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

GoSecure TITAN

GoSecure Titan®

MANAGED EXTENDED DETECTION & RESPONSE

(MXDR)

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® MXDR offers the best-in-class response time from threat detection to mitigation, delivering rapid response and active mitigation services that directly touch the customers' network and endpoints. For over 20 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk & security maturity through MXDR and Professional Services solutions delivered by one of the most trusted and skilled teams in the industry.

YOUR TRUSTED ALLY

GoSecure Titan®

MANAGED EXTENDED DETECTION & RESPONSE

[Keep Your Business Safe And Secure]

Addressing and combatting the escalating sophistication of ransomware, malware, and other threats poses a daily challenge for security teams. A swift and efficient response can determine whether an organization faces just another routine day or suffers catastrophic damage.

GoSecure Titan® MXDR is built on an open XDR infrastructure, integrating all GoSecure Managed Security Services into one powerful service & platform. It offers comprehensive protection for networks, endpoints, email, and the cloud, providing a unified view of security operations through a single pane of glass.

Unlike other all-in-one MXDR solutions, GoSecure Titan® MXDR delivers superior threat detection and response at a more affordable price, making it the smart choice for organizations seeking complete security without breaking the budget and current infrastructure investment.

GoSecure TITAN

MANAGED EXTENDED DETECTION & RESPONSE

Your ally to consolidate, evolve & thrive

[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.

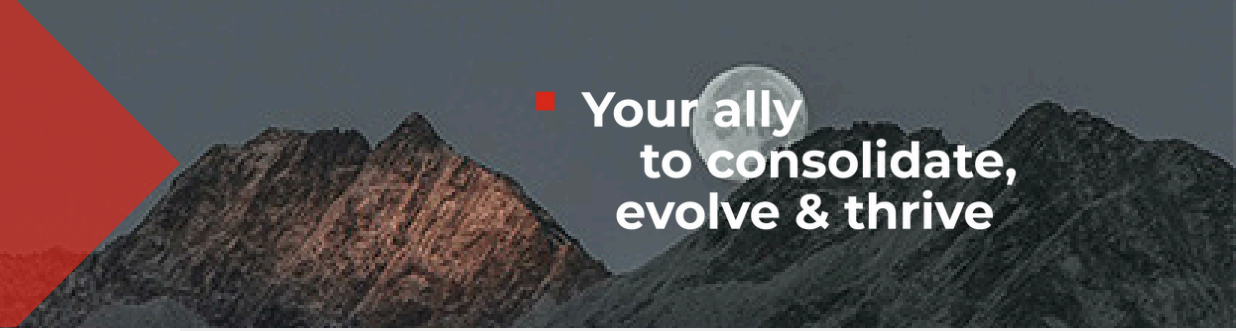
Built on an open XDR architecture, our MXDR service is designed to support existing investments by allowing choice within various elements of the configuration and to help your organization in its consolidation efforts.

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.

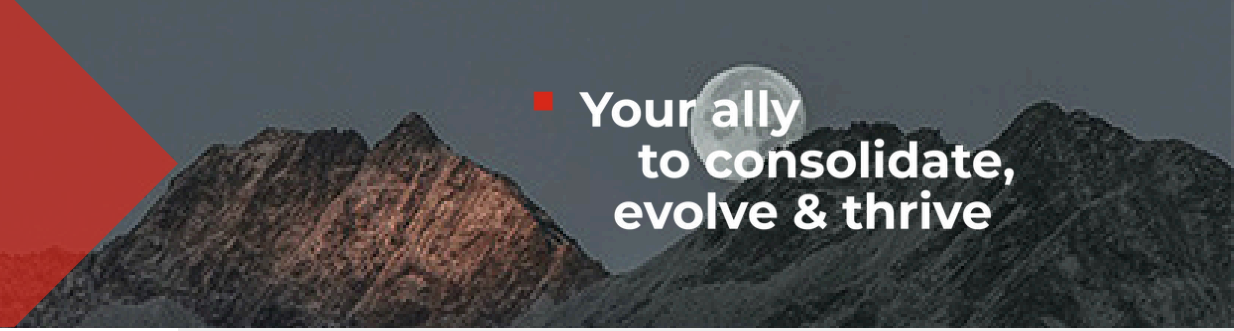
It commands more time from network security managers than virtually any other activity. And it's easy to get wrong, particularly by IT administrators doing double duty as their organizations' IT security staff.

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

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

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/