GoSecure

www.gosecure.net

GoSecure
SOLUTIONS OVERVIEW

GoSecure

YOUR TRUSTED ADVISOR

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.

DEFEND YOUR ORGANIZATION WITH CYBERSECURITY SOLUTIONS FROM GOSECURE

Security teams face the challenge of preparing for, identifying and responding to the increasingly sophisticated threats posed by ransomware, phishing, social engineering and other cyber-attacks. Rapid and effective mitigation can mean the difference between just another day at the office and lasting catastrophic damage to your organization.

Protecting from accelerating cyber threats requires a layered security approach. That's why we have built a portfolio of complementary offerings. When each of our three pillars; **GoSecure Titan® Managed Security Solutions**, **GoSecure Titan® Software Solutions** and expert **GoSecure Advisory Services** are included in a comprehensive cybersecurity approach, the value and effectiveness of the solutions are amplified and the results are noticeable.

The cornerstone of **GoSecure Titan Managed Security Solutions** is the *Proven Protection, Fast Response* delivered by our **GoSecure Titan® Managed Detection and Response (MDR)** service. With a market-leading detection to mitigation response time of 15 minutes, you'll be ready for advanced attacks and have managed support options from the experienced threat hunters on the GoSecure team. Other managed solutions extend our expert managed support to help with important core security activities like firewalls, vulnerability management and SIEM.

GoSecure Titan Software Solutions help block threats from the most prominent attack vectors, so they never make it into the environment through email and web filtering capabilities, as well as in-memory analysis options.

And with expert **GoSecure Advisory Services**, your organization can *Test, Assess and Improve* your security posture. Identify risks and gaps, optimize your security tools, test your people, processes and technology—get the big picture or focus on a specific area of concern. GoSecure helps your organization learn and grow with every engagement.

GoSecure Titan® Managed Detection & Response

Proven Protection, Fast Response

GoSecure Titan Managed Detection & Response (MDR) can identify, block and report potential breaches, backed by the experienced threat hunters in the GoSecure Active Response Center (ARC) who respond swiftly to help address issues with a best-in-class 15-minute detection to response time.

- 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 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.

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.

"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 LLC

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 Broad Visibility and Expanded Protection in a Centralized Platform with GoSecure Titan

GoSecure Titan offers expanded protection, broad visibility and scalability in a managed detection and response platform. The GoSecure Titan platform centralizes critical data from GoSecure Titan Managed Detection & Response (MDR) services into a single pane of glass. Our platform not only provides better protection and prioritizes the most critical alerts—checking for three times more unique event types than the industry standard—but it also allows organizations to detect more threats, mitigate faster and lower overall security costs. With customizable views and alerts that ensure security organizations are able to prioritize their efforts, the GoSecure Titan platform delivers the intelligence that matters.

GoSecure Titan Managed Security Solutions

GoSecure Titan Managed Firewall | Optimize Your Perimeter

GoSecure Titan® Managed Firewall helps organizations address the challenge of monitoring and managing their firewall infrastructure. GoSecure has the skills and resources to manage any size environment and any number of firewalls.

- Operating 24x7x365, the GoSecure Active Response Center (ARC) provides global coverage to keep your firewalls operating at peak efficiency.
- Your organization will benefit from a combination of our threat intelligence, managed security solutions expertise, shared global delivery capability and in-depth network security knowledge to help secure your organization's first line of defense.

GoSecure Titan Managed Security Information & Event Management | Improve Alert Response

GoSecure Titan® Managed Security Information and Event Management (SIEM) services combine comprehensive visibility across IT environments within a centralized tool with easy-to-understand dashboards and robust reporting. GoSecure Titan Managed SIEM focuses on rooting out malicious behavior and limiting alert fatigue. We have use cases built on the MITRE ATT&CK framework with a library of more than 300 pre-built options. GoSecure Titan Managed SIEM offers two levels of service, **GoSecure Titan Managed SIEM Essentials** and **GoSecure Titan Managed SIEM Enterprise**, and is a good fit for organizations who want:

- A single tool to manage, filter and analyze data from numerous sources improves the ability to potentially spot threats and traces of malicious activity that may have previously gone undetected.
- To speed up the time to verify potential issues by applying use cases to identify high-risk, high-confidence threats and limit false positives with options for monitoring and management by experts at GoSecure.
- The ability to define parameters for logging and storage of data, as well as provide extensive reporting capabilities that support compliance objectives.

GoSecure Titan Vulnerability Management as a Service | Maintain Your Defenses

GoSecure Titan Vulnerability Management as a Service (VMaaS) delivers complete solution options for organizations to keep systems and applications updated and in compliance. For organizations who want ongoing support, we offer managed options to remediate issues and improve security posture.

- GoSecure Titan VMaaS is a flexible offering designed to give organizations the right level of protection for their needs. Our options include scanning, patch management or full-service deployment across covered systems and applications.

GoSecure offers a **Vulnerability Scan Assessment Report** for organizations who want to identify if GoSecure Titan VMaaS is the right fit. This 2-week engagement gives you line of sight into gaps in patching and asset issues.

- Our team of experts provides recommendations to reduce risk and improve your patching program. The engagement concludes with a one-hour consultation to review our findings and a complete asset and vulnerability analysis report full of insights that you keep.

GoSecure Titan Software Solutions

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 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 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 ADVISORY SERVICES

Test, Assess and Improve with expert Advisory Services from GoSecure

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, polices and people with emphasis on group problem-solving under pressure. Communications, documentation and cross-functional engagement are also evaluated throughout the exercises.

GoSecure Custom Cybersecurity Consulting Services | Put Our Experts to Work for You

Our team spans security disciplines to deliver proactive advice and recommendations to improve security posture tailored to your organization's needs.

- **GoSecure Custom Cybersecurity Consulting** engagements are designed to meet the specific needs of your organization and optimize your cybersecurity programs. We assist organizations who want to focus on building proactive solutions to some of the biggest challenges in cybersecurity today — from how to defend against breaches to plans for recovery after an attack.
- Our engagements can include, but are not limited to, customized tabletop exercises, immersive offensive exercises and custom testing, threat simulation and threat emulation, threat intelligence workshops and briefings, technology and architecture strategy reviews, compliance and third-party risk policy / program reviews.

Don't see what you are looking for? Contact us to learn about our full range of custom consulting expertise.

GoSecure Cybersecurity Assessment | Understand and Improve Security Posture

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

- The **CSA Elite** and the **CSA Enterprise** packages both offer a comprehensive review of security posture. The package options vary based on the detail of analysis needed and breakdown of security elements reviewed. Both will deliver important insights that can help your organization drive security roadmaps and develop strategies to ensure you are getting value and results from your security technologies. Recommendations will focus on risks and issues in the industry associated with your organization.
- The **CSA Essentials** package is based on our Enterprise offering but streamlined and focuses exclusively on the areas that have the highest likelihood of incidents and breaches for your organization's industry.

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 retainer programs and emergency incident response services based on NIST SP 800-61r2 and SANS best practices.

- **GoSecure Incident Response Retainer (IRR)** - When a breach happens, organizations with a GoSecure Incident Response Retainer in place have priority access to experienced professionals to help quickly contain and address the issue. IRR clients benefit from a team who already knows the systems, processes and people at your organization thanks to the Response Roadmap developed during the onboarding process.
- **Emergency Incident Response (IR) Services** - The Incident Response team can provide emergency services with a short-term engagement. We offer access to security professionals who can help navigate through emergent incidents on a case-by-case basis.

"It (the Cybersecurity Assessment) was incredibly useful, done in a sympathetic way. Of course, it generated two years of work, but it got us to where we are—decent firewall, decent switches, decent integrations with endpoints—all those pieces. If we had not done that security assessment, I don't think we would have gotten to where we need to be."

Alan Tottman
Director of Information Management and Technology
Nova Scotia Pension Services Corporation

GoSecure ADVISORY SERVICES

Test, Assess and Improve with expert Advisory Services from GoSecure

GoSecure Red & Purple Team Services | Improve Your Defenses

Red Team and Purple Team services can help you improve your security posture, deliver enhanced cybersecurity defenses and help better prepare your team to respond to real-world attacks. All engagements are custom-designed to the specific needs of your organization.

- **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.
- **Collaborative Threat Hunting** engagements can be offered after a Red or Purple Team service or as a stand-alone. These custom-designed services will help enhance threat hunting skills for the in-house team by working with GoSecure experts on a real-world threat hunt scenario.

"A Purple Team engagement allows an organization to pinpoint strengths and weaknesses in people, processes and technology in a safe environment–before the threats become a reality."

Maxime Nadeau
GoSecure Ethical Hacker

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 Review** and **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 offers **Payment Card Industry Data Security Standard (PCI DSS)** services.GoSecure is a Qualified Security Assessor in Canada and can conduct a full assessment resulting in a Report on Compliance (ROC), as well as assist organizations who need help withthe Self-Assessment Questionnaire (SAQ).

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 can offer engagements based on your threat model, including industry and technology stack.

- Our team delivers engagements that will identify where and how adversaries can target your organization, including internal and external networks, web applications, mobile apps, wireless networks, endpoints and mobile devices, physical security and social engineering/ phishing attacks.
- GoSecure also has the specialized skills to assist with code review, SAP testing, cloud testing and embedded device/IOT/SCADA/industrial device testing, and other custom engagements.

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 that could potentially compromise current or future operations.
- The SCA can identify potential risks to your networks, endpoints and more. Your organization will receive a comprehensive report that explains our findings in detail.

GoSecure

Contact Information

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

sales@gosecure.net

www.gosecure.net