www.gosecure.ai

GoSecure

GoSecure
SERVICE OVERVIEW

GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Extended Detection and Response (MXDR) service. The GoSecure Titan® Platform delivers predictive multi-vector detection, prevention, and response to counter modern cyber threats. GoSecure Titan® Managed Extended Detection & Response (MXDR) offers the best-in-class response time from threat detection to mitigation with a solution that identifies, blocks, & reports potential breaches. For over 20 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MXDR and Professional Services solutions delivered by one of the most trusted and skilled teams in the industry.

YOUR TRUSTED ALLY

DEFEND YOUR ORGANIZATION WITH CYBERSECURITY SERVICES 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 Extended Detection & Response Services**, **GoSecure Titan® Platform** and expert **GoSecure Professional Security 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 Extended Detection & Response** is the Proven Protection, Fast Response delivered by it's services. With a market-leading detection to mitigation response time, you'll be ready for advanced attacks and have managed support options from the experienced threat hunters on the GoSecure team.

It's services extend to our expert managed support to help with important core security activities like firewalls, vulnerability management and **GoSecure Titan® Managed Security Information & Event Monitoring (Managed SIEM)**.

With early warnings, the **GoSecure Titan® Platform** blocks many attacks before they can impact an organization. GoSecure Titan® Platform is more than a MXDR platform, more than a security operations platform. It's a single platform that can balance consolidation, transparency and actionability, allowing cybersecurity professionals from across your organization to stay above the crowd, be in control, act and thrive.

And with expert **GoSecure Professional Security 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.

MANAGED EXTENDED DETECTION & RESPONSE (MXDR)

GoSecure TITAN

[Detect & Mitigate Faster]

Organizations are seeking more visibility into the health of their infrastructure and events within their technologies and security professionals share a single top concern – protecting their organizations from attacks.

The GoSecure Titan® MXDR service, built upon four foundational pillars—Next-Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Inbox Detection and Response (IDR)—delivers proactive and comprehensive threat protection.

Built on an open XDR architecture, our MXDR service is designed to support existing investments by allowing choice within various elements of the configuration and to help your organization in its consolidation efforts.

GoSecure Titan® MXDR identifies, blocks and reports potential breaches, often before the organization is even aware there is an issue – backed by the experienced threat hunters in the Security Operations Center (SOC) who respond swiftly to help remediate issues with a best-in-class response time from detection to mitigation.

GoSecure Titan® Managed Extended Detection & Response offers:

- Protection against advanced threats
- The ability to do more with your investments
- Human-powered service
- A foundation you can trust & build upon

GoSecure TITAN

GOSECURE TITAN® MANAGED ENDPOINT DETECTION & RESPONSE (EDR)

[Defend Your Endpoints]

GoSecure Titan® EDR solution combines market-leading visibility with multi-observational analysis to detect threats more effectively and respond faster.

While traditional antivirus has been effective at stopping known attacks, adversaries now leverage new techniques to bypass these defenses. With obfuscation, encryption, and fileless malware that operates in memory, these threats evade traditional security technologies.

Our solution acts as a unified shield, providing multi-layered defense that detects not only known vulnerabilities but also preemptively identifies and mitigates emerging threats before they can cause harm.

GoSecure Titan® Managed Endpoint Detection & Response offers:

- In-Memory Detection
- Predictive Analytics
- Automatic Mitigation
- Responsiveness

GOSECURE TITAN® VULNERABILITY MANAGEMENT AS A SERVICE (VMAAS)

[Maintain Your Defenses]

With 60% of breaches involving unpatched known vulnerabilities, **GoSecure Titan® VMaaS** is designed to Identify assets and exposure through scanning, Prioritize threats using contextual analysis and Respond by updating systems and applications to strengthen resistance to attacks, shorten remediation times and maintain compliance.

Many organizations lack the resources, time, and expertise to effectively manage vulnerabilities and often spend their time patching the wrong vulnerabilities.

The GoSecure Titan® VMaaS service combines industry leading technology with expert analysis to provide unsurpassed speed, accuracy, consistency, and reliability the organization customized vulnerability management program making them more secure while saving time and money.

GoSecure Titan® VMaaS is:

- Operational time savings
- Proactively reduce cyber risk
- Immediate ROI
- Real-time visibility, reporting & metrics
- Maintaining compliance

GOSECURE TITAN® MANAGED SECURITY INFORMATION & EVENT MONITORING (SIEM)

[Improve Alert Response]

GoSecure Titan® Managed SIEM focuses on rooting out malicious behavior and limiting alert fatigue. It offers advanced security intelligence, comprehensive incident handling, simplified compliance, scalability, threat intelligence integration, and optimized security operations. With our cutting-edge solution, we empower organizations to actively protect their valuable assets and maintain a robust security posture in the face of evolving cyber threats.

GoSecure combines best-in-class tools with proprietary threat intelligence built over years of operational experience to help clients shape a platform that delivers the right intelligence for them with fewer false positives.

GoSecure Titan® Managed SIEM is:

- Real-time incident handling
- Comprehensive visibility
- Compliance and regulatory support
- Customizable and scalable
- Comprehensive protection

GOSECURE TITAN® MANAGED PERIMETER DEFENSE (MPD)

[Optimize Your Perimeter]

Continuous monitoring and management of your perimeter defenses is the first line of defense for any organization's network.

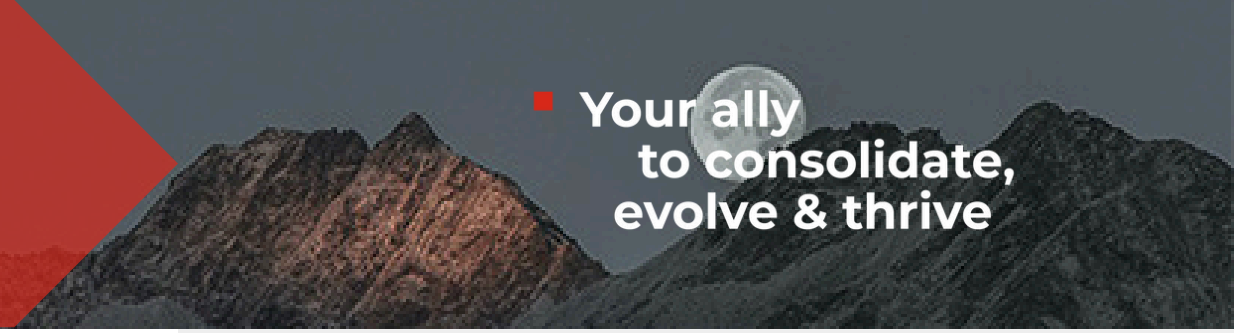
It commands more time from network security managers than virtually any other activity. And it's easy to get wrong, particularly by IT administrators doing double duty as their organizations' IT security staff.

GoSecure's network security team provides the required expertise to identify and implement better perimeter controls ensuring that externaly facing systems are protected.

GoSecure Titan® Managed Perimeter Defense offers:

- Better security 24x7
- Easier maintenance
- Faster deployment
- Reduced expense

GoSecure TITAN



GOSECURE TITAN® INBOX DETECTION & RESPONSE (IDR)

[Safeguard The Inbox]

Employees are now part of the solution, not the problem. Security teams are overburdened dealing with one of the top threat vectors in today's landscape—phishing.

Both investigating suspicious email from automated email security filters and reviewing employee submissions consume time and resources some teams don't have available. Most organizations continue to offer employee awareness training and fine tune email security programs, but have not been able to stop opportunistic, targeted threats via email from turning into potential security breaches.

GoSecure Titan® Inbox Detection & Response (IDR) gives every user the ability to test any suspicious email. They can finally stop worrying about missing threats, wasting time wondering what to do, or worrying about "crying wolf" too often. With a simple click, employees now become a united force against phishing.

GoSecure Titan® IDR is:

- Phishing & malware defense
- Inbox integration & ease
- Office 365 compatibility
- Customizable team control

GOSECURE TITAN® THREAT MODELER

[Mitigate The Threats]

GoSecure Titan® Threat Modeler is a sophisticated tool merging traditional threat modeling and MITRE ATT&CK, providing a holistic view of an organization's threat landscape.

This integration goes beyond just identifying control gaps; it evaluates security program maturity by incorporating security assessment results, contextualizing security controls based on identified threats.

By mapping technical controls to MITRE ATT&CK techniques, the tool prioritizes threat remediation and fortifies security. It also assesses program maturity by integrating security assessments and aligning controls with deployed technologies and known threats, ensuring targeted and effective defenses.

GoSecure Titan® Threat Modeler offers:

- Comprehensive threat landscape representation
- Control coverage insights
- Evaluation of security program confidence and maturity
- Meaningful scores and contextualized controls

GOSECURE TITAN® IDENTITY

[Control Your Operations]

Designed to generate alerts based on specific real-world offensive techniques, **GoSecure Titan® Identity** is a suite of technologies that deliver detections and alerts as a service.

Organizations uses GoSecure Titan® Identity to provide high quality (low false negative and false positive) alerts to their in-house operations personnel without the need to build and maintain complex data-science-based analytics. Its detections are classified by MITRE ATT&CK technique which facilitates triggering response procedures/runbooks within the client's operations center.

It is optimized to detect the most critical identity-related attacks, thus providing high security value.

By implementing **GoSecure Titan® Identity**, organizations will:

- Improve their ability to detect threats
- Respond to identity-based threats promptly
- Reduce the risk of data breaches, unauthorized access, and other security incidents that may arise from compromised user identities.

GOSECURE TITAN® SECURE EMAIL GATEWAY (SEG)

[Optimize Your Perimeter]

GoSecure's Titan® Secure Email Gateway (SEG) shields organizations from diverse email threats while enhancing email communication security.

Functioning as a filter between internal and external email traffic, it blocks malicious or unwanted emails from reaching recipients' inboxes.

The SEG ensures email communication's security, integrity, and confidentiality, serving a critical role in safeguarding against threats that could compromise data security, harm reputation, or incur financial losses.

As an integral part of an organization's cybersecurity strategy, Secure Email Gateways complement solutions like Endpoint Detection and Response (EDR), intrusion detection systems, firewalls, and antivirus software.

GoSecure's Titan® Secure Email Gateway offers:

- Enhanced email security
- Filtering capabilities
- Data protection

PLATFORM

GoSecure TITAN

[Beyond An Operations Platform:A Comprehensive Security Ecosystem]

The GoSecure Titan® Platform consolidates critical security data, provides unmatched visibility and delivers proven protection with customizable views.

With early warnings, the **GoSecure Titan® Platform** blocks many attacks before they can impact an organization. Combined with GoSecure Titan® Managed Extended Detection and Response (MXDR) Foundation, expert human threat hunters are delivering mitigation services to help ensure that threats are addressed quickly and effectively to protect the organization from significant damage.

GoSecure Titan® is more than a MXDR platform, more than a security operations platform. It's a single platform that can balance consolidation, transparency and actionability, allowing cybersecurity professionals from across your organization to stay above the crowd, be in control, act and thrive.

GoSecure Titan® Platform is:

- Your Centralized Security Hub
- Simple and Scalable
- Regaining Control
- Staying Above the Crowd

PROFESSIONAL SECURITY SERVICES

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.
- **Digital Forensics & Incident Response (DF&IR) Services** - Comprised of security experts with years of experience in response and forensics, helping minimize the exposure and facilitating rapid mitigation and clean-up. Whether you need a full-blown investigation, or simply another set of eyes, GoSecure can meet your needs with a Digital Forensics & Incident Response (DF&IR) Services.

GOSECURE SECURITY MATURITY ASSESSMENT (SMA)

[Understand & Improve Your Security Posture]

Gain a comprehensive understanding of security posture, risks and gaps with a GoSecure Security Maturity Assessment - providing actionable insights into cybersecurity posture and delivering practical recommendations based on your organization size, industry, etc.

- **Enhance Your Information Strategy** - If you have an existing information security strategy, your organization will benefit from an evaluation of its current cybersecurity posture, as well as the opportunity to determine if you are getting the most value out of your current security tools. Our experts can recommend updated configurations, find gaps or help identify areas for investment.
- **Strategic Security Roadmap** - Crafts tailored roadmaps by analyzing your security posture, presenting vital insights and recommendations aligned with your risks. This roadmap, equipped with dashboards and compliance connections, empowers proactive measures for heightened security. Ideal for new programs or entrants to an organization, it establishes baselines across crucial security elements and offers targeted improvement suggestions for configurations and investments.

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, etc.
- GoSecure also has the specialized skills to assist with code review, SAP testing, cloud testing and embedded device/IOT/SCADA/industrial device testing, radio frequency, and other custom engagements.
- **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.

MICROSOFT SECURITY OPERATION (SECOPS)

Your ally
to consolidate,
evolve & thrive

[Assess, recommend, deploy and configure Microsoft security tools and component]

The objective of this engagement is to fortify the organization's digital ecosystem by addressing key security considerations across various dimensions. GoSecure aims to identify and rectify potential vulnerabilities, misconfigurations, and weaknesses within the M365 environment to mitigate the risk of exploitation by malicious actors.

This assessment will closely examine the effectiveness of identity and access management controls, ensuring robust authentication and authorization mechanisms. Additionally, the assessment focuses on enhancing data governance and protection, scrutinizing data classification, labeling, and safeguarding mechanisms to secure sensitive information. The assessment extends to email security, evaluating configurations to guard against phishing, spam, and malware threats. Through comprehensive vulnerability assessments, threat modeling, and incident response simulations, we aim to proactively address potential threats specific to the organization's M365 usage.

Moreover, our assessment includes an evaluation of user awareness and training programs, providing actionable recommendations and a roadmap for security improvements. The overarching goal is to ensure compliance with industry standards, foster continuous improvement, and fortify the organization's resilience against evolving cyber threats.

PROFESSIONAL SECURITY SERVICES

GOSECURE BREACH READINESS SERVICES (BRA)

[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 exercises.

GOSECURE SECURITY COMPROMISE ASSESSMENT (SCA)

[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 Extended Detection and Response (MXDR)** 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 ARTIFICIAL INTELLIGENCE GOVERNANCE ASSESSMENT (AI)

[Ensuring AI tools are responsible, safe and ethical]

GoSecure's AI Governance Assessment delivers significant business benefits by improving operational efficiency and strategic positioning. It streamlines AI policies, data management and addresses AI-related risks.

- Independent of regulation, it adapts to emerging legislation with flexibility. Ethical AI practices foster trust, credibility and stakeholder confidence, positioning the organization as a responsible AI leader, promoting innovation and attracting investors.
- This assessment ensures long-term sustainability by updating AI frameworks to align with new legislation, industry best practices and societal expectations.

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.

www.gosecure.ai

GoSecure TITAN

CONTACT INFORMATION

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

sales@gosecure.ai

www.gosecure.ai
www.gosecure.ai/managed-extended-detection-response/