

GoSecure  
**TITAN™**  
**MANAGED**  
**SOLUTIONS**

# GoSecure **YOUR TRUSTED ADVISOR**

GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Detection and Response service. For over 10 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MDR and Advisory Services solutions delivered by one of the most trusted, skilled and experienced teams in the industry.



## GoSecure **TITAN™ MANAGED SECURITY SOLUTIONS**

### Defend Your Organization

Identifying and responding to the increasingly sophisticated attacks posed by ransomware, malware and other threats, challenges security teams daily. Rapid and effective mitigation can be the difference between just another day at the office and catastrophic damage to an organization. As security teams struggle to keep up with a constant stream of alerts and potential incidents, managed security services offer the tools and support to DEFEND organizations from threats in the evolving cybersecurity landscape.

A full range of GoSecure Titan™ Managed Security Solutions can find more potential issues and mitigate them faster than traditional offerings. Organizations get the support needed to defend against breaches across networks, endpoints, email, and the cloud—backed by experts available 24/7/365 who often resolve threats before the client even knows they existed. Organizations are able to answer the question—“Are we secure?” with a resounding “Yes.”



### GoSecure Titan Managed Detection & Response | Trust in Your Security

**GoSecure Titan Managed Detection & Response (MDR)** identifies, blocks and reports potential breaches, backed by the experienced threat hunters in the GoSecure Active Response Center (ARC) who respond swiftly to help remediate issues with a best-in-class response time of 15 minutes from detection to mitigation.

- Flexible, bundled offerings deliver organizations the coverage they need to defend against breaches, along with support from experienced security professionals who become an extension of the in-house security team.
- The GoSecure Titan MDR portal centralizes client security health data—delivering easy to understand charts and graphs for network, endpoint and event data—as well as reporting and centralized ticketing into a single pane of glass.



### GoSecure Titan Endpoint Detection & Response | Defend Your Endpoints

Endpoints are a constantly growing point of exposure for organizations—and they can be compromised 24/7, 365 days a year. **GoSecure Titan Endpoint Detection & Response (EDR)** tools automate monitoring and mitigation activities to stop threats before they can spread—and when purchased with GoSecure Titan MDR services, get support from expert analysts who address potential threats as an extension of the security in-house team.

- Automates the identification and containment of suspicious activity - and blocks potentially malicious threats such as fileless malware attacks, while delivering visibility across endpoints for data collection and analysis.
- Will remove or contain potential threats in the early stages of an attack, along with analytics and forensics tools that predict threat intentions and help pinpoint root causes.



### GoSecure Inbox Detection & Response | Safeguard the Inbox

**GoSecure Inbox Detection & Response (IDR)** a solution, empowering users to send any suspicious email for professional evaluation and response—which saves organizations valuable time and resources while protecting against breaches.

- Easily deploys into Office 365 desktop, web and mobile inbox – streamlining the process to submit suspicious email and delivering a seamless user experience with 24/7 support and analysis of submissions by GoSecure experts.
- Delivers a combination of automated scanning and skilled human analysis from GoSecure experts when reviewing submissions—returning an easy-to-understand status—typically minutes after submission.
- Offers immediate incident response for threats, including global removal for malicious messages.



### GoSecure Titan Insider Threat Detection & Response | Deter Insider Threats

Increasingly, threats are emerging from accidental, negligent or malicious activity inside organizations where traditional cybersecurity defenses are not prepared to combat them. **GoSecure Titan Insider Threat Detection & Response (ITDR)** can help monitor, detect, deter and respond to these often-overlooked threats.

- Go Secure Titan ITDR enables organizations to define policies that will protect from accidental exposure and monitor for suspicious behavior, pinpointing threats for deeper investigation and collecting legal evidence as needed.
- More than 50 rulesets can be deployed across endpoints to manage access, trigger alerts, degrade access automatically and ensure action is taken quickly when a threat is detected.



### GoSecure Titan Next Generation Antivirus | Stop the Breaches

**GoSecure Titan Next Generation Antivirus (NGAV)** transcends traditional tools to help protect organizations from modern threats such as ransomware and fileless attacks. Backed by the experienced threat hunters in GoSecure Active Response Center (ARC), it monitors and blocks potential breaches across browsers, email, document readers and more—as well as scans memory for malicious activities such as fileless attacks, flagging activities based on organization-specific defined rules.

- Continuous 24/7 automated monitoring and managed support protects organizations around the clock. The GoSecure ARC determines the severity of identified threats and responds accordingly to contain, mitigate and resolve problems—often before the organization even knows there was an issue.
- Integrates seamlessly with existing technologies and operating systems such as Windows, Mac and Linux without impacting performance.



### GoSecure Titan Network Detection & Response | Protect Your Networks

Gaining visibility into the cloud, virtual and on-site networks is critical to defend against breaches but requires significant resources – especially to answer corresponding alerts and investigate potential threats. **GoSecure Titan Network Detection and Response (NDR)** delivers comprehensive network visibility along with support from the skilled analysts at GoSecure to help protect against threats.

- Centralizes monitoring and reporting on network activities including categories for threats, mapping for events and source/destination IPs, to stop breaches before they can spread.
- Offers automated analysis from the Log Intrusion Detection System, as well as hunts for threats through the real-time behavioral analysis of the Network Intrusion Detection System (NIDS), which combines third-party threat intelligence with a proprietary GoSecure developed rulesets.



## GoSecure Titan Managed Firewall | Optimize Your Perimeter

GoSecure Titan Managed Firewall services helps organizations address the challenge of monitoring and managing their firewall infrastructure. The GoSecure Active Response Center (ARC) provides global coverage to keep firewalls operating at peak efficiency 24/7, 365 days a year.

- GoSecure Titan Managed Firewall supports industry leading vendors with full 24 x 7 monitoring of all systems for performance and/or availability issues.
- Incident, Change and Emergency Management are all handled by the skilled professionals in the GoSecure ARC, taking the burden off the in-house security teams and ensuring that environments of any size are maintained at peak efficiency and issues are handled quickly.



## GoSecure Titan Managed Security Incident & Event Management | Improve Alert Response

GoSecure Titan Managed Security Incident & Event Management (SIEM) offers support for organizations who want the benefit of collecting and analyzing security data in a central location but may not have the resources to address every alert. Two packages offer flexible support options for organizations based on needs, budget and business model.

- **GoSecure Titan Managed SIEM Essentials** offers a basic package for maintenance, annual service reviews, regular reporting, a self-service console, as well as managed and on-demand solution support.
- **GoSecure Titan Managed SIEM Enterprise** builds on the Essentials package with after-hours monitoring for high-risk use cases, regular change requests, monthly security reviews and a custom client runbook which determines actions that will be taken by the GoSecure team to support the in-house security team.



## GoSecure Titan Vulnerability Management as a Service | Maintain Your Defenses

GoSecure Titan Vulnerability Management as a Service (VMaaS) helps defend against the constantly changing threat landscape by keeping operating systems and applications up to date and in compliance. Support from GoSecure experts is available around the clock, coupled with scanning, deployment and reporting tools that save security teams time and improve security posture.

- GoSecure VMaaS is designed to identify assets and exposure through scanning, to prioritize threats using contextual analysis and to respond to issues by updating systems and applications.
- The experts at GoSecure will manage the patch process for operating systems and applications, offer full compliance reporting and develop remediation practices based on the business and security needs of the organization—enhancing security posture and delivering immediate ROI.

## Contact Information



Tel: 855-893-5428

24/7 Emergency: 888-287-5858



[sales@gosecure.net](mailto:sales@gosecure.net)



[www.gosecure.net](http://www.gosecure.net)

[www.gosecure.net/managed-detection-response](http://www.gosecure.net/managed-detection-response)