Secureworks

WHITE PAPER

Security Consolidation Options for Microsoft-Centric Organizations (That Won't Break Your Budget)

According to Gartner, 75% of organizations are pursuing security vendor consolidation to improve their risk posture and/or reduce spend.

Strategies for achieving this include taking advantage of bundled packages such as the Microsoft 365 E5 license. However, many organizations need to ensure that they are covering their non-Microsoft technologies as well, and choose one of two options:

1. Deploying a SIEM solution, such as Microsoft Sentinel, despite their intrinsic complexity, high deployment and unpredictable and typically high operational costs.
2. Adopting a modern open XDR platform that is vendor neutral to consolidate security while leveraging existing investments.

Let's unpack the available options that Microsoft centric organizations have to achieve cybersecurity consolidation by focusing on E5 security capabilities, Microsoft Sentinel and alternatives that might deliver the same (or better) outcomes without breaking your budget.

Consolidated Security with Microsoft E5 Security

The Microsoft 365/E5 Security bundled licenses are popular with Microsoft centric customers. With a per-user based model, they are easy to license and scope and provide immediate access to a variety of security tools and capabilities. Some relevant security features that organizations can benefit from when deciding to move to an E5 license include endpoints (Defender for Endpoint), e-mail (Defender for Office 365), cloud identities (Entra ID Protection), Active Directory and on-premise identities (Defender for Identity) and cloud access (Defender for Cloud Apps).

Additionally, the E5 license also provides access to Microsoft Defender XDR. This capability coordinates and centralizes detection, investigation and response across the previously mentioned Defender and security capabilities.

Defender XDR also provides advanced new features on top of the other individual Defender solutions such as Automated Investigation and Response (AIR) and Threat Hunting with 30 days of data storage.

However, it's important to note that Defender XDR is focused on Microsoft technology, which leaves a gap in terms of holistic visibility and detection capabilities across modern hybrid environments. As a result, organizations that opt to leverage Microsoft Defender often look to complement it with an additional SIEM or vendor agnostic XDR solution.

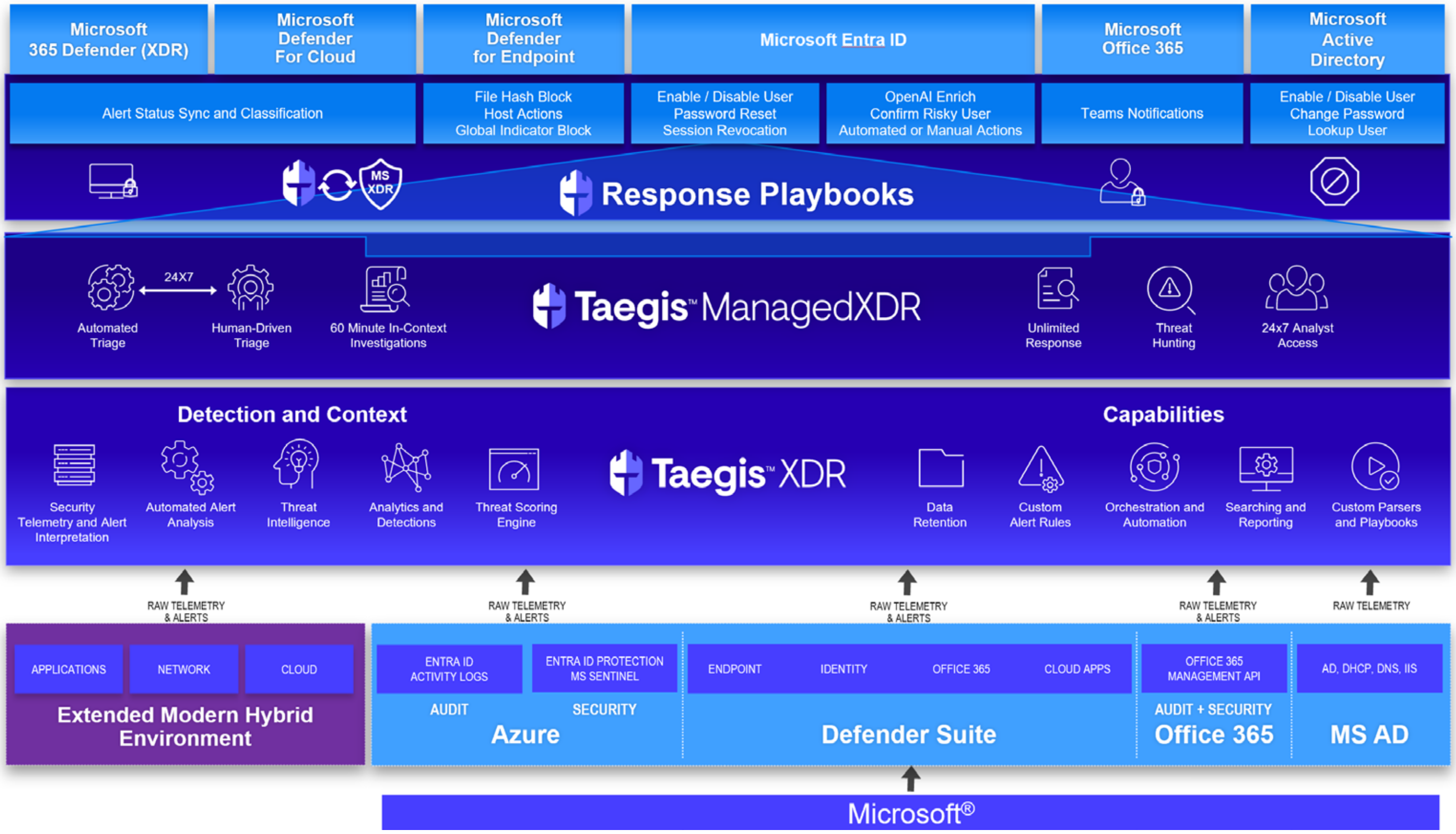
SIEM vs. Open XDR

One of the first options that Microsoft centric organizations consider for providing holistic visibility is Microsoft's native cloud SIEM solution, Microsoft Sentinel. Many security experts agree that Sentinel is one of the top SIEM solutions available, yet experience shows it also comes with significant challenges, which is expected from such a complex and customization dependent tool. Leveraging a solution such as Microsoft Sentinel requires a high level of security maturity, expertise, and people to deploy, manage and use it. For organizations without an unlimited security budget, it's just as important to understand that budgeting for Microsoft Sentinel is very difficult to predict due to the consumption-based licensing model. More on that below.

Another option that often proves to be a better fit is a third-party open XDR platform that can seamlessly integrate into the Microsoft environment to leverage available input and signals, enhance them with its own advanced detection capabilities, and put that into the context of the broader environment by integrating with all other relevant non-Microsoft sources (network, infrastructure, third-party cloud, third-party EDR vendors, etc.). Some of the advantages organizations see in the open platform Secureworks® Taegis™ XDR are:

- Multi-EDR support, including Microsoft Defender for Endpoint.
- The broadest integration into the Microsoft ecosystem, from independent third-party providers.
- An included EDR agent to complement Defender on assets where the latter is not licensed.
- 12 months of data retention included at no additional cost.
- Predictable endpoint-based licensing.

Learn how Secureworks helps Microsoft centric organizations make the most of their E5 Security License and Microsoft Defender.



So what kind of costs should organizations take into account when considering Microsoft Sentinel or a third-party independent XDR platform such as Taegis XDR?

Cost Considerations for Microsoft Sentinel vs. Taegis XDR

The following analysis focuses on software-only cost considerations and scenarios, without any layer of managed services on top. A bit later we will highlight a few aspects organizations need to be aware of when trying to optimize costs and potentially cut corners.

Microsoft Sentinel Cost Considerations

- Microsoft Sentinel is licensed on a consumption-based model that takes into account Data Ingestion and Data Retention time.
- Microsoft Sentinel is not licensed under any license bundle, such as E5.
- Microsoft Sentinel costs include data storage (Log Analytics) and the actual Sentinel capabilities.
- Microsoft Sentinel provides 90 days of free data storage, and more costs extra.
- Microsoft Sentinel provides two types of log storage – Analytic Logs and Basic Logs. Analytic Logs are the ones truly relevant for security purposes (running complex queries, analytics rules, extended storage). Basic logs have a very limited retention time (eight days) and are not suitable for security monitoring.

- There are many other moving parts in terms of potential costs associated with Sentinel, for example: data archiving and archive retrieval, searching through archive, searching through basic logs, running automation tasks via Logic Apps.
- Microsoft provides a few free log sources with Microsoft Sentinel, but they are very Microsoft centric, limited in volume and type and in the context of holistic monitoring and visibility create very little benefit in terms of total cost.
  More details can be found here, but we will also provide practical examples below.

Taegis XDR Cost Considerations

Taegis XDR is licensed based on endpoint (EDR enrolled asset) count. All other integrations (network, e-mail, identity, infrastructure, cloud and so on) come at no additional cost.

Standard data retention in hot storage (alerts and raw events and logs) for 12 months included in the price, with the option to extend storage up to 5 years.

All-inclusive licensing (XDR platform, data retention, native EDR agent, integrations, orchestration and automation, over 20,000 out of the box countermeasures/detection capabilities).

Real-World Scenarios: Microsoft Sentinel vs. Taegis XDR Cost Comparisons

Using the public facing documentation, calculator and pricing of Microsoft Sentinel as well as our experience in security monitoring and real data from environments of organizations we deliver technology and services for, we have extracted three representative examples of costs for true holistic monitoring for both Microsoft Sentinel as well as Taegis XDR. The scenarios below use the following assumptions:

- Based on hot storage retention for 12 months.
- List price without any additional discounts.
- Based on security monitoring best practices—in the case of Sentinel that means Analytic Logs (in contrast to Basic logs) and complete integration into modern hybrid infrastructures (not focused solely on Microsoft log sources).
- Based on real, representative types and sizes of organizations.

USE CASE 1:

Small Organization in the Manufacturing sector

As a rather small company with fewer than 1,000 endpoints but within a sector that is highly targeted by threat actors, this organization decided Microsoft E5 offers the perfect balance between a comprehensive set of security features (consolidation) at a price-per-user that was more efficient compared to buying individual separate solutions. However, with an extremely small team of IT experts and one CISO, it was clear they needed a trusted third party to look into what their new Defender environment considered to be malicious, make sense of that and investigate it in the broader context of their infrastructure. Just like in many manufacturing organizations, their network was considered to be a very important control, especially when considering traffic between the IT and OT environments.

Secureworks Taegis MXDR proved to be the right choice for this organization for the following reasons:

- **E5 Integration:** Taegis XDR perfectly integrated with Defender and other E5 components, and the MDR for Microsoft service took away the burden of investigation and response from the customer, 24/7.
- **Consolidated endpoint and network visibility:** Taegis XDR integrated and cross-correlated out of the box between the Microsoft ecosystem and the network security devices.
- **Better TCO, improved Time to Value:** The price point for Taegis XDR was significantly superior to a similar Microsoft Sentinel deployment, and the full deployment of the Secureworks MXDR services delivered quicker time to value compared to a similar Managed Sentinel service.

Organisation Profile & Technologies	
Endpoints	Under 1000, deployed with Defender for Endpoint
Firewalls	FW_Vendor1
Other Integrations	Azure, Office 365

Data Usage	
Raw Monthly Data Volume	2.7 TB
Raw Daily Data Ingestion	91 GB

Monthly Data Storage Capacity (uncompressed)	
Sentinel	**Taegis XDR**
2.7 TB Current usage	22 TB Included in License

List price cost considerations with 12 months retention	
Microsoft Sentinel	$136,452
With potential Sentinel discount for Azure / E5 customers (**~10,000$, 7.3%**)	$126,452
Savings with Taegis XDR	**59%**
Taegis XDR storage headroom	**714%**

USE CASE 2:

Medium Organization in the Services sector

In the next example, this medium-sized organization active in the services sector with between 2,500 and 5,000 endpoints had already deployed Defender for Endpoint. However, the existing analyst team proved to be too small to deal with all the alerts and observations produced by their environment. Not having a centralized dashboard that supports automating false positive triage, correlating and responding not only for the Defender capabilities but also their other endpoint, network and cloud deployments was not helping either. Moreover, the team was available only during regular business hours, which meant there were no true 24/7 monitoring and response capabilities.
On the network side, even though the main entry points were protected with Barracuda devices, there was still a need for additional deep packet inspection with prevention capabilities for north-south as well as east-west traffic.

This organization chose Secureworks Taegis ManagedXDR on the basis of:

- **Included EDR agent:** The Secureworks Taegis EDR agent that comes at no additional cost complemented the existing Defender for Endpoint deployment, on assets where the Microsoft E5 license was not available.
- **Cross-correlation across the entire landscape:** Integrated Microsoft capabilities as well as other third-party network, email security and endpoint solutions, including the ability to bring in custom log sources.
- **Centralized response:** Provided orchestration and automation across the entire Microsoft and non-Microsoft landscape from one central platform.
- **Native Network Detection and Response:** Seamlessly integrated Secureworks Taegis NDR for additional detection and prevention capabilities on the network.
- **24/7 MDR service:** End-to-end detection and response, with included unlimited response engagements and proactive threat hunting.

Organisation Profile & Technologies	
Endpoints	Between 2,500 and 5,000, deployed with a combination of Defender for Endpoint and Taegis EDR
Firewalls	FW_Vendor2
Other Integrations	Secureworks Taegis NDR, Non-Microsoft EPP, SASE, Non-Microsoft E-mail Security, Azure, Office 365

Data Usage	
Raw Monthly Data Volume	10.5 TB
Raw Daily Data Ingestion	350 GB

Monthly Data Storage Capacity (uncompressed)	
Sentinel	**Taegis XDR**
10.5 TB Current usage	83 TB Included in License

List price cost considerations with 12 months retention	
Microsoft Sentinel	$450,972
With potential Sentinel discount for Azure / E5 customers (**~23,000$, 5.1%**)	$427,452
Savings with Taegis XDR	**68%**
Taegis XDR storage headroom	**690%**

USE CASE 3:

Large Organization in the Energy sector

Our final example is a large organization in the energy sector with more than 10,000 endpoints. Even though this organization is using Microsoft services such as Azure cloud and Office 365, on the endpoints they decided to stay with CrowdStrike. Being a more mature company, they were aware of the significant costs that SIEM solutions bring due to their consumption-based model. An important requirement they had was to benefit as much as possible from a rich set of out-of-the-box detection capabilities, fully maintained and managed by the provider, thus avoiding the complexity and time required to develop their own use cases—which is the case with SIEM-like solutions, including Microsoft Sentinel.

Some of the most important aspects for which they chose Secureworks Taegis ManagedXDR were:

- **Multi-EDR support:** Taegis XDR allowed for seamless integration with their existing CrowdStrike EDR as well as the ability to adapt if they ever decided to move to a different EDR provider, such as Microsoft Defender.
- **Hundreds of out-of-the box integrations:** With a combination of on-premise and cloud log sources.
- **Out-of-the-box detection capabilities:** Over 20,000 countermeasures, including state of the art AI and machine-learning based detectors.
- **12 months of log retention included:** Having over 100 multi-vendor firewall devices, their infrastructure was prone to produce a lot of data.
- **Data storage headroom:** Ability to grow in terms of data storage—over eight times the current volume—with no technical or commercial impact.
- **All-inclusive pricing model:** No limit on number of integrations with EDR agent and data storage included.
- **Predictive pricing:** Endpoint-based rather than consumption-based.

Organisation Profile & Technologies	
Endpoints	Over 1,000 deployed with CrowdStrike
Firewalls	100+ FW_Vendor3 and FW_Vendor4 devices
Other Integrations	SASE, DHCP, DNS, IIS, Azure, Office 365, Non-Microsoft E-mail Security

Data Usage	
Raw Monthly Data Volume	36.5 TB
Raw Daily Data Ingestion	1218 GB

Monthly Data Storage Capacity (uncompressed)	
Sentinel	**Taegis XDR**
36.5 TB Current usage	309 TB Included in License

List price cost considerations with 12 months retention	
Microsoft Sentinel	$1.487.532
With potential Sentinel discount for Azure / E5 customers (**~79,000$, 5.3%**)	$1,408,532
Savings with Taegis XDR	**70%**
Taegis XDR storage headroom	**746%**

Beware of Cost Optimization that Increases Risk

Looking at the cases above, it is easy to understand why Microsoft Sentinel and other SIEM solutions can significantly exceed most organizations' budgets. It's important to note that attempting to optimize costs without careful consideration can lead to an increased risk exposure. When estimating costs for Microsoft Sentinel as an internal exercise or even guided by a Managed Sentinel MDR/MSSP provider, we encourage you to always ask yourself:

1. **Am I monitoring my entire environment?**
   Often, organizations end up integrating only a subset of their relevant log sources into Sentinel, mostly the ones that come free of charge for Microsoft centric customers: Azure, Office 365 and Defender alerts. This has at least two drawbacks that increase the risk of a breach:

   - Lack of visibility and detection capabilities across the true hybrid environment. Ignoring network traffic and detections, third-party identity or cloud providers, raw operating system logs and many more can significantly increase the chances of a breach.
   - Without additional visibility and significant development in terms of detection capabilities (for example, analytics rules), Sentinel will resemble more of an alert relay capability rather than a true cross correlation and detection tool. As such, it provides relatively small value on top of Defender XDR.

2. **Am I ingesting all the relevant logs?**
   Organizations (many times under the guidance of third-party consultants and MDR providers) frequently start filtering out events before being ingested into Microsoft Sentinel. Usually that happens at the connector level, where filters are put in place to decrease the volume of logs.

   This directly contradicts the concept of complete visibility and detection capabilities. Threat actors find ways to exploit weaknesses and come up with new tactics and techniques faster than ever before. How can you know that precisely the data you chose to ignore today is not the data you so desperately need to identify tomorrow's zero day? And can you afford to take that risk?

3. **Am I storing the data long enough to address all my requirements?**
   Threat hunting, incident response, forensics, and compliance are all crucial aspects of a sound cybersecurity program that rely on historic data. Our experience as one of the leading providers of incident response services shows that it is ideal to have raw data available in hot storage for at least 12 months.

Microsoft Sentinel and other SIEM solutions can significantly exceed most organizations' budgets.

We would advise organizations to always evaluate, and if needed, challenge a model where their data is stored for a short period of time (basically anything under 12 months) or moved early to some form of cold storage. Cold storage (such as an archive) will not provide timely access to information because it is slower, will not allow for the same complexity of queries, and any interaction with it (searching or even moving data back to hot storage) will incur additional costs.

4 **Can I put the data I ingest to good use?**
As explained earlier, Sentinel supports two ingestion capabilities: Analytic or Basic logs. The latter will be significantly cheaper, and sometimes used as a means to optimize costs.

However, from a security standpoint, that data is almost useless. It can't be used for building analytics rules on top of, the query language is significantly reduced, and moreover, it only lives in hot storage for eight days. So even if this will significantly decrease costs, we encourage organizations to challenge the real value of that data once stored in Basic logs.

Learn more about Secureworks solutions for Microsoft, or ask one of our experts about a personalized Total Cost of Ownership comparison.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

CORPORATE HEADQUARTERS

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MIDDLE EAST

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971
4 420 7000

ASIA PACIFIC

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.