Cyber Falcon

UnderDefense

Managed Detection & Response

Everyone can be hacked. The difference is in Response. We build Cyber Resiliency.

6 Hours
Average industry time of reaction between notification about critical incident and reaction

34 Hours
Average time for IT/Security team to take an response action and remediate the threat

50 Days
Attackers will stay undetected in your network with impacting your key assets, IP, code, brand, pricing

What is MDR?

Managed Detection and Response is a service that combines continuous monitoring of a business's digital assets with an "always-on" certified incident response team to defend your network to first prevent, and ultimately to respond to a cyber attack.

1. **Acquire industry leading expertise to help drive detection and response**. The level of competency and experience gained from investigating a myriad of incidents across different client environments results in a world class MDR expert team. For a typical enterprise, finding, developing, and retaining this talent is not impossible, but it's not affordable.

1. **Become proactive rather than becoming the attacker's victim waiting to react**. Being proactive means always to be vigilant. Detection and response teams fail because they can't escape the constant deluge of activities to which they have to react and respond. An MDR service is the way out for shifting in the direction of a proactive security approach.

1. **Sharing responsibility with your internal security team**. Even when a security organization has a detection and response team, deciding what to prioritize is a challenge. For example, the internal team may focus on external threats but hand off insider threat incidents to an outside firm performing MDR.

Awards & Recognition

REVIEWED ON Clutch ★★★★★ 31 REVIEWS

Clutch #1 Cyber Security Company in 2020

Gartner ★★★★★

Gartner Top 10 Security Consulting Vendor

comparitech

Best SIEM provider by Comparitech

A TRANSBORDER VENTURES Joint

We take your existing tools, tune them to max and automate response to minimize reaction time and better protect your business

UnderDefense

UD Analysts Team

Your tools of choice

splunk> · Azure Sentinel · elastic · SentinelOne · Radar · LogRhythm · chronicle · CROWDSTRIKE · Cyber Falcon

Managed Detection and Response

The most Cost-effective service

Why MDR?

When business critical assets are at risk in today's digital economy, protecting those assets must be of the utmost priority. Increasingly, compliance and regulatory entities require logging & security monitoring be in place. It's no secret that there is a scarcity of skilled cybersecurity professionals, it is in the millions, which has generated a significant challenge for CIOs and CISOs to identify, hire, and retain top talent to protect their digital landscape.

In order to build your own Security Monitoring today, business owners need to make large CAPEX investments and most CFOs & CEOs prefer predictable Operational expenses. In-house SOCs are typically very expensive, overloaded, engineers are burning out from boring routine, and 24x7 coverage is a struggle to gain full visibility of attacks and policy violation inside the network.

The UnderDefense MDR

A tailor-made approach to predict, prevent, detect and respond to malicious activity. It's a perfect choice for proactive companies who want to strengthen their security postures and remain a step ahead of the cybercriminals.

- we recapture value from your cyber security tool investments
- we make your tools works effectively
- we automate response to react to incidents in minutes, not hours
- we watch your environment 24x7 and notify you about confirmed Threats and anomalies

40 000

Endpoints Protected by UnderDefense Globally Today

Cloud Security Focus

we are experts in top cloud platforms

amazon web services

amazon web services Certified — SysOps Administrator - Associate

amazon web services Certified — Solutions Architect - Associate

aws certified Security Specialty

Azure

Microsoft Certified — Azure Security Engineer Associate

Google Cloud Platform

Google Cloud Certified — Professional Cloud Security Engineer

Google Cloud Certified — Professional Cloud Network Engineer

Key Features:

Worlds' best cybersecurity experts as part of your team

Automated Incident Response

24/7/365 Protection

Advanced Forensics

Customized approach to cybersecurity

MDR Services by UnderDefense Include :

- **360 degree cybersecurity at a scale:** UnderDefense offers both Defensive and an Offensive capabilities enabling us to identify our clients true cybersecurity needs and provide 360 protection. We support global multinationals as well as SMB & mid-market enterprises. Supporting clients globally, our 24/7 MDR team offers continuous security monitoring with elite talent in an economically attainable model.
- **Advanced threat prevention:** A vital part of a proactive approach to cybersecurity is continuous monitoring to threat detection that targets your business. Multiple teams enable UnderDefense to deliver complex threat analysis. Based on research, known attack methods, and unusual activity indicators, UnderDefense's SOC experts work to identify persistent threats. They work with battle-tested tools to analyze network telemetry, logs from security devices, applications, and systems to rapidly uncover time-sensitive insights about active threats and reduce dwell time. These processes enable UnderDefense security experts to identify even the most sophisticated attacks before they start.
- **Elite team of experts:** Ranked as one of the highest cybersecurity firms globally, our experts have deep knowledge in proactive threat hunting. We know that every business environment is unique which is why our designated security experts focus on your security posture and business requirements to upfit and complement your cybersecurity maturity. Our tailored approach provides insight into data exfiltration, discovers advanced persistent threats and gaps in security posture, and as a result, develops the most effective cyber-protection for your business.
- **High-powered automatization:** Unlike other MDR providers, we are not limited to simply monitoring and notification, but can also implement automatization to deliver response at machine speed, detect important incidents between false positives through continual analysis of threat indicators and behavioral data, and help you maximize the value of your tools without acquiring new ones, by working in the background to configure, tune, and optimize technologies and processes based on your unique profile.
- **Dedicated security experts to protect your highest risk assets**: Focused on your security and business requirements, your designated security expert works as a member of your team to level up your security maturity. In-depth individualized evaluation, protection, and customized response services enhance MDR services for greater insight into data exfiltration and discovery of advanced persistent threats.

Additional Exceptional Capabilities:

Some additional capabilities and deliverables that make our MDR exceptional as a part of our service offering, or that complement it, not available through other well known MDR vendors are:

- Flexibility of SOAR integration of your choice (e.g. Phantom, Siemplify, Demisto)
- Offensive security capabilities (Ethical Hacking, Penetration Testing)
- Security hardening and implementation
- Compliance visibility and implementation capabilities (SOC2, ISO, HIPAA)
- Executive and board level cyber resiliency consulting
- Cloud security setup and hardening
- Self provisioning portal with all agents
- Cyber Resiliency training and program guidance
- Malware analysts
- Office 365 / Google apps & cloud API integration AWS cloud trail API integration
- Alerting via Slack or email enabled
- Deep Dark Web monitoring / leaked accounts monitoring

UnderDefense MDR Packages, Capabilities & Features

	Standard	Enhanced	Professional
Detection	**Level 1**	**Level 2**	**Level 3**
Co-Managing your EDR/NGAV	X	X	X
24x7 monitoring and notifications	X	X	X
Alert triage	X	X	X
Direct Chat with our analysts in 24x7 mode	X	X	X
Remediation guidance	X	X	X
Co-Managing your SIEM,(Splunk, Elastic, Logrythm. IBM Qradar, Archsight, RSA etc)		X	X
Proactive threat hunting		X	X
Advanced Metrics, reporting and summaries for Compliance		X	X
UnderDefense Library with 1500+ detection rules		X	X
Weekly Reporting		X	X
Several best of breed Threat Intel Feeds			X
Tuning your security tools			X
Malware analysts			X
Response			
Incident validation and notification	X	X	X
Manual Remote response with customer IT (40 hours/y)		X	X
Containment and remediation			X
Resilience recommendations			X
Automated Response Integration with customer Tools			X
Advanced service details			
24x7 Alert triage performed by UD analysts	X	X	X
Scheduled Automated Reports	X	X	X
Office 365 / Google Apps & Cloud API Integration AWS Cloud Trail API Integration	X	X	X
Alerting via Slack or Email enabled	X	X	X
Nessus Vulnerability Scan Log Integration		X	X
Free Knowledge Transfer		X	X
Vulnerability Management		X	X
Web-based portal login		X	X
Handle multi-step investigations: trace activities associated with compromised systems and apply the kill-chain methodology to see the attack lifecycle		X	X
Compliance Management		X	X
Dedicated Customer engagement manager		X	X
8x5 Technical Support		X	
Continuously monitor: clearly visualize security posture with dashboards, key security indicators, static & dynamic thresholds, and trending		X	X
PCI, HIPAA and CIS Top 20 Pre-Defined Reports		X	X
24x7 Technical Support			X
Prioritize and act: optimize, centralize, and automate incident detection workflows with alerts, centralized logs, and pre-defined reports and correlations			X
Custom Reporting Enabled			X