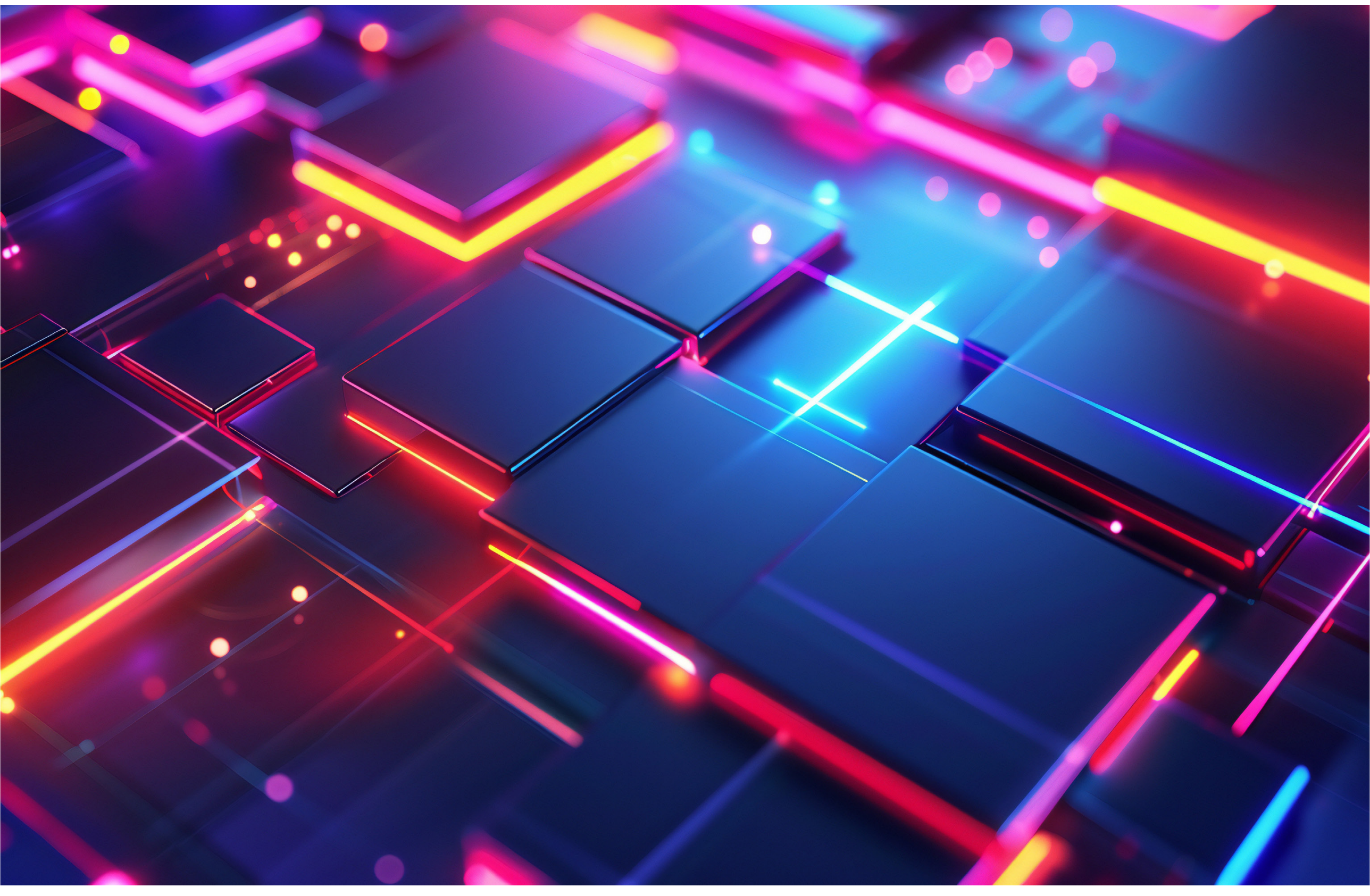
DEEPWATCH™

Always Watching. Always Protecting.™

WHITEPAPER

The Deepwatch Guardian MDR Platform™ Enhances Microsoft Sentinel

Delivering proactive 24/7/365 defense, freeing internal teams to focus on strategic security initiatives.



www.deepwatch.com/microsoft-sentinel

Executive Summary

In today’s complex threat landscape, organizations struggle to maintain robust security operations. **Microsoft Sentinel** offers a powerful, cloud-native Security Information and Event Management (SIEM) solution, but its effectiveness can be significantly amplified with the integration of the **Deepwatch Guardian MDR Platform™ (Deepwatch MDR)**. This whitepaper outlines how Deepwatch MDR enhances Microsoft Sentinel by providing continuous monitoring, expert threat detection, rapid response capabilities, and a reduction in security operational burden, ultimately improving an organization’s security posture.

The Evolving Threat Landscape

Cyber threats are becoming more sophisticated and frequent, making it challenging for in-house security teams to keep pace. The volume of alerts, the shortage of skilled cybersecurity professionals, and the complexity of modern IT environments often lead to alert fatigue and missed threats. Organizations need more than just tools; they need **24/7/365 vigilance** and expert human analysis to effectively combat these threats.

Microsoft Sentinel: A Powerful Foundation

Microsoft Sentinel provides a scalable and intelligent SIEM solution that collects security data across an enterprise, detects threats, and automates responses. Its key features include:

Cloud-Native Scalability:

Built on Azure, it offers elastic scalability to handle vast amounts of data.

Integrated Threat Intelligence:

Leverages Microsoft's global threat intelligence.

AI and Machine Learning:

Uses advanced analytics for anomaly detection and threat identification.

Automation and Orchestration:

Enables automated responses to common threats.

While Sentinel is a robust platform, effectively managing and optimizing it requires significant resources and expertise, which many organizations lack.

How Deepwatch MDR Augments Microsoft Sentinel

Deepwatch MDR complements Microsoft Sentinel by providing the **people, processes, and technology** necessary to maximize its value. This partnership transforms Sentinel from a powerful SIEM into a comprehensive, proactive security operations center (SOC).

1. 24/7/365 Expert Monitoring and Triage

Deepwatch's security experts provide constant surveillance of an organization's environment. They:

- **Monitor Sentinel Alerts:** Proactively review and triage alerts generated by Microsoft Sentinel.
- **Reduce Alert Fatigue:** Filter out false positives and prioritize legitimate threats, allowing in-house teams to focus on critical incidents.
- **Contextualize Threats:** Enrich alerts with additional threat intelligence and contextual information to understand the full scope of an attack.

2. Advanced Threat Detection and Hunting

Beyond what Sentinel's out-of-the-box capabilities offer, Deepwatch MDR provides:

- **Custom Detections:** Develops and deploys custom detection rules tailored to an organization's unique environment and threat profile, enhancing Sentinel's detection capabilities.
- **Proactive Threat Hunting:** Leverages the data in Sentinel to actively hunt for stealthy threats that might bypass automated detections. This includes searching for indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with advanced persistent threats (APTs).
- **Behavioral Analysis:** Implements advanced behavioral analytics to identify anomalous user and entity behavior that may indicate a compromise.

3. Rapid Incident Response

When a threat is detected, Deepwatch MDR ensures a swift and effective response:

- **Guided Response Playbooks:** Integrates with Sentinel's automation features to orchestrate and execute pre-defined response playbooks.
- **Expert-Led Remediation:** Deepwatch's security analysts guide organizations through remediation steps, providing clear instructions and support to contain and eradicate threats.
- **Forensic Analysis:** Conducts initial forensic analysis to understand the attack's scope, impact, and root cause, facilitating a thorough recovery.

4. Reduced Operational Burden and Cost Savings

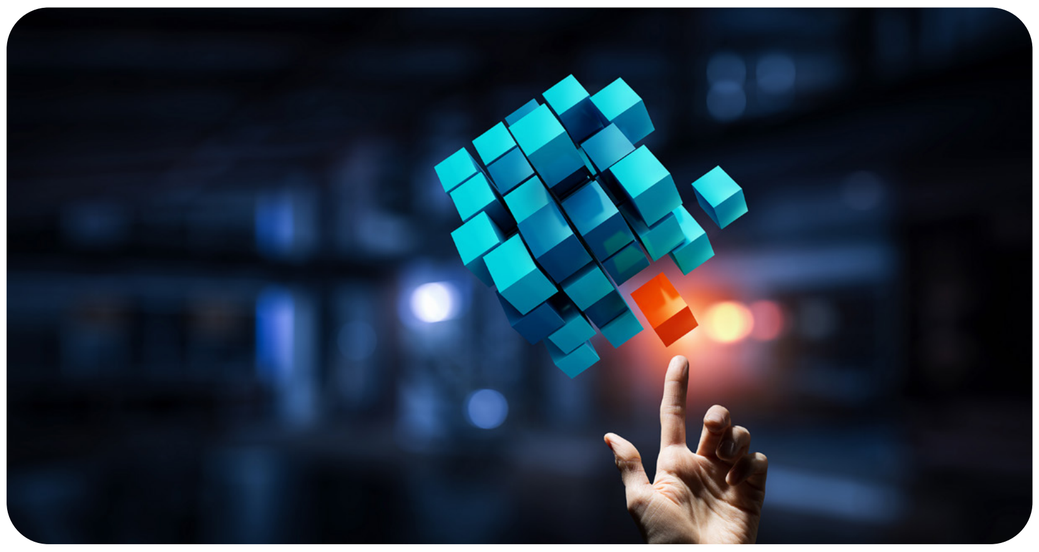
Partnering with Deepwatch MDR allows organizations to:

- **Optimize Sentinel Investment:** Ensure that Microsoft Sentinel is configured optimally and continuously tuned for maximum effectiveness.
- **Address Staffing Shortages:** Fills the gap in cybersecurity talent by providing access to a team of highly skilled security professionals without the overhead of hiring and training an in-house SOC team.
- **Improve ROI:** Maximize the return on investment in Microsoft Sentinel by leveraging Deepwatch's expertise to fully utilize its features and capabilities.
- **Predictable Security Costs:** Shift from unpredictable incident response costs to a more predictable monthly operational expense.

5. Continuous Improvement and Strategic Guidance

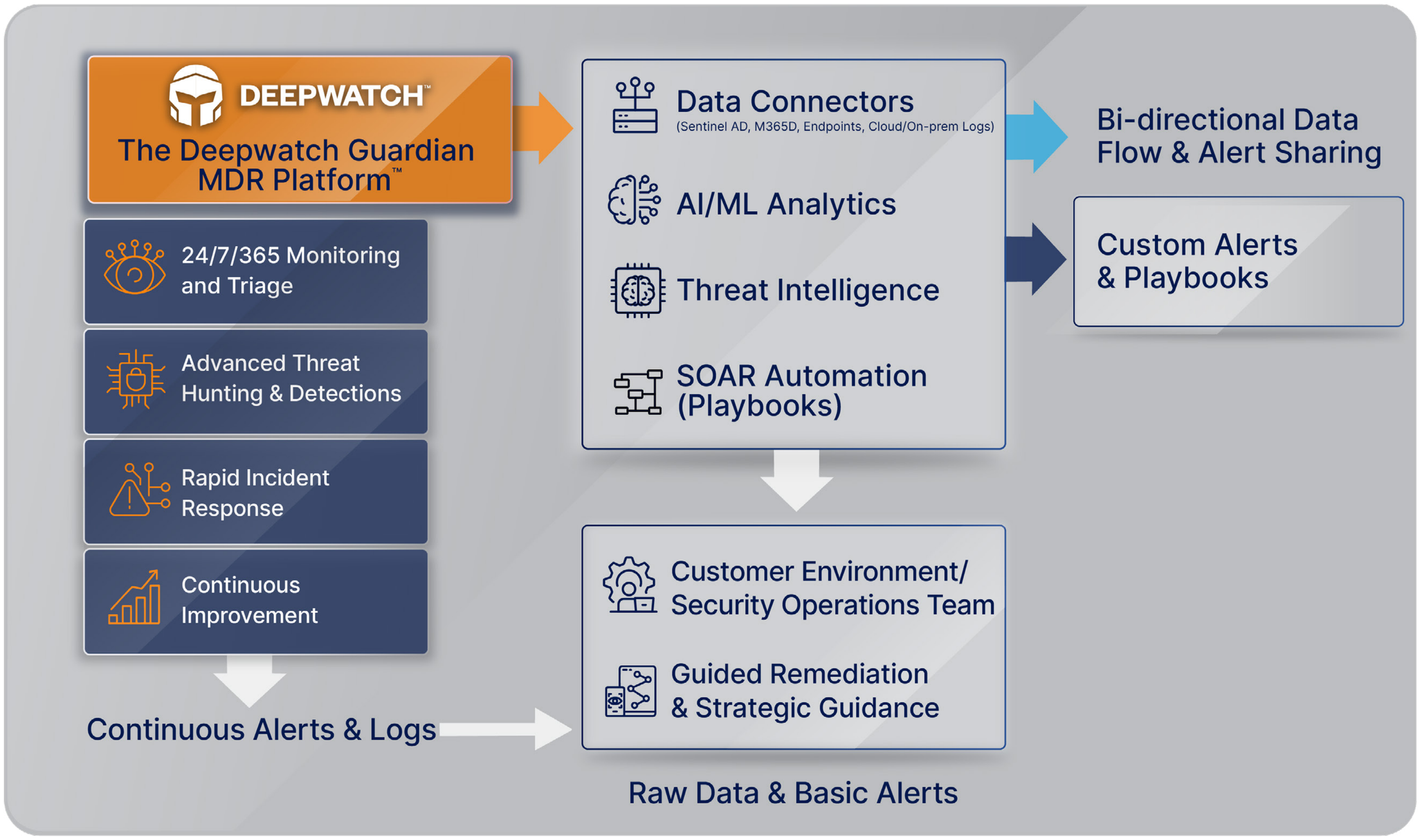
Deepwatch provides ongoing value through:

- **Regular Reporting and Insights:** Delivers detailed reports on security posture, detected threats, and recommendations for improvement.
- **Security Posture Optimization:** Provides strategic guidance on improving security controls and processes based on threat intelligence and an organization's specific risk profile.
- **Compliance Support:** Assists organizations in meeting regulatory compliance requirements by maintaining a strong security posture and providing necessary audit trails.



Deepwatch MDR and Microsoft Sentinel Integration Diagram

This diagram illustrates how Deepwatch MDR seamlessly integrates with Microsoft Sentinel to provide enhanced security operations.



1. **Data Ingestion:** Microsoft Sentinel acts as the central hub for ingesting security logs from various sources (Azure AD, M365D, Endpoints, Cloud/On-prem Logs) via its data connectors.
2. **Sentinel Processing:** Sentinel applies AI/ML analytics, leverages integrated threat intelligence, and utilizes its Security Orchestration, Automation, and Response (SOAR) capabilities (playbooks) to detect threats and generate alerts.
3. **Bi-directional Integration:** Deepwatch MDR establishes a bi-directional data flow with Microsoft Sentinel. This allows Deepwatch to:
   - Ingest raw data and basic alerts from Sentinel for further analysis and threat hunting.
   - Push custom alerts, detection rules, and response playbooks back into Sentinel, enriching its capabilities.
4. **Deepwatch MDR Capabilities:** Deepwatch's security experts perform 24/7/365 monitoring and triage, advanced threat hunting, and develop custom detections, all powered by the data within Sentinel. They also drive rapid incident response efforts.
5. **Customer Environment Interaction:** Deepwatch's Security Operations team provides guided remediation and strategic guidance directly to the customer's in-house security teams, leveraging the insights gained from Sentinel and Deepwatch's platform.

Solution Benefits

- **Accelerated Threat Detection:** AI and expert human analysts uncover and respond to threats in real time.
- **Reduced Alert Fatigue:** 98% reduction in false positives empowers teams to focus on critical incidents.
- **Measurable Security Improvement:** Deepwatch MDR drives year-over-year maturity, leveraged through Sentinel's rich analytics.
- **Flexible, Scalable Operations:** Deepwatch's MDR architecture adapts to customer environments and scales with Sentinel's cloud-native design.
- **Maximized ROI:** Deepwatch MDR optimizes Sentinel investments, yielding rapid detection, reduced response times, and cost-efficient security operations.

Conclusion

The integration of the Deepwatch Guardian MDR Platform with Microsoft Sentinel offers a powerful and comprehensive security solution. By combining Sentinel's robust cloud-native SIEM capabilities with Deepwatch's expert human-led threat detection, hunting, and response, organizations can significantly enhance their security posture, reduce operational overhead, and confidently navigate the evolving threat landscape. This partnership allows businesses to achieve **24/7/365 proactive defense**, freeing their internal teams to focus on strategic security initiatives.

DEEPWATCH™

Always Watching. Always Protecting.™

Deepwatch® is the leader in Precision MDR powered by AI and humans. We amplify human expertise with AI insights to reduce the risks that matter most to your business. Our protection is proactive, preemptive and responsive, tuned to your business, with no black boxes, and watched by experts 24/7/365.

Learn more: **www.deepwatch.com/microsoft-sentinel**

Follow us:

Blog | LinkedIn | Facebook