Solution Brief

MaxxMDR

Rapid detection, zero-latency response, and a relentless focus on using offense to strengthen defense.

We Don't Just Deliver Alerts. *We Deliver Outcomes.*

Finding a service provider or tool to generate security alerts is easy. The hard parts are:

- Making sure you don't have visibility gaps
- Preventing your team from being overwhelmed by noise
- Responding quickly with the right expertise when critical incidents occur
- Staying focused and engaged as threats are investigated, contained, and evicted

Legacy managed security service providers make these items your problems. And even managed detection and response (MDR) providers often forget the "R" when critical security incidents occur.

That's why we created a different kind of MDR solution: **MaxxMDR**.

MaxxMDR at a Glance

- 24x7x365 threat detection
- Zero-latency response
- Integrated reporting, automation, and ticketing
- Continuous threat exposure management
- Deception token deployment and monitoring
- Seamless DFIR engagement

MDR with a Big 'R'

MaxxMDR acts as an extension of your in-house security team, providing 24x7x365 threat detection and response. There are four key elements that set us apart:

- We take the time to understand your unique environment and risk factors and tailor our MDR approach for a perfect fit
- We play the lead role in the response process, performing in-depth investigation when needed and guiding you to resolution
- We proactively identify opportunities to enhance your security posture before weaknesses can be exploited
- We apply learnings from a broad range of offensive security activities to continually improve your defensive security measures

This means that we don't deliver new problems to your team's doorstep. We handle many security incidents before you ever hear about them, and we provide a high-value, guided response when critical threats require your attention.

Turning Data into Reliable Security Signals

Important storylines about risk are often waiting to be told in activity log data. But too often, they are either overshadowed by noise or missed because of visibility gaps.

MaxxMDR solves this by:

- Collecting signals from your most critical data sources, including endpoint detection and response (EDR) platforms, cloud providers, identity providers, network security devices, custom applications, and more
- Applying high-fidelity detection content that is tuned to your environment to separate the security signals that matter from the noise
- Applying lessons learned through threat response and offensive security activities to proactively improve the effectiveness and accuracy of our detection techniques

Tech-Enabled MDR

DEVO

splunk> a CISCO company

exabeam

SentinelOne

CROWDSTRIKE

Microsoft Defender for Endpoint

Executing Zero-Latency Response

The teams in our globally distributed security operations centers (SOCs) initiate a set of zero-latency response workflows whenever critical threats are detected, following pre-agreed rules of engagement. Whenever possible, we take proactive actions on your behalf, such as isolating compromised systems or initiating other automated responses through your EDR platform. And when deeper investigations are necessary, our SOC analysts are empowered to engage an overlay team of threat response experts early in the response process. This team performs an in-depth assessment to further understand the scope of compromise and develops detailed response recommendations. This means that critical events never sit in a queue waiting for attention. Response is immediate, and our team leads the way to resolution. For large-scale incidents that require engagement of specialized digital forensics and incident response (DFIR) experts, the fast action by our SOC and threat response teams accelerates these efforts and provides timesaving supporting research.

Continuously Assessing Your Threat Exposure

While ongoing threat detection is essential, it is not enough on its own. The ideal outcome is identifying possible threats and weaknesses before they escalate into a critical incident. That's why we proactively perform continuous threat exposure management (CTEM) for all MaxxMDR customers.

Our CTEM approach includes:

- External vulnerability scanning to ensure that we always have a clear and up-to-date view of your attack surface
- Monitoring for information about your IT infrastructure in the public domain and "dark web" that could potentially be used as part of an attack

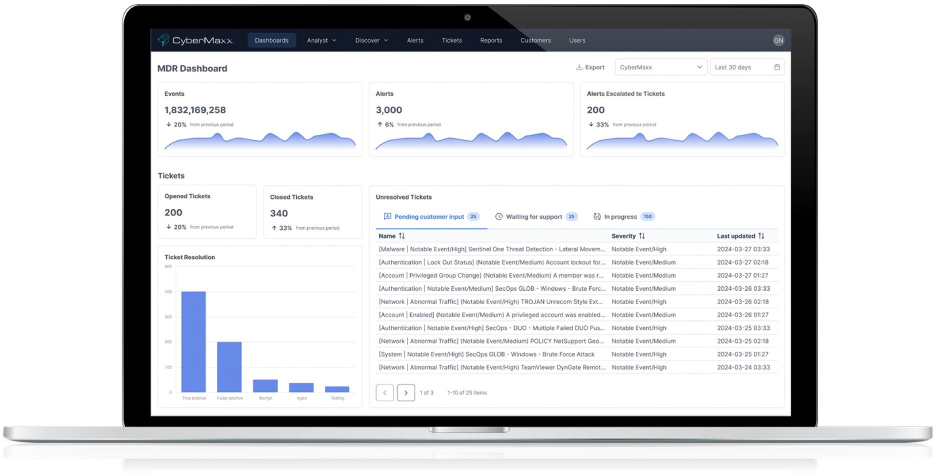
By performing these functions on an ongoing basis, CTEM acts as an early warning system, detecting many types of emerging threats early – before negative business impacts occur.

Mastering the Art of Deception

Another proactive measure we take for MaxxMDR customers is the deployment and monitoring of file-based deception tokens. These decoy files are strategically placed within your network to mislead and track attackers who breach your environment. Any engagement with these deception tokens will alert our SOC, revealing the attackers' presence and tactics. This acts as a complement to our primary threat detection techniques, further reducing dwell time when breaches occur and giving our threat responders detailed insights into the attackers' tools and techniques that can then be turned against them as part of the response.

MaxxProtect Platform

MaxxMDR is powered by the MaxxProtect Platform, which brings all of your essential MDR technologies together into a unified interface.



Name ⇅	Severity ⇅	Last updated ⇅
[Malware | Notable Event/High] Sentinel One Threat Detection - Lateral Movem...	Notable Event/High	2024-03-27 03:33
[Authentication | Lock Out Status] (Notable Event/Medium) Account lockout for...	Notable Event/Medium	2024-03-27 02:18
[Account | Privileged Group Change] (Notable Event/Medium) A member was r...	Notable Event/Medium	2024-03-27 01:27
[Authentication | Notable Event/Medium] SecOps GLOB - Windows - Brute Forc...	Notable Event/Medium	2024-03-26 03:33
[Network | Abnormal Traffic] (Notable Event/High) TROJAN Unrecom Style Ext...	Notable Event/High	2024-03-26 02:18
[Account | Enabled] (Notable Event/Medium) A privileged account was enabled...	Notable Event/Medium	2024-03-26 01:27
[Authentication | Notable Event/High] SecOps - DUO - Multiple Failed DUO Pus...	Notable Event/High	2024-03-25 03:33
[Network | Abnormal Traffic] (Notable Event/Medium) POLICY NetSupport Geo...	Notable Event/Medium	2024-03-25 02:18
[System | Notable Event/High] SecOps GLOB - Windows - Brute Force Attack	Notable Event/High	2024-03-25 01:27
[Network | Abnormal Traffic] (Notable Event/High) TeamViewer DynGate Remot...	Notable Event/High	2024-03-24 03:33

This includes:

- A fully managed security information and event management (SIEM) platform
- All necessary data feed connections to support ongoing monitoring activities
- A proprietary library of threat detection content, expertly tuned to your needs and risk profile
- Integrations with complementary security systems, such as EDR, to support automated responses
- Dashboards, reports, and full event details
- Integrated ticketing functionality

The MaxxProtect Platform is designed with transparency in mind. Even as you entrust us to perform sensitive security monitoring and response activities on your behalf, you always have complete visibility into our approach and activities.

Use Offense to Fuel Defense with the MaxxMDR Cyber Resiliency Bundle

Our optional MaxxMDR Cyber Resiliency Bundle integrates a robust set of recurring offensive security services with your MDR approach, including:

- Assessments of your security configurations
- External and internal penetration testing
- Deployment and monitoring of hardware-based deception tokens

Bringing offensive and defensive security together into a holistic model elevates the effectiveness of your MDR approach by:

- Empowering our threat responders with an even deeper understanding of your IT environment and security stack
- Identifying additional opportunities to reduce your attack surface proactively
- Applying learnings from offensive security activity to make ongoing improvements to our MDR detection techniques and content

About CyberMaxx

CyberMaxx, founded in 2002, is the leading provider of managed detection and response (MDR) services. We help customers reduce risk by tightly integrating MDR with offensive security, threat hunting, security research, digital forensics and incident response (DFIR) to continually adapt to new and evolving threats. Our modern MDR approach is tailored to the unique characteristics and risk factors of each customer, enabling us to take full ownership of the response process and, optionally, manage key security controls. By thinking like an adversary and defending like a guardian, we help our customers stay a step ahead of threat actors.

Learn More, Today!

To learn more about CyberMaxx's solutions please visit, CYBERMAXX.COM to get started.