GoSecure

MANAGED DETECTION AND RESPONSE

For many organizations, security is an either/or decision as need far outweighs available resources. The need for new technology is apparent, but not so the budget or experienced personnel. GoSecure offers advanced, cloud-delivered detection and response solutions backed by the hyper-experienced team from our Active Response Center.

STOPPING ATTACKS BEFORE YOU KNOW THEY HAPPEN

Cyberattacks are a daily occurrence. Cybercriminals are constantly changing tactics and techniques to bypass the latest security approaches. Cybersecurity teams find themselves at a loss against this daily onslaught. Too much information, not enough people or time, insufficient skills; any one can describe the world of today's security professionals.

GoSecure Managed Detection and Response (MDR) watches your endpoints and networks, looking for even the smallest hint of suspicious activity. GoSecure Active Response Center (ARC) threat hunters maintain 24x7 vigilance to protect your organization from the latest, advanced cyberattacks. Going beyond traditional indicator of compromise threat hunting, GoSecure MDR utilizes behavioral analysis to understand "what it does" combined with "what it can do" to develop the appropriate mitigative response and act on your behalf. That is why our customers are happy to know that we respond to attacks before we notify them – act first, notify second.

Why GoSecure?

Visibility: Collecting over 150 unique event types, compared to an industry average of less than 50, GoSecure MDR starts with this highest level of visibility. From endpoints to network to email and web traffic, the GoSecure ARC has the most behavior data of any MDR provider from which to start their investigations.

Analysis: Combining the benefits of machine learning with the strength of human analysis, GoSecure MDR exposes even the slightest hint of suspicion from its massive data pool. By analyzing behaviors, rather than simply binary indicators of compromise (bad IP address, known malicious websites, etc.), GoSecure MDR can "connect the dots" between seemingly disconnected behaviors. This allows GoSecure MDR to identify attacks that are both brand new as well as variants of previous attacks.

Experience: Managed Detection and Response is purpose built to address the limitation of previous Managed Security Services. And GoSecure has been delivering MDR longer than any other vendor. The focus of everything from our automation to the human threat hunters in the GoSecure Active Response Center is designed to identify threats, investigate the depth and scope of those threats and execute the appropriate mitigation response.

Response: Detecting attacks is vital but stopping them is just as important. With an industry average dwell time of, by some reports, over 80 days, attackers have plenty of time to exist within a network and perform their malicious actions. GoSecure MDR was built to do one thing – detect and respond in less than 15 minutes. And, most importantly, mitigate attacks with zero false positives. Our customers expect us to respond – and we deliver.

WORKING TOGETHER TO MAXIMIZE EFFECTIVENESS

GoSecure MDR delivers the breadth of functionality required to protect every organization from todays advanced attacks. Every element is designed to work both independently, but also collaboratively with all others. And the GoSecure ARC is constantly operationalizing all interactions to maximize their synergistic interoperability.

Next-Generation Antivirus

Replace legacy antivirus solutions with the latest endpoint anti-malware technology to address emerging, fileless, memory-based attacks and more.

Endpoint Detection & Response

Leverage cutting edge threat hunting and machine learning to continuously monitor and observe all aspects on endpoint activity to mitigate attacks before they happen.

Inbox Detection & Response

Stop phishing and ransomware attacks in the email inbox before they ever reach the endpoint.

Proactive Threat Hunting

Not content with just reviewing alerts, the GoSecure Active Response Center uses alert data to deliver proactive threat hunting specific to your environment. As attack techniques change, it requires a team that understands how to connect the proverbial pieces to find the threats targeting your organization.

Multi-Dimensional Threat Intelligence

Threat intelligence is the foundation of all security operations. GoSecure combines threat intelligence from numerous sources, in addition to our own dedicated research, to create our proprietary multi-dimensional threat intelligence.

Context-Based Incident Response

Stopping attacks as quickly as possible is the goal of every security organization. By understanding the context of an attack, GoSecure MDR is able to quickly respond in the exact way necessary to mitigate the initial attack and set the stage to defend against future attacks.

Network Detection & Response

Proactively monitor and detect unwanted network traffic activity to identify and mitigate network compromises and internal attacks.

Insider Threat Detection & Response

Detect and eliminate malicious and unwanted behavior by employees and administrators to secure data and protect business reputation.

In-Memory Analysis

The only true in-memory threat detection, GoSecure In-Memory Analysis scans live memory, reverse engineers suspicious code and then predicts malicious intent.

GoSecure

GoSecure is recognized as a leader and innovator in cybersecurity solutions. The company is the first and only to integrate an Endpoint and Network threat detection platform, Managed Detection and Response services, and Cloud/SaaS delivery. Together, these capabilities provide the most effective response to the increased sophistication of continuously evolving malware and malicious insiders that target people, processes and systems. With focus on innovation quality, integrity and respect, GoSecure has become the trusted provider of cybersecurity products and services to organizations of all sizes, across all industries globally. To learn more, please visit: https://www.gosecure.net.