GoSecure Advisory Services offer comprehensive end-to-end assessment and testing solutions to help organizations evaluate their cybersecurity posture, risks and gaps. The experts at GoSecure can assess the capability of an organization to protect, defend and respond to threats—and collaborate with in-house resources to ensure that recommended improvements are actionable and practical. GoSecure Advisory Services provide real-world solutions to protect against breaches.

GoSecure Titan Software Solutions help block the threats, so they never make it into the environment. The combination of email and web security, along with in-memory analysis, deliver comprehensive protection to block attacks and stop malicious content before it can reach users.

GoSecure Titan Managed Detection and Response (MDR) offers a market-leading detection to mitigation response time of 15 minutes, delivering rapid action against today’s advanced attacks. GoSecure Titan Managed Security Solutions combine industry-leading security technology with highly skilled professionals who become an extension of the in-house security team, to mitigate threats before they can compromise sensitive data or business operations, allowing you to maximize your most valuable resources.

Prepare for, identifying and responding to the increasingly sophisticated threats posed by ransomware, phishing, social engineering and other attacks, 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. Our full range of GoSecure Titan® Managed Security Solutions, GoSecure Titan® Software Solutions and expert Advisory Services help protect against and find more potential issues than traditional offerings. And with managed services, teams get the support they need to mitigate threats faster and recover with as little impact to the organization as possible.

GoSecure is a recognized global leader and innovator in cybersecurity solutions. We believe people make technology better. With focus on combining the best of technology with skilled people, GoSecure has become the trusted cybersecurity advisor to organizations of all sizes, across all industries. Our expert cybersecurity staff works as an extension of your IT operations across the endpoint, network and inbox... and beyond.
Benjamin Corll, VP of Cybersecurity and Data Protection / Chief Information Security Officer, Coats Group, PLC

“The great visibility and control help me sleep better at night with peace of mind that we have broad visibility and control - and that 6,500 of our systems are secure.”

Benjamin Corll, VP of Cybersecurity and Data Protection / Chief Information Security Officer, Coats Group, PLC

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 customizable views 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 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 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.

Get the Managed Detection & Response advantage with support delivered by skilled threat hunters who become an extension of your in-house security team.

When I asked about the potentially infected machine GoSecure told me ‘We covered you first, before even telling you that you have a problem.’ And that specific event made us sign up the next day.”

Scott Howell, Managing Director of Technology and Information Services, McInnes Cooper
GoSecure Titan Responder PRO | Investigate the Threats

GoSecure Titan Responder PRO offers memory forensics and behavioral analysis capabilities. GoSecure Titan Responder PRO cuts through the wide array of anti-forensic measures employed by today’s cybercriminals to uncover artifacts critical for incident response and threat hunting.

• Leverages the proprietary behavioral engine, Digital DNA, to develop impact scoring, which assists in malware analysis and helps identify other threat indicators.
• Searches, identifies and reports on critical digital artifacts like passwords, encryption keys, internet search histories and other forensic data located in memory.
• Intuitive interface integrates smoothly with existing tools and processes to streamline your investigative workflow and produce rapid results.

GoSecure Titan Secure Web Gateway | Block Web-based Threats

GoSecure Titan Secure Web Gateway provides real-time malware defense and URL classification using a combination of automated and human threat intelligence, supported by GoSecure Titan Labs. GoSecure Titan Secure Web Gateway is a highly effective and affordable solution to enforce organizational policies and to keep users secure from advanced web-based attacks.

• Powerful control features and real-time malware defense helps defend against exposure from botnets, viruses, malware and more.
• Comprehensive reporting and real-time monitoring make it easy to manage with improved user productivity, low latency and lower false positive rates.

GoSecure Titan Managed Firewall | Optimize Your Perimeter

GoSecure Titan Managed Firewall services help 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 Secure Email Gateway | Stop Email Attacks

GoSecure Titan Secure Email Gateway offers protection from email-based threats generated by viruses, spam and ransomware, as well as socially engineered threats including phishing, business email compromise and account takeover.

• A hosted solution that can be provisioned immediately, without having to install any hardware or software.
• Robust and dynamic phishing and spam filter technology combined with advanced malware protection and malware sampling technologies to quickly and effectively identify and block attacks before they reach the user.

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.

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 maintain the tools themselves. 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 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 Managed Firewall | Optimize Your Perimeter

GoSecure Titan Managed Firewall services help 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 Firewall | Optimize Your Perimeter

GoSecure Titan Managed Firewall services help 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 Security Compromise Assessment | Find the Threats

A GoSecure Security Compromise Assessment (SCA) can help find the hidden threats that automation alone may not detect. The SCA combines 60 days of GoSecure Titan Managed Detection and Response (MDR) with skilled, experienced human threat hunting, which delivers an edge over pure automation that can find threats to sensitive data that could potentially compromise current or future operations. The SCA can identify potential risks to your networks, endpoints & more.

GoSecure Privacy & Compliance Services | Improve Data Protection

GoSecure Privacy & Compliance Services evaluate and improve data protection and privacy practices to help achieve compliance goals.

- A comprehensive Privacy Practices Assessment delivered by the trusted privacy and security experts at GoSecure will evaluate the current privacy programs in place, assess the regulatory landscape that applies to an organization and help improve compliance with regional, national and international data protection standards.
- GoSecure Payment Card Industry Data Security Standard (PCI DSS) services are available for organizations who need help with the Self-Assessment Questionnaire (SAQ) and in Canada, GoSecure is a Qualified Security Assessor who can conduct a full assessment, resulting in a Report on Compliance (ROC).

GoSecure Red & Purple Team Services | Improve Your Defenses

GoSecure Red Team and Purple Team services can help deliver improved security posture, enhanced cybersecurity defenses and a better prepared team - ready to respond to real-world attacks.

- GoSecure Red Team strategic engagements combine multiple available attack techniques with experienced security professionals to the test the in-house reaction and detection capabilities at an organization.
- GoSecure Purple Team strategic engagements take a 'test, fix, test again, repeat' approach to rapidly improve security posture for organizations through a long-term, collaborative engagement with in-house teams.

GoSecure Penetration Testing Services | Test Your Defenses

Rely on Penetration Testing from GoSecure to help identify the impact attackers can have on an organization. The Offensive Security Certified Professional (OSCP) team at GoSecure will design a program based on the threat model, including industry and technology stack of an organization.

- GoSecure delivers programs that will identify where and how adversaries can target an organization, including internal and external networks, web applications, mobile apps & devices, Wi-Fi, endpoints, physical security and phishing attacks.
- GoSecure can also assist with code review and embedded device/industrial testing.

GoSecure Incident Response Services | Respond and Recover Faster

A cyberattack can happen to an organization at any time. GoSecure Incident Response programs prepare organizations to contain, resolve and recover from breaches faster, minimizing operational, financial and reputational impact. GoSecure offers both year-long retainer programs and emergency incident response support services that come with recovery guidance and dark web monitoring from expert threat hunters.

GoSecure Cybersecurity Assessment | Determine Your Security Maturity

Gain a comprehensive understanding of security posture, risks and gaps with a GoSecure Cybersecurity Assessment (CSA) providing actionable insights into cybersecurity maturity and delivering practical recommendations based on the type of organization—size, industry, etc. Choose from two packages.

- The CSA Enterprise includes several phases that assess the critical aspects of your technology, environments, policies and procedures, targeted to deliver overall security improvements.
- The CSA Essentials package is streamlined and highly focused, designed to provide the most important insights that can drive security roadmaps and improvements that address the biggest risks and issues based on the industry associated with an organization.

GoSecure Breach Readiness Services | Prepare for Cyberattacks

GoSecure Breach Readiness Services test and sharpen incident response capabilities and prepare organizations to respond when a breach happens.

- The GoSecure Breach Readiness Assessment (BRA) offers a comprehensive evaluation of incident preparedness from business continuity to incident response and through disaster recovery, ensuring that the people, processes, tools and policies are ready when a breach happens.
- GoSecure Tabletop Exercises are custom-designed, real-world exercises that test tools, processes, policies and people with emphasis on group problem-solving under pressure. Communications, documentation and cross-functional engagement are also evaluated throughout the exercise.

GoSecure Red & Purple Team Services | Improve Your Defenses

Red Team and Purple Team services can help deliver improved security posture, enhanced cybersecurity defenses and a better prepared team - ready to respond to real-world attacks.

- GoSecure Red Team strategic engagements combine multiple available attack techniques with experienced security professionals to the test the in-house reaction and detection capabilities at an organization.
- GoSecure Purple Team strategic engagements take a 'test, fix, test again, repeat' approach to rapidly improve security posture for organizations through a long-term, collaborative engagement with in-house teams.

GoSecure Privacy & Compliance Services | Improve Data Protection

GoSecure Privacy & Compliance Services evaluate and improve data protection and privacy practices to help achieve compliance goals.

- A comprehensive Privacy Practices Assessment delivered by the trusted privacy and security experts at GoSecure will evaluate the current privacy programs in place, assess the regulatory landscape that applies to an organization and help improve compliance with regional, national and international data protection standards.
- GoSecure Payment Card Industry Data Security Standard (PCI DSS) services are available for organizations who need help with the Self-Assessment Questionnaire (SAQ) and in Canada, GoSecure is a Qualified Security Assessor who can conduct a full assessment, resulting in a Report on Compliance (ROC).

GoSecure Security Compromise Assessment | Find the Threats

A GoSecure Security Compromise Assessment (SCA) can help find the hidden threats that automation alone may not detect. The SCA combines 60 days of GoSecure Titan Managed Detection and Response (MDR) with skilled, experienced human threat hunting, which delivers an edge over pure automation that can find threats to sensitive data that could potentially compromise current or future operations. The SCA can identify potential risks to your networks, endpoints & more.
Contact Information

Tel: 855-893-5428
24/7 Emergency: 888-287-5858

sales@gosecure.net

www.gosecure.net