BDO DIGITAL

Microsoft

Microsoft
2023 Partner of the Year

Winner
Security Award

Supercharge your security operations with MXDR

Improve your Security Operations Center (SOC) efficiency with unrivaled threat intelligence and automated attack disruption of sophisticated attacks like ransomware with MXDR Active Protect.

The current state of security operations

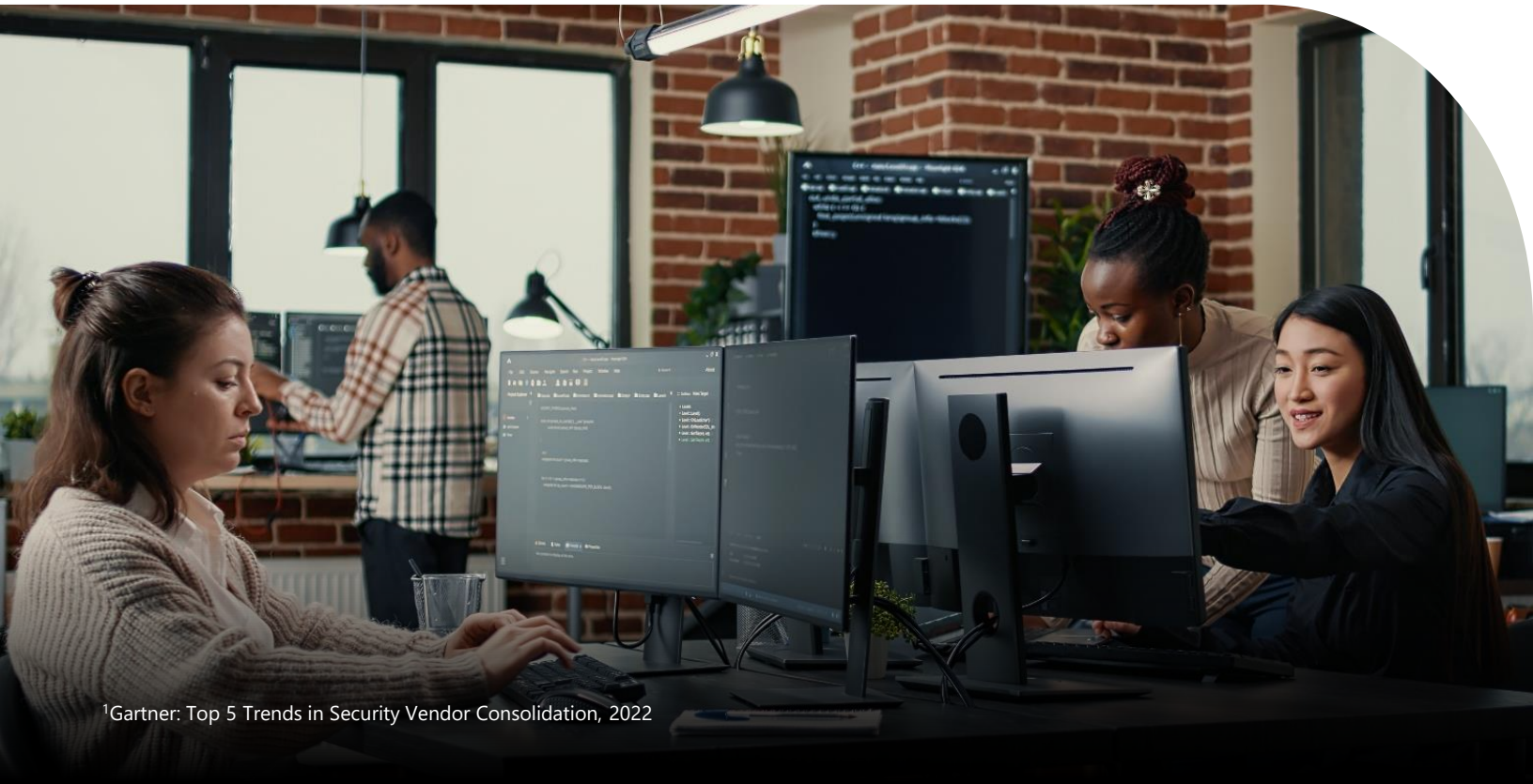
Growing frequency, speed, and sophistication of threats

Today's cybersecurity landscape continues to see an increase in attacks across all categories – more phishing, more ransomware campaigns, more identity-centric threats, while also growing in velocity. With the ransomware as a service (RaaS) gig economy on the rise, anybody can now get their hands on tooling developed by the cyberworld's most prolific nation-state attackers, increasing their success rates and ability to scale.

Siloed solutions are slowing response

It's no longer enough to protect your endpoints and have an entirely separate email security strategy. Attacks are targeting the gaps between these siloed point solutions and crossing multiple domains, leaving defenders to have to manually correlate individual alerts together to detect a broader attack. Sophisticated attacks are moving across email and endpoints, all the way to user identities, cloud applications and your data. A point solution strategy leaves security analysts to manually correlate alerts together to identify attacks because they never see the big picture. This not only slows down detection, but investigation and remediation as well.

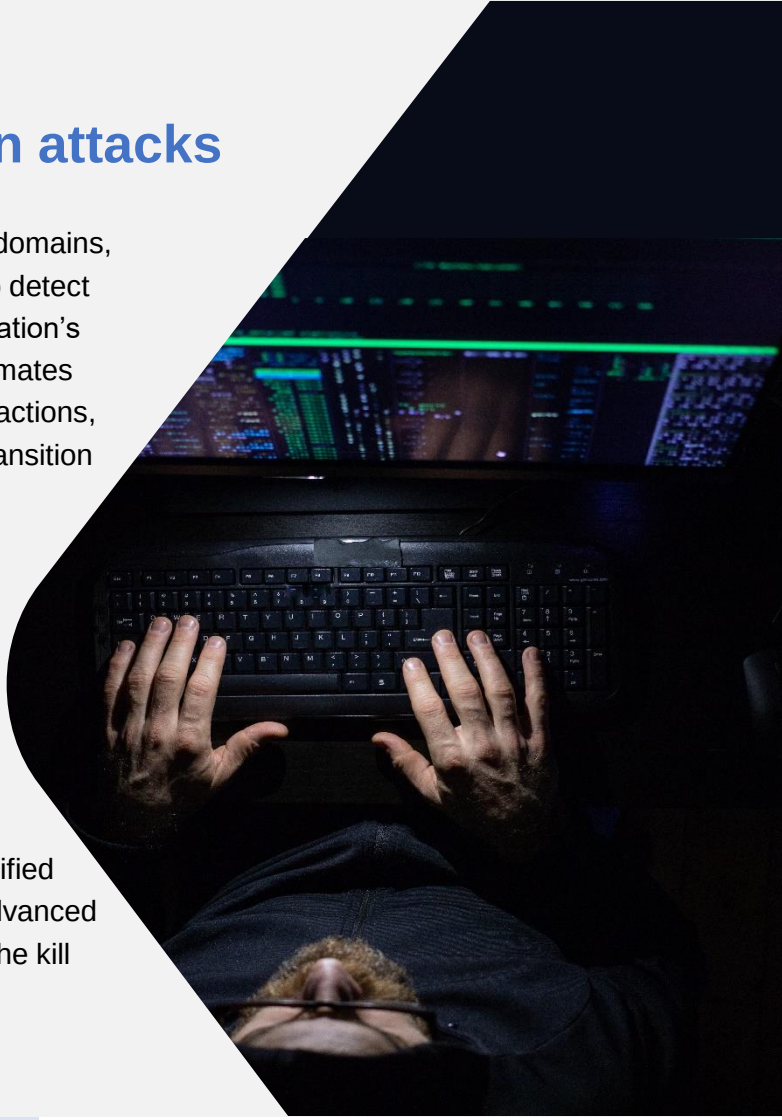
According to a Gartner study, security decision makers are becoming more dissatisfied with the operational inefficiencies and lack of integration that come with using a diverse range of traditional security tools and are instead seeking more effective and integrated solutions.[1]



[1]Gartner: Top 5 Trends in Security Vendor Consolidation, 2022

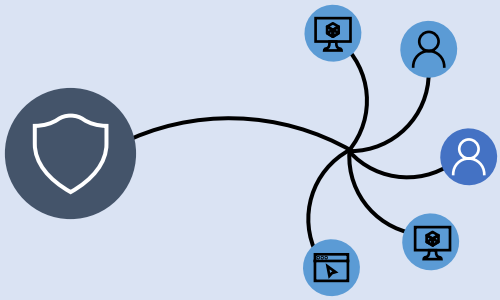
MXDR—the answer to modern attacks

To tackle the nature of modern attacks crossing multiple domains, security teams need a unified solution that allows them to detect and respond to threats more efficiently across an organization's entire digital estate. Using powerful intelligence that automates the correlation and analysis of data, as well as response actions, MXDR can help the Security Operations Center (SOC) transition from a reactive approach to a proactive defense strategy, while improving threat detection, response times, and most importantly freeing up time for the SOC analysts to focus on proactive hunting and prevention.



Managed Extended Detection and Response

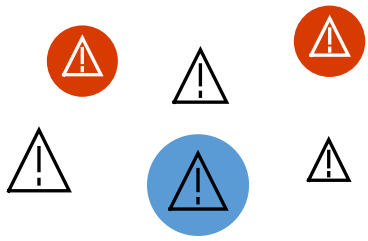
(MXDR) solutions are designed to deliver a holistic, simplified and efficient approach to protect organizations against advanced attacks. They give SOC teams a more complete view of the kill chain for more effective investigation and provide auto remediation across multiple domains using vast sets of intelligence and built-in artificial intelligence (AI).



Managed Extended Detection and Response

- Holistic security and signal correlation across identity, email, endpoint, cloud app, data loss prevention (DLP) security, and more
- Incident-based investigation and response experience
- Protects against advanced attacks such as ransomware and business email compromise (BEC)

vs.



Endpoint Detection and Response (EDR)

- Endpoint security only
- Siloed endpoint alerts
- Can only help fend off endpoint-specific attacks and lacks the big picture to help with advanced attacks

MXDR gives security teams a new way to drive process and cost efficiency across their operations. As you consider an MXDR solution for your organization, look for this critical set of capabilities:

01.

Advanced kill chain visibility and protection

To protect against advanced attacks, MXDR solutions need to cover different asset types and unify security for critical threat entry points like email and identity, but also protect attack points further down in the kill chain including endpoints, cloud apps, and DLP data. By consolidating these data sources, MXDR solutions correlate low level alerts into a single incident and help uncover the full kill chain of a sophisticated attack that would be overlooked by point security solutions.

02.

Unified investigation and response

Effective MXDR solutions are designed to enable security analysts to be more effective. Incident-based investigation showing the end-to-end view of attack, contextual deep dives, and response playbooks with best practices, are all critical in making it easier for SOC teams to investigate and respond to attacks more efficiently.

03.

Automation

The increasing volume and speed of advanced attacks challenge the capacity of most security teams. MXDR solutions provide automation in two ways. They use the breadth of their underlying signal and AI to provide built-in automation to respond to advanced attacks, but also provide options for companies to create custom automations. Both help scale the SOC scale.

04.

Broad intelligence and threat vector visibility

An MXDR solution should incorporate intelligence. It should draw insights from a broad set of sources to analyze signals and better understand the threat landscape, as well as first-party research that informs prevention, detection, and protection mechanisms. A greater number and diversity of signals enhance the ability to see and understand more threat vectors, allowing the MXDR solution to quickly identify an attack at an earlier stage, reduce the amounts of alerts and incidents, and enable the SOC team to respond to the latest threats more effectively.

05.

Improved total cost of ownership

MXDR enables vendor consolidation for organizations by integrating multiple, siloed security tools purchased into a unified solution. It removes the need to purchase from various vendors and the manual work needed to correlate signals. Instead, MXDR provides a comprehensive solution for detection, response, and remediation - reducing acquisition costs and process overhead.

Stay ahead of advanced attacks

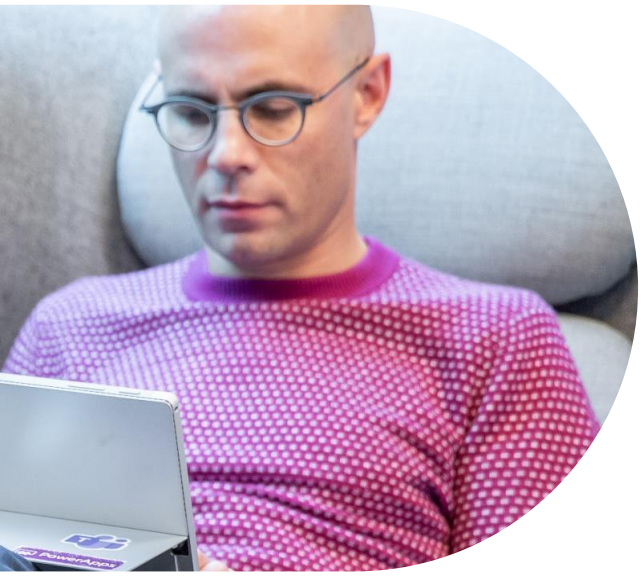
Speed matters in a security analyst's daily operations. That's why Active Protect provides unified investigation and response designed to deliver the most efficient experience for SOC teams for faster response times.

For a streamlined investigation, Active Protect provides a visual graph of the attack, showing all impacted entities to help the SOC easily understand how the attacker went from compromise to target.

You can investigate alerts in the context of the entire incident and use in-product remediation playbooks to respond quickly—all as a connected experience without context switching. You can even dive deep with a single language for advanced hunting across all services. Additionally, to make sure automations help you respond even faster Active Protect supports real-time custom detections.

Enabling a data-centric SOC with DLP signal

DLP is crucial for organizations to protect sensitive information and mitigate the risk of data loss or leakage. Integrating DLP alerts into the incident investigation experience gives SOC analysts an entirely new way to prioritize, based on the sensitivity of affected data.



Active Protect gives you the ability to understand the impact of a data breach quickly by correlating DLP alerts into the MXDR incident view, the ability to conduct advanced hunting, as well as take remediation actions directly from the Active Protect portal. Adding data-centricity into your SOC experience will simplify the correlation of an attack to the detection of data leaks to understand the impact end-to-end faster and more effectively.

Supercharge your SOC experience with Active Protect, the BDO Digital MXDR solution

A comprehensive MXDR solution, Active Protect delivers a unified investigation and response experience and provides native protection across endpoints, hybrid identities, email, collaboration tools and cloud applications with centralized visibility, powerful analytics and automatic attack disruption. With Active Protect, organizations can gain a broader set of protections including email security and identify and access management as critical preventative solutions, benefit from auto-healing capabilities for common issues, and scale SOC teams with MXDR-automated disruption to protect against ransomware and other advanced attacks more effectively while safeguarding organizations' business continuity.

Active Protect provides defenders with a host of key capabilities to stay ahead of attackers, including:

1. Enable rapid response with MXDR-prioritized incidents

Active Protect correlates native signals across multi-platform endpoints, hybrid identities, email, and collaboration tools, as well as SaaS apps and DLP insights to provide a complete view of the kill chain. This deep context allows SOC teams to investigate and respond at the incident level, making prioritization easy and remediation faster.

2. Disrupt advanced attacks at machine speed

Active Protect leverages the breadth of our MXDR signal and our research-informed, AI-driven detection capabilities to identify advanced attacks like ransomware and provides automatic response at the incident level with automatic attack disruption. Attack disruption contains in-progress attacks by automatically disabling or restricting devices and user accounts used in an attack—stopping progression and limiting the impact.

Scale your SOC team with automatic containment of affected assets

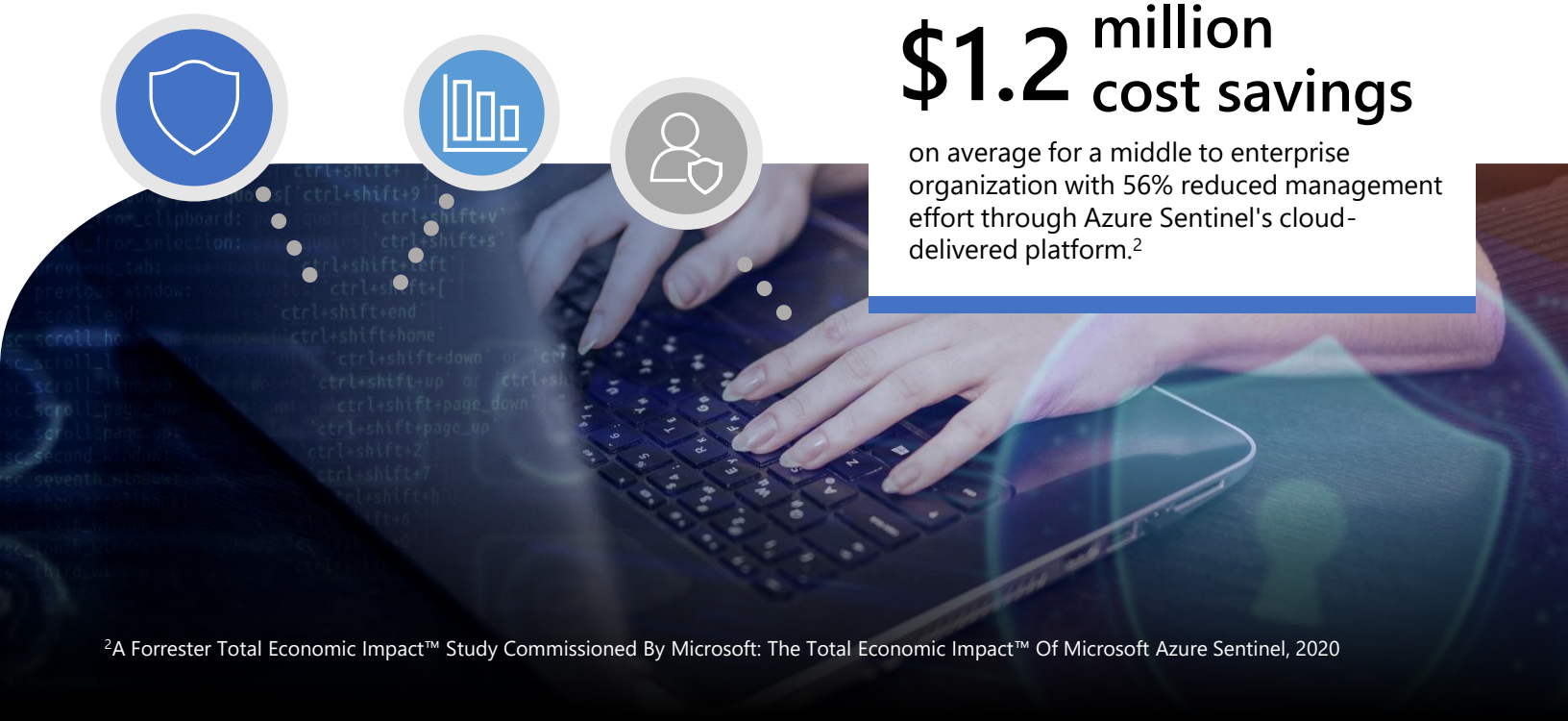
Automatic attack disruption is designed to contain attacks in progress by automatically disabling or restricting compromised devices and user accounts—stopping progression and limiting the impact to organizations. This is a big innovation; today most security teams can't respond fast enough to sophisticated attacks like ransomware or BEC campaigns and are typically reactive by cleaning up based on impact. With attack disruption, attacks are contained to a small number of assets, dramatically minimizing the impact and improving business continuity.

We help future proof your solutions:

Our team embraces technology, constantly researching new threats and vulnerabilities to new technology so we are able to better protect you. We practice defense in depth and offer a full suite of threat management solutions – MDR, Vulnerability Management as a Service (VMaaS), Infrastructure Management, Threat Intelligence and Threat Hunting), and we pull this all together to provide a holistic solution with strong integration points for faster time to resolution.

$1.2 million cost savings

on average for a middle to enterprise organization with 56% reduced management effort through Azure Sentinel's cloud-delivered platform.[2]



[2]A Forrester Total Economic Impact™ Study Commissioned By Microsoft: The Total Economic Impact™ Of Microsoft Azure Sentinel, 2020

3. Beyond Traditional MDR

Traditional managed detection and response (MDR) combines technology and the expertise of experienced professionals to deliver a modern security solution. An MDR solution hunts for threats, provides monitoring, and responds to those threats to keep an organization safeguarded. A security operations center delivers these services remotely, helping companies to limit the impact of threats without having to hire more staff. At BDO Digital, we took things even further beyond traditional MDR. By combining all the great benefits of MDR with Active Insights and Active Assure, we're able to deliver a comprehensive, one-of-a-kind security solution to organizations looking to strengthen their defense and cybersecurity program.

Benefits of Active Insights

Reduce costs and reallocate resources by identifying under-used and over-allocated licenses.

Drive continuous cost optimization, using in-depth visibility to enhance governance, reduce tool sprawl, and redirect savings into value-add programs.

Maximize security coverage by identifying and managing risks through enhanced configurations.

Benefits of Active Assure

Demonstrate effectiveness of MMXDR solution and de-risk the business through continuous testing.

Provide ongoing validation and peace of mind in near real time confirming the security controls, and processes are functioning as expected as your IT landscape and threats change.

Enable continuous testing and counter-measure deployment (purple teaming) for continuous strengthening of the cyber program.

The MXDR with Azure Sentinel Differentiators [3] :

79%

reduction in false positives

80%

reduction in the amount of labor associated with investigation, leading to $2 million in efficiency gains

201%

ROI - with a payback period of less than six months

[3]BDO Digital: Managed EndPoint Detection & Response with Azure Sentinel, 2023

What customers are saying

Helping a manufacturing company improve their cybersecurity posture

BDO Digital's MXDR solution helped this manufacturing company by saving them time and allowing them to monitor their environment 24x7x365. Our solution also provides the client with ongoing recommendations for continuous improvement of their security posture to support their business as it continues to evolve.

Modernizing a cyber program for a behavioral health organization

A behavioral health organization was looking to improve their overall cyber posture and reduce the risk of incidents. BDO Digital's MXDR solution helped them do exactly that while also helping them consolidate partners, rationalize technology and reduce costs, and improve end-user satisfaction.

Summary

BDO Digital MXDR offers enhanced threat hunting, detection, and quick response across endpoint, network, on premises, and cloud environments to enable visibility across all areas of your information systems. Our team of security specialists leverage Microsoft Azure Sentinel and are rooted in more than 25 years of industry threat detection and response experience. We can identify risk, initiate counter-measures, reduce downtime, and help organizations manage security response.

Our MXDR solution works for you so that you can focus on driving your business forward!

Request a free trial today

Starting with a 60-day trial allows customers to experience Microsoft Sentinel's threat intelligence and security analytics platform delivered through BDO Digital's Active Protect service at no cost.

Step 1:
Onboard

Step 2:
Deliver

Step 3:
Review

Ready to get started?

Contact us today.