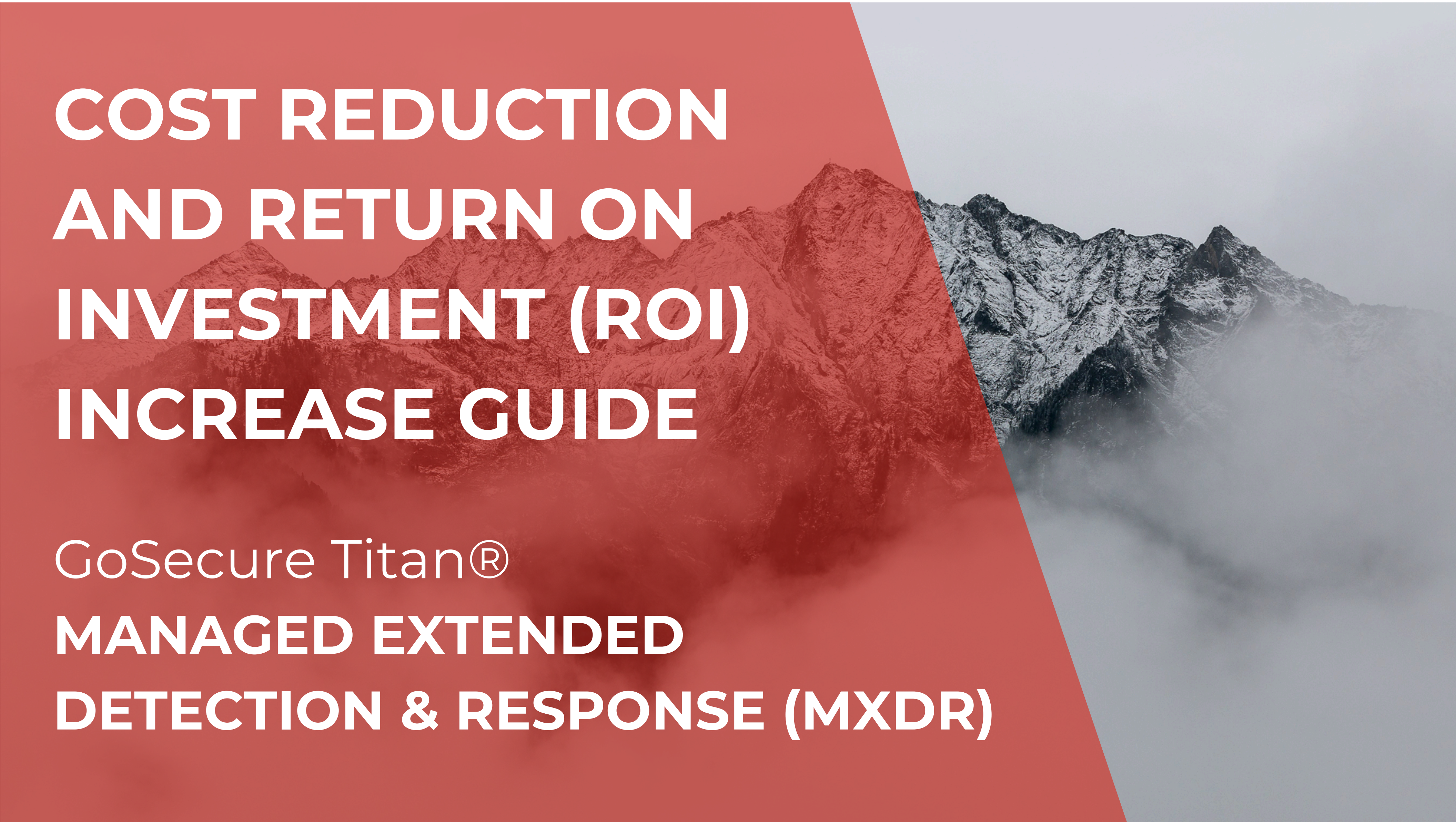
https://gosecure.ai/managed-extended-detection-response-foundation/

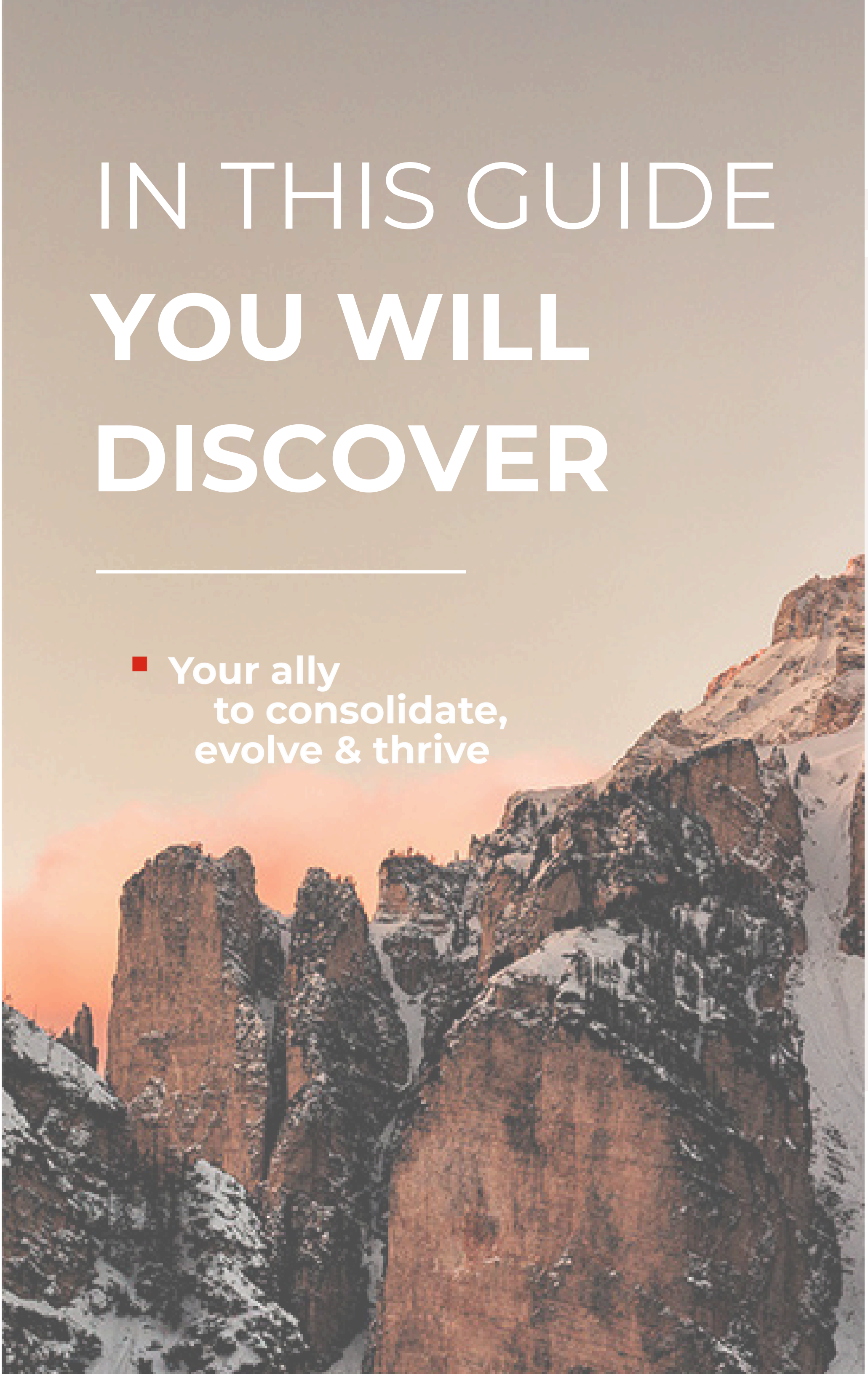


COST REDUCTION AND RETURN ON INVESTMENT (ROI) INCREASE GUIDE

GoSecure Titan®

MANAGED EXTENDED DETECTION & RESPONSE (MXDR)

GoSecure



IN THIS GUIDE **YOU WILL DISCOVER**

- Your ally to consolidate, evolve & thrive

E-MAIL@GOSECURE.AI ✉

WWW.GOSECURE.AI 🌐

CONSOLIDATION

Why?

The importance of robust cybersecurity measures cannot be overstated. As organizations strive to safeguard their sensitive data and digital assets from increasingly sophisticated threats, the question of how best to manage their cybersecurity infrastructure becomes paramount.

A recent survey by Gartner uncovered that in 2022, 75% of organizations contemplated consolidating their security vendors—a nearly 50% surge from 2020. This statistic underscores a growing recognition within the industry of the need to streamline and optimize cybersecurity strategies.

Indeed, many enterprises grapple with a plethora of security vendors, with 43% acknowledging they work with over ten providers. This proliferation of vendors not only complicates operational efficiency but also poses challenges in terms of cost management, risk assessment, and overall security posture.

In recent years, the global economic landscape has undergone significant shifts: soaring inflation, reduced spending, and escalating layoffs have prompted organizations to reevaluate their expenditure practices. The recent spate of layoffs across industries has underscored and exacerbated the prevailing skills shortage. Companies don't have enough space to keep experts for every security solution or to work closely with many different vendors.

In this guide, we will discuss the many benefits of consolidating cybersecurity solutions, address the perceived hurdles for consolidation and explore how organizations can navigate this transformative process to enhance their cybersecurity resilience and efficacy.

75%

of organizations are pursuing security vendor consolidation

43%

of organizations are working with more than 10 vendors

GOSECURE

BENEFITS

Consolidating cybersecurity solutions empowers organizations to build a more robust and resilient security posture, optimize their security investments, and adapt more effectively to evolving cyber threats. By simplifying management, reducing costs, enhancing visibility, and improving integration, consolidation enables organizations to stay ahead of the curve in an increasingly complex and challenging threat landscape.

Your ally to consolidate, evolve & thrive

✉ E-MAIL@GOSECURE.AI

🌐 WWW.GOSECURE.AI

› ENHANCED SECURITY POSTURE

In 2021, IBM released findings from its sixth annual Cyber Resilient Organization Study. The study revealed that 45% of security teams use over 20 tools to investigate and respond to a cybersecurity incident.

The complexity and fragmentation caused by employing numerous disparate tools from various vendors often hinder rather than bolster cybersecurity efforts. Each tool operates in its silo, generating its own set of alerts, metrics, and interpretations of security events.

As a result, security teams find themselves overwhelmed with data, spending precious time toggling between different platforms and attempting to reconcile conflicting information. This "tool fatigue" not only diverts attention from actual security threats but also contributes to what industry insiders refer to as the "alert overload" phenomenon. With so many alerts and notifications flooding their screens, security analysts struggle to prioritize incidents effectively, often leading to critical threats being overlooked or ignored.

Consolidating security vendors offers a solution to this issue by providing a unified platform for managing security operations. With all security data centralized and correlated in one dashboard, organizations can streamline their cybersecurity efforts, improve response times, and foster better collaboration among teams.

By simplifying complexity and reducing tool fatigue, consolidating security vendors strengthens the organization's overall security posture and enhances resilience against cyber threats.

COST REDUCTION AND IMPROVED RETURN ON INVESTMENT

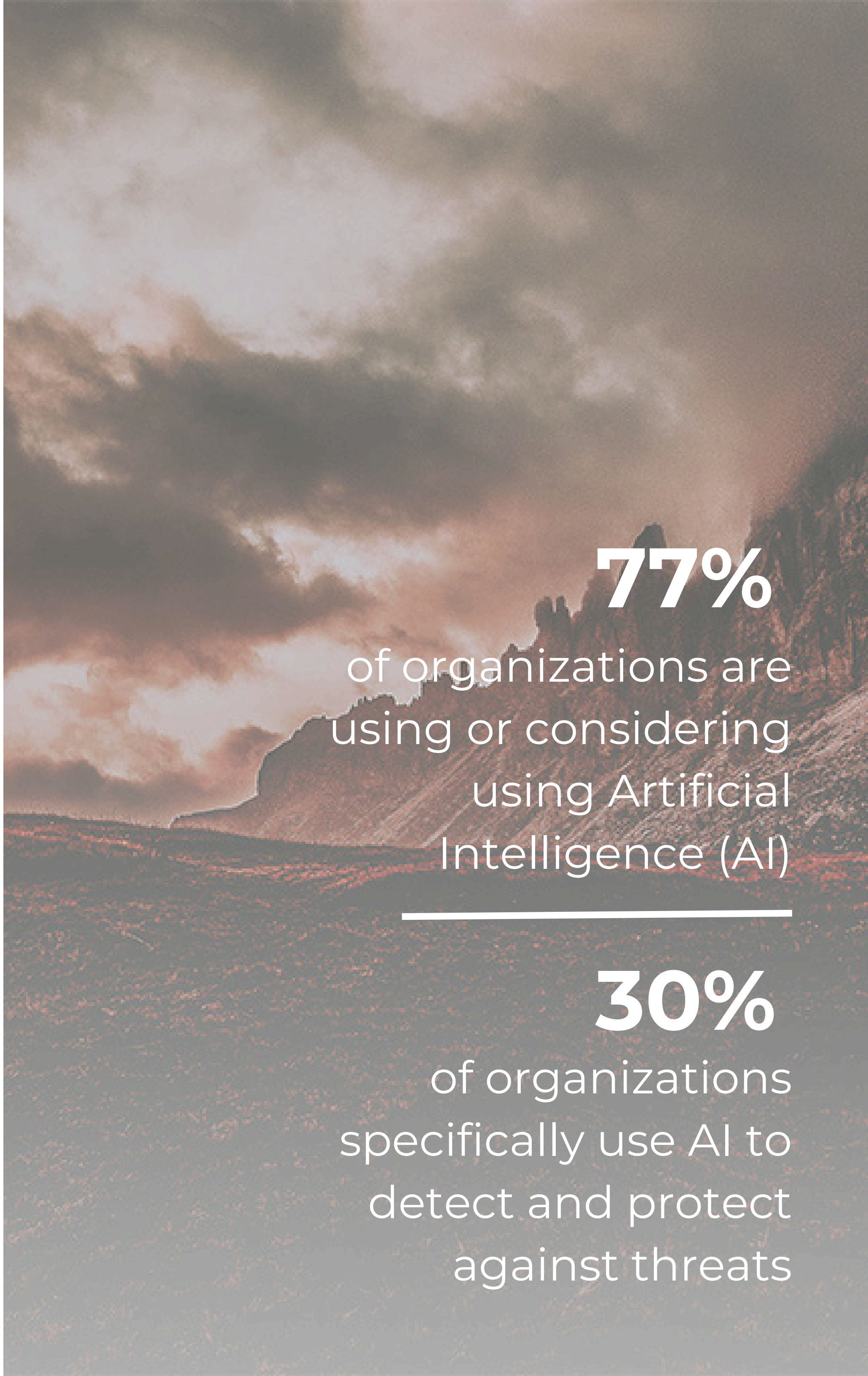
When it comes to cybersecurity, simplicity often breeds strength. Consolidating your organization's security posture isn't just about reducing complexity; it's also about maximizing returns on investment. One of the easiest ways to save on your security budget is by assessing and eliminating redundancies in your security solutions.

By reducing the number of vendors and streamlining services, organizations can often benefit from consolidation discounts from their preferred vendors. These cost savings can then be redirected to other areas within the organization, such as staff training or investments in cutting-edge security technologies.

Take IBM, for example. Their research indicates that 77% of organizations are either using or considering the use of Artificial Intelligence (AI) in their cybersecurity efforts. AI has a wide range of applications, with nearly 30% of organizations specifically leveraging it for threat detection and protection.

By consolidating security solutions and reallocating budgetary savings, organizations can afford to invest in training their IT teams in AI, machine learning, and other emerging technologies, thus enhancing their cyber defense capabilities without exposing themselves to unnecessary risks.

Moreover, consolidation can lead to significant time savings in threat detection and response. Managing multiple security tools from different vendors often requires jumping between platforms, transferring data, and sorting through false positives and redundant alerts. Consolidating these tools streamlines data management, providing access to a single platform for threat monitoring and response. This efficiency not only saves time but also increases productivity and employee satisfaction, ultimately enhancing the overall return on investment of the organization's security program.



77%

of organizations are using or considering using Artificial Intelligence (AI)

30%

of organizations specifically use AI to detect and protect against threats

INCREASING OPERATIONAL EFFICIENCY

Efficiency and productivity flourish when organizations undertake the strategic initiative of minimizing their supplier numbers. This practice liberates a significant amount of time and resources, allowing teams to redirect their focus from mundane administrative tasks to more strategic and value-driven initiatives.

By consolidating suppliers, organizations lay the foundation for fostering deeper and more meaningful relationships with their chosen vendors. These strengthened partnerships often yield tangible benefits beyond the mere transactional exchange of goods or services, including preferential pricing, access to exclusive resources, and enhanced customer support.

A streamlined supplier ecosystem provides organizations with enhanced visibility and control over their operational landscape. By reducing the complexity associated with managing multiple suppliers, organizations gain clearer insights into the performance of each solution. This heightened transparency enables proactive issue identification and resolution, minimizing the risk of system vulnerabilities and potential security breaches. Additionally, streamlined supplier relationships facilitate more efficient communication and collaboration, leading to smoother integration processes and faster response times to emerging challenges.

Consolidation simplifies compliance efforts by providing a more cohesive and unified approach to regulatory adherence. With fewer suppliers to manage, organizations can streamline their compliance processes, ensuring that they meet the necessary industry standards and regulatory requirements. This proactive stance not only reduces the risk of non-compliance penalties but also enhances the organization's reputation and credibility within the industry.

The strategic consolidation of suppliers offers numerous benefits that extend far beyond operational efficiency. By fostering stronger relationships, enhancing visibility and control, and simplifying compliance efforts, organizations position themselves for long-term success and growth in an increasingly competitive business landscape.

> [“We had the choice of hiring one or two others (internally) and ensuring that we could keep their skills up to date – and making sure we kept them with us. Or we could build a partnership with a managed security services provider like GoSecure. We chose to try this side, to have access to experienced cybersecurity professionals and to make sure that we would be supported 24/7/365 for emergencies.”]
>
> **Frederick Pouliot**
> Senior IT Director, Agri-Marché

PERCEIVED CHALLENGES

GoSecure TITAN

While the benefits of consolidation are apparent, some organizations may still view perceived drawbacks as reason enough to steer clear. However, many objections to consolidation are based on misunderstandings or a lack of context, and two major concerns are often voiced.

- **Your ally to consolidate, evolve & thrive**

E-MAIL@GOSECURE.AI

WWW.GOSECURE.AI

FOMO ON "BEST-OF-BREED" SOLUTIONS

One common hesitation towards cybersecurity consolidation stems from the fear of missing out on the supposed "best-of-breed" solutions. Organizations often spend considerable time researching and evaluating various products for each specific security need, hoping to find the perfect fit. However, they may discover that while one provider excels in one aspect, it falls short in others. This dilemma can create doubts about the compatibility of consolidation with quality.

Nevertheless, a growing number of professionals now assert that the advantages of consolidation far outweigh those of the "best-of-breed" approach. Recent findings from a Gartner survey reveal that **41% of respondents identified enhancing their organization's risk posture as the primary benefit of consolidating security solutions**. This underscores the significant improvements in security, operational efficiency, and end-to-end visibility that consolidation offers.

Contrary to the belief that individual solutions are superior, experts argue that the cumulative effect of a consolidated approach ensures much more effective security. Rather than relying on disjointed solutions, which may excel in isolation but struggle to integrate seamlessly, a consolidated strategy provides a cohesive framework that addresses security challenges comprehensively. In essence, it's not about having the best individual tools but rather about integrating them into a unified and synergistic security ecosystem.

FEAR OF GETTING STUCK WITH A PROVIDER

One of the key concerns that arise with consolidation is the fear of being locked into a single provider. Many organizations hesitate to consolidate their technology stack, fearing that the chosen provider may fall short or fail to deliver on its promises. This apprehension stems from the potential scenario of being stuck with a subpar solution until the end of the contract or subscription period.

To alleviate concerns about consolidation with mediocre quality providers, it's essential to conduct thorough evaluations of potential partners. Assessing different providers ensures that each candidate can meet your product requirements, mitigate security vulnerabilities, and keep pace with industry innovations. Here are some critical questions to consider when evaluating potential providers:

- **Security Approach:** Understand how the provider approaches security. Inquire about their reliance on third-party vendors for security management and whether any of your data will reside on their systems. Additionally, seek insights into how they have responded to security threats in the past to gauge their efficacy in safeguarding your organization's assets.
- **Cost Considerations:** Clarify all costs associated with the provider's services. Often, initial pricing may not include maintenance, additional subscription fees, license additions, or other necessary modules. By comprehensively understanding potential costs, you can ensure budget adherence and avoid surprises from hidden fees.
- **Integration Compatibility:** Evaluate how well the provider's tools integrate with your organization's existing systems. While the features of a solution may be impressive, seamless integration with your infrastructure is crucial. Opting for a provider whose tools align seamlessly with your systems minimizes the need for customization and reduces implementation challenges.
- **Transition Flexibility:** Anticipate future needs and consider the ease of integration or transition to alternative providers. As organizational requirements evolve, the ability to switch providers smoothly becomes paramount. By asking pertinent questions about onboarding and offboarding processes upfront, you can ensure seamless transitions in the future.

Once these hurdles are overcome, organizations can confidently embark on their consolidation journey, bolstering their security posture and operational efficiency.

GoSecure

INITIAL STEPS

Navigating the labyrinth of your current cybersecurity infrastructure and vendors might appear overwhelming initially.

However, fear not! We're here to lead you through the consolidation journey with confidence. As you embark on this endeavor, it's imperative to grasp a thorough understanding of all your available tools and solutions while gathering insights about the involved vendors.

Much like you require a clear view of your system to make informed security choices, thoroughly inspecting your existing technology stack is crucial to pinpoint areas ripe for consolidation. This introspective analysis lays the foundation for a successful consolidation strategy, empowering you to optimize your cybersecurity infrastructure effectively.

✉ E-MAIL@GOSECURE.AI

🌐 WWW.GOSECURE.AI

› AVOIDING LAYERED CONSOLIDATION

Once you've inventoried your existing resources, the next step is devising a smart strategy for consolidation. Our recommendation? Focus on consolidating functions rather than layers. Here's why: your infrastructure likely incorporates various security layers, each serving as a safety net to identify vulnerabilities—a tactic commonly known as "defense in depth." For instance, you might have one solution dedicated to endpoint monitoring and another to manage threats across your entire ecosystem.

But why avoid consolidating different layers? Doing so could inadvertently weaken your security stance by removing valuable redundancies within your system. The principle of secure design relies on redundancy to mitigate the risk of a "single point of failure."

In the intricate hybrid infrastructure landscape of today, adopting a defense-in-depth approach isn't just prudent—it's imperative.

CONSOLIDATION OF FUNCTIONS

Function consolidation emerges as a cornerstone strategy for organizational resilience. By focusing efforts on vital areas such as cloud security, vulnerability management, and application security, organizations can bolster their defenses and streamline their operations. This consolidation not only enhances visibility and risk management but also fosters a cohesive approach to cybersecurity.

Examining specific layers of cybersecurity more closely unveils further opportunities for optimization. By identifying functions ripe for consolidation, such as detection and response or integrating threat intelligence and vulnerability management, organizations can refine their security posture. In essence, function consolidation empowers organizations to navigate continuously evolving threat conditions with agility and resilience, ensuring they remain one step ahead of potential risks while streamlining their cybersecurity efforts.

FINDING THE RIGHT TOOLS

Once you've identified the best functions to consolidate or how you want to approach function consolidation across different layers, you need to determine the most suitable offerings and tools for your organization.

If securing your cloud migration is a priority, here are some critical features to look for in consolidation offerings and solutions:

Risk Prioritization

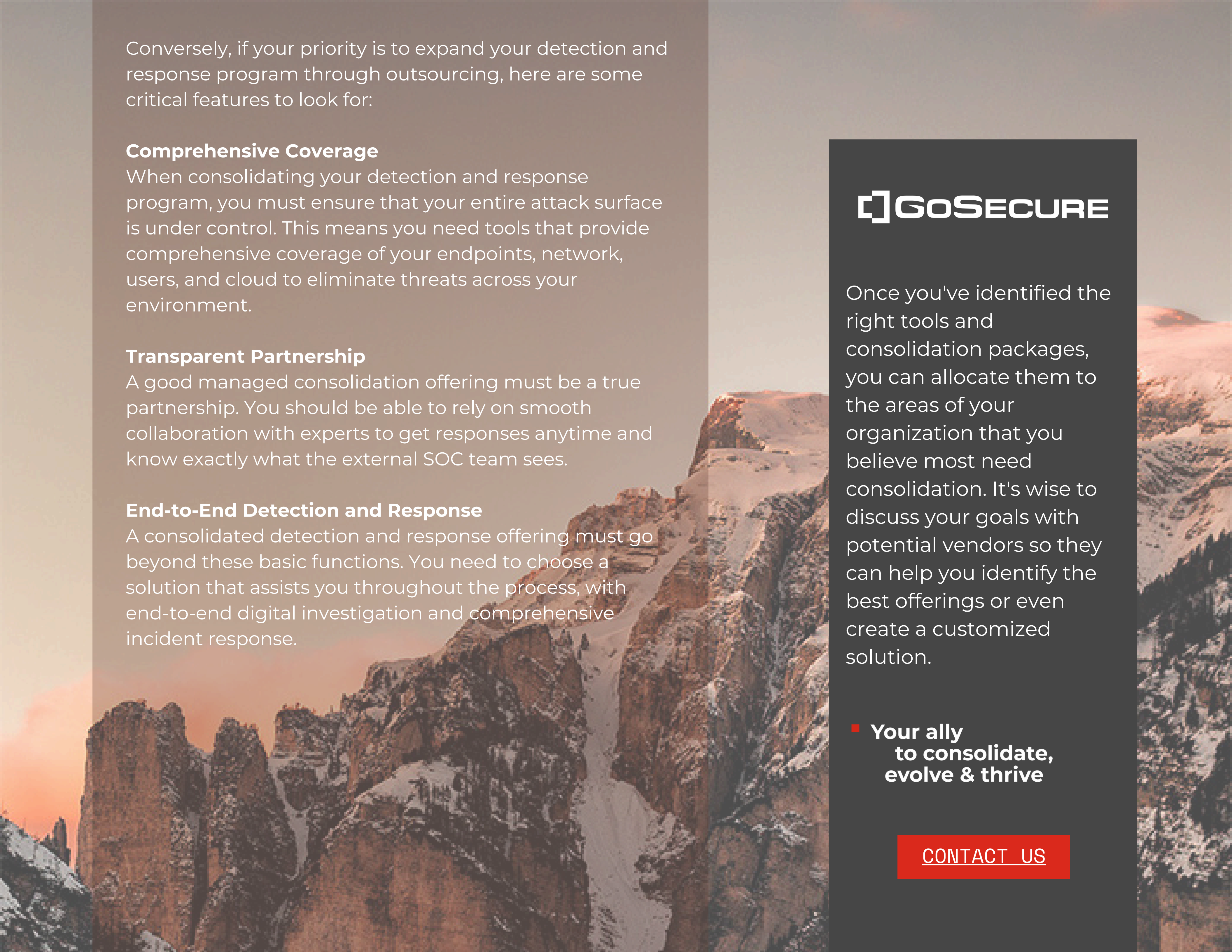
Consolidation can avoid the confusion caused by multiple data streams from different solutions, but you also need to find a tool that provides the necessary context to classify risk signals across your ecosystem. This includes solutions that enable your team to determine which unwanted ports are open on your public assets.

Compliance Automation

Your consolidated solution should help you comply with internal and external regulations by detecting and remedying gaps. Tools that monitor and enforce industry-specific regulations while working seamlessly with your workflows to ensure continuous compliance are preferred.

Security Scanning

Security threats are constantly evolving, which is why continuous scanning and testing of your infrastructure's applications are essential to your security strategy. An ideal consolidation offering should provide your organization with real-time security assessments, detailed reports for better team collaboration, and valuable insights into evolving risks. The best tools will also ensure your team is aware of the four main types of risks in your system: known risks, known unknown risks, unknown known risks, and unknown unknown risks.



Conversely, if your priority is to expand your detection and response program through outsourcing, here are some critical features to look for:

Comprehensive Coverage
When consolidating your detection and response program, you must ensure that your entire attack surface is under control. This means you need tools that provide comprehensive coverage of your endpoints, network, users, and cloud to eliminate threats across your environment.

Transparent Partnership
A good managed consolidation offering must be a true partnership. You should be able to rely on smooth collaboration with experts to get responses anytime and know exactly what the external SOC team sees.

End-to-End Detection and Response
A consolidated detection and response offering must go beyond these basic functions. You need to choose a solution that assists you throughout the process, with end-to-end digital investigation and comprehensive incident response.

GoSecure

Once you've identified the right tools and consolidation packages, you can allocate them to the areas of your organization that you believe most need consolidation. It's wise to discuss your goals with potential vendors so they can help you identify the best offerings or even create a customized solution.

**Your ally
to consolidate,
evolve & thrive**

CONTACT US

GOSECURE

GOSECURE TITAN® MXDR

YOUR ULTIMATE ALLY IN YOUR CONSOLIDATION

35%

Organizations choosing GoSecure Titan® MXDR can achieve cost savings of up to 35%.

FROM 100% TO 300%

Organizations can achieve a positive ROI within the first year of implementing an open XDR solution.

60%

Reduction in security incidents by up to 60% following the implementation of GoSecure Titan® MXDR

Your ally to consolidate, evolve & thrive

✉ E-MAIL@GOSECURE.AI

🌐 WWW.GOSECURE.AI

GOSECURE TITAN® MXDR SEAMLESSLY INTEGRATE WITH EXISTING SECURITY TOOLS, OFFERING CENTRALIZED MANAGEMENT WITHOUT THE NEED FOR REPLACEMENTS.

By leveraging our open XDR technology, GoSecure Titan® MXDR delivers unmatched visibility, detection, and response capabilities, enabling organizations to effectively address evolving cyber threats. With a single pane of glass and a highly flexible ecosystem, you can incorporate your current technology, allowing for seamless ingestion and management.

BENEFITS OF GOSECURE TITAN® MXDR'S OPEN XDR

- ENHANCED THREAT VISIBILITY
- IMPROVED INCIDENT RESPONSE
- COST EFFICIENCY
- EMPLOYEE PRODUCTIVITY
- FLEXIBILITY AND ADAPTABILITY

GOSECURE TITAN® MANAGED EXTENDED DETECTION & RESPONSE (MXDR)

A FOUNDATION YOU CAN TRUST AND BUILD UPON

GoSecure Titan® MXDR, powered by our open XDR technology, is a comprehensive cybersecurity solution that addresses organizations' challenges and needs effectively.

With its advanced threat detection, automated response actions, cost-efficient solutions, and productivity enhancements, GoSecure Titan® MXDR empowers organizations to strengthen their security posture, mitigate risks, and protect against growing digital threats.

LEARN MORE

YOUR ULTIMATE ALLY

Choose GoSecure as your ultimate ally with a proven record of expertise, research excellence, and a commitment to addressing the transforming challenges of endpoint threats. Our notoriety in the cybersecurity world is a testament to our dedication to providing innovative, effective solutions that safeguard organizations in an increasingly complex digital environment.

GET SECURE

CONTACT INFORMATION

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

✉ sales@gosecure.net

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