burnout and that your team is excited to use
Mapping threats against assets is hard	☐	Automatic asset discovery
	☐	Ability to tag assets depending on their business value
	☐	Ability to map known threats against any customer's assets to see where they may not have sufficient log coverage for early detection
Far too many alerts and false positives		**Types of signals you need to detect:**
	☐	Across the entire infrastructure to find more complicated patterns of attack
	☐	Across time to find trends going back months or longer
		How do signals need to be enhanced:
	☐	Correlating related alerts from various sources with tickets, users, and asset
	☐	Prioritizing and scoring to assess which signals should be addressed first for maximum effectiveness

