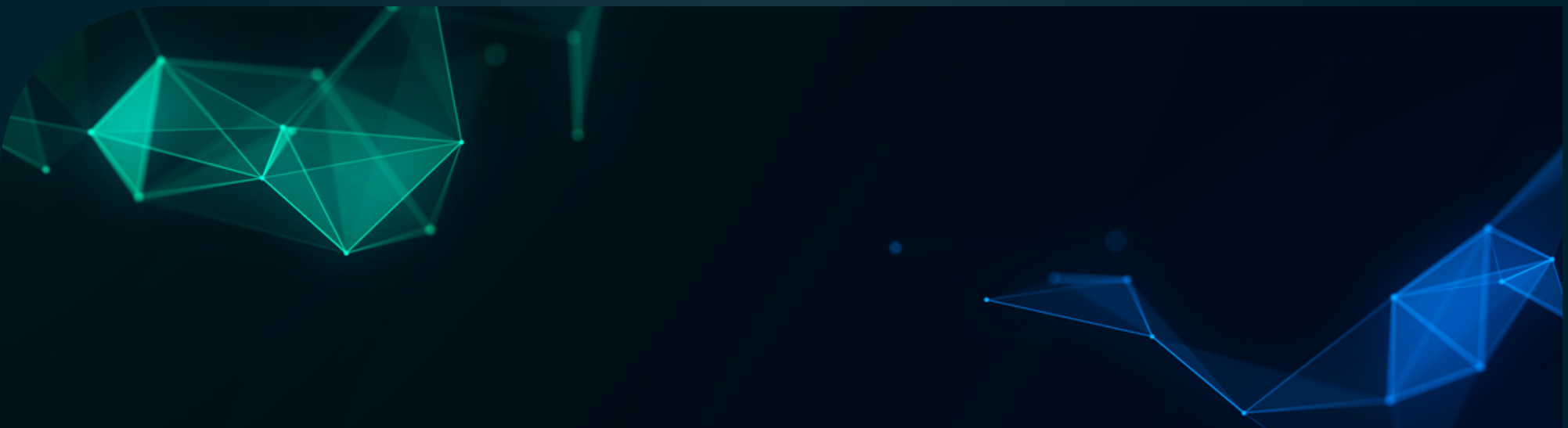
MAVERC

Security Without Boundaries

Capabilities designed to protect
Small Businesses from Cyberattacks



Our understanding of technology as it relates to time, cost, and performance allows us to quickly navigate through the nuances and challenges of organizations to provide bespoke solution and ensures we deliver on all projects and programs.

MAVERC

Maverc.com

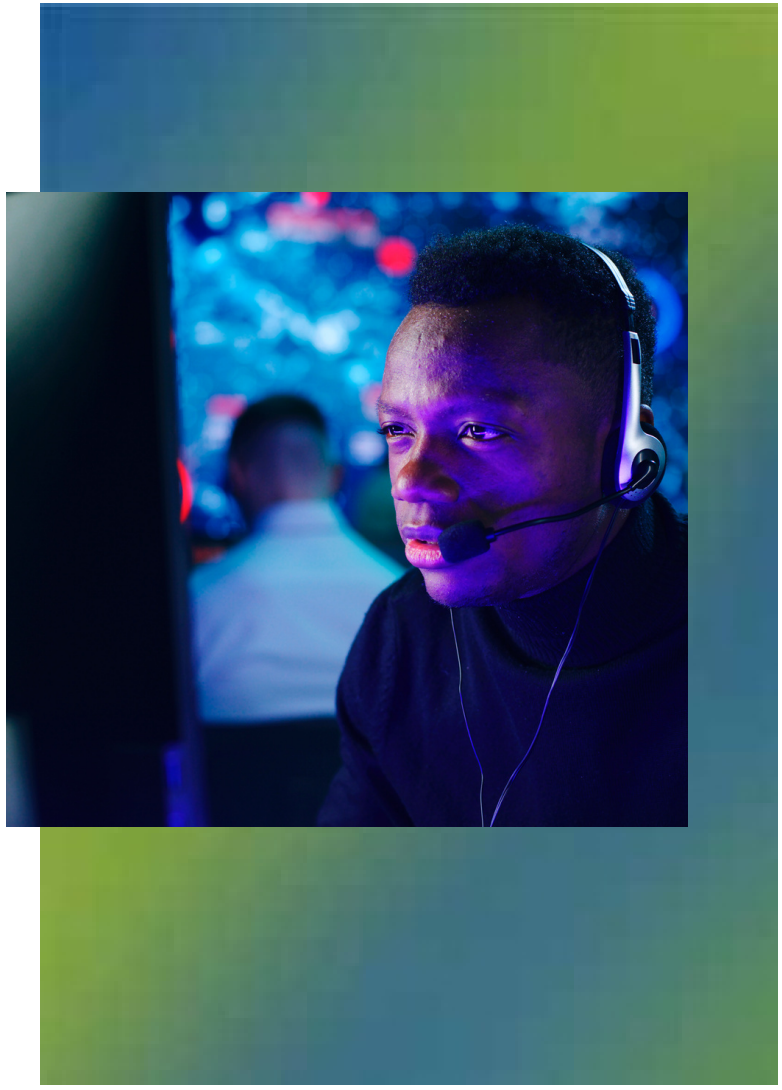
Introduction

Cybersecurity was traditionally seen as a concern for large enterprises, which possess vast technology, substantial finances, and sensitive data, necessitating the protection of their reputations. As such, hackers primarily focused on significant targets like retail giants, healthcare establishments, and financial institutions. Breaches in these areas gained considerable media attention.

However, the landscape has shifted considerably.

Now, businesses of every size heavily depend on technology, facing sophisticated cyber threats. This change has put small and mid-market companies in a vulnerable position, leading to a problematic scenario:

- Small businesses, though reliant on technology, often lack IT management skills and cybersecurity knowledge, making them easy targets for cybercriminals, especially with limited budgets to hire and maintain skilled security personnel.
- Mid-market organizations might have some IT staff and a basic understanding of security. However, even with more maturity than smaller businesses, they struggle with the complexities of integrating various software and human resources necessary to counteract persistent cyber threats.
- To address these issues, both small and mid-sized enterprises frequently collaborate with external service proveiders or value-added resellers. These partnerships aim to bridge gaps and enhance their defensive capabilities against cyber threats.



- These third-party capabilities are flexible, capable of scaling to meet varying needs while mitigating the initial cost barriers. They also transfer the responsibility of talent management and expertise to the service provider, addressing workforce and knowledge limitations. Crucially, though often overlooked, these capabilities must cover a broad range of security requirements that encompass the entire lifecycle of a cyber attack. For effective defense, a business needs to identify potential vulnerabilities in their infrastructure, detect attempted and successful infiltrations, assess the extent of any damage, ensure the removal of threats, and safely restore systems to their pre-attack state. This is a complex and multifaceted task.

- However, there's a significant challenge: these third-party providers **themselves** struggle to keep up with evolving threats. They often depend on a plethora of disjointed tools and services that may be inefficient, provide incomplete information, or leave vulnerabilities that attackers can exploit. Additionally, these providers face similar issues with staffing and skills shortages due to the high demand and low availability of skilled cybersecurity professionals. This raises a critical question: who ensures that these service providers and resellers are equipped to fulfill the promises made to their clients?

Solution: Maverc XDR Platform

ThreatHunting

Managed EDR

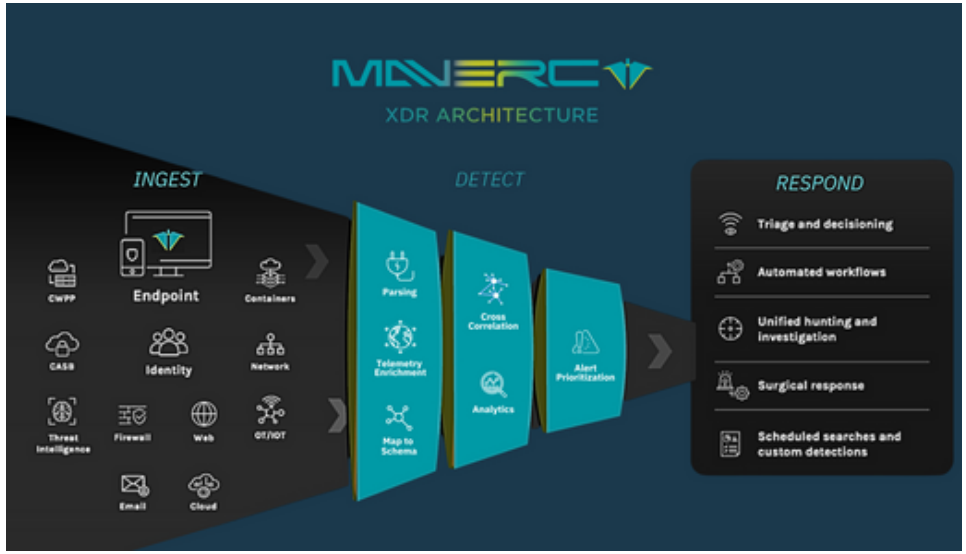
Threat Intelligence

Vulnerability Management

Incident Response

Attack Surface Management

Maverc brings together advanced software and expert knowledge to enhance the cybersecurity of small and mid-market businesses. We offer high-quality security solutions at an affordable price, focusing precisely on the needs of these businesses. Additionally, we provide our services through existing third-party partners, ensuring minimal disruption for these companies. Our comprehensive range of security services is not only user-friendly but also backed by our dedication to educating and empowering the community. This approach positions Maverc as a distinct and valuable ally in combating cyber threats.



MAVERC

Maverc.com

XDR/MDR The Maverc Way: Cyber Security Without Boundaries

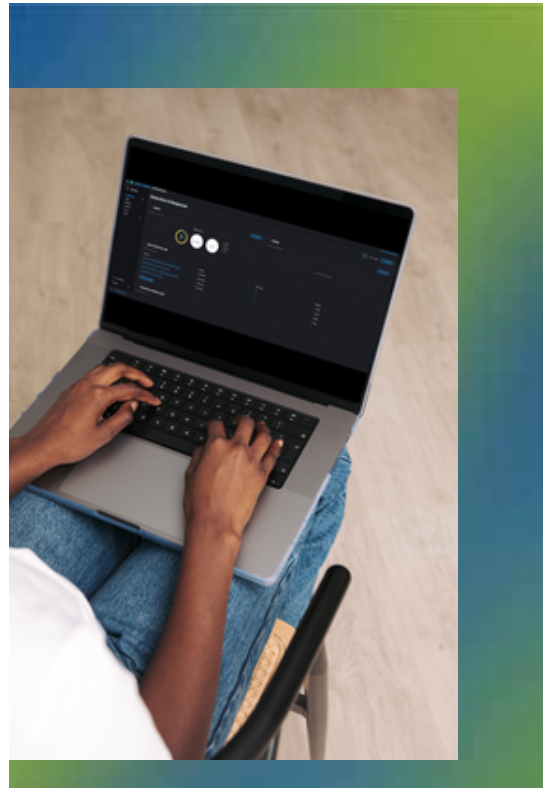
What does it mean to have a managed XDR platform, and what distinguishes Maverc in this area? As the significance of cybersecurity has escalated, its management has become more complex. This issue is particularly present for small and mid-market organizations, which often find themselves constrained by limited knowledge, budget, and resources to counteract sophisticated cyber threats.

In their cybersecurity efforts, many businesses, whether handling IT internally or via third-party providers, rely on an assortment of isolated tools and solutions. These tools are designed for specific functions but often lack cohesion, leading to a cumbersome and inefficient management experience.

In response, businesses may gravitate towards IT or security platforms that propose a unified solution, combining technology, services, training, and enablement. However, these platforms can introduce new challenges: they may be complicated to manage, generate too many alerts, offer inconsistent performance across different features, and be costly.

Maverc's Managed XDR Platform is specifically crafted for the needs of small and mid-market businesses (SMBs). Our approach simplifies security, allowing businesses to concentrate on critical issues and enabling individuals without deep security expertise to effectively respond to cyber threats, all at a price suitable for our target markets.

The "managed" part of Maverc means that we do most of the heavy lifting. This approach ensures our platform is accessible to non-cybersecurity professionals, reducing stress and making security a reliable and less burdensome aspect of business operations.



We deliver large enterprise cybersecurity capabilities to the Organizations that need it the most- SMBs

MAVERC

Maverc.com

Our distinguishing features

Threat Hunting

Modern businesses require comprehensive security measures that cover every phase of the attack lifecycle. To meet this need, Maverc offers a robust set of managed services for endpoint protection, detection, and response. These services are supported around the clock by a dedicated team of threat analysts. This approach ensures effective defense against various cybersecurity threats, including ransomware and malicious intrusions.

The Threat Response Team forms the core of the Maverc platform, serving as a crucial ally in combating cyber threats. Comprising of always highly trained and certified experts, this team handles the intensive work of continuous threat monitoring. They provide world-class support and detailed guidance for identifying sophisticated cyber-attacks, ensuring defense around the clock.

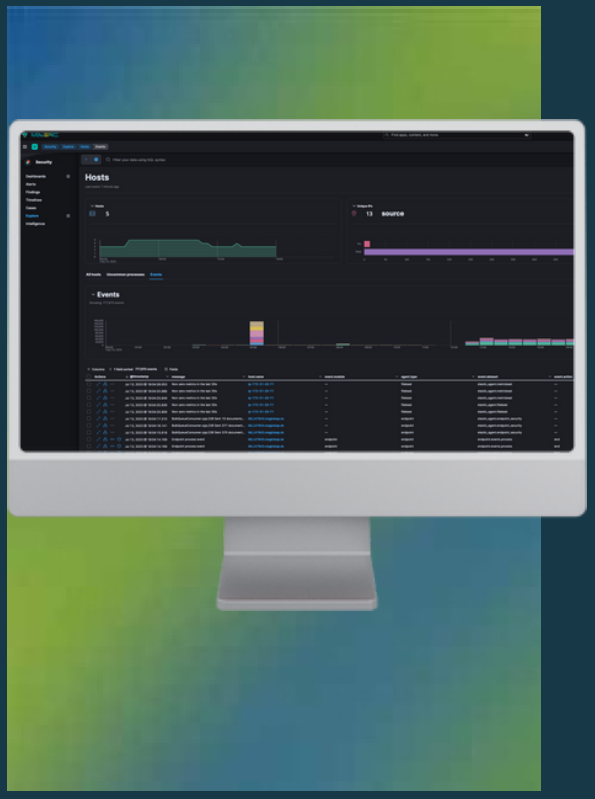
Key Benefits :

- Access to a team of highly skilled professionals with deep knowledge of hacker methodologies.
- Continuous monitoring and investigation of potential security threats, along with the elimination of false alarms and the generation of tailor-made incident reports for effective response to confirmed threats.
- Constant examination of hacker techniques and emerging threats, enhancing our proficiency and ensuring you stay at the forefront of cybersecurity.

MAVERC

LEARN MORE

Our distinguishing features



Find the Needle in The Haystack

Security tools often produce a high volume of activity. They continuously scan and monitor, trying to differentiate between harmless and harmful activities. This often results in numerous alerts and tickets, many of which are false alarms or irrelevant. Consequently, businesses need dedicated staff to oversee these systems, sorting through the clutter to identify the truly critical issues. This approach may work for larger enterprises, but it's less feasible for small and medium-sized businesses (SMBs).

Maverc simplifies this process.

Our Threat Response Team meticulously examines all suspicious activities and detections and ensures that our partners only get notified about genuinely important matters. We provide clear prioritization of alerts, differentiating between low and high-priority ones. Our system facilitates the implementation of recommended automated actions and provides straightforward guidance for any necessary manual interventions.

Threat Hunting Operations Workflow

Identify

Maverc deployed agents searches all the locations commonly exploited by hackers for concealment, targeting malicious actors who misuse legitimate applications, evade other security measures, or are in the midst of deploying harmful payloads such as malware and ransomware.

Analyze

Our approach transcends automated detection by incorporating context-sensitive manual analysis conducted by our T.R.T. team. Our security analysts examine endpoint and agent surveys to identify and capture elusive hacker strategies, ensuring even the most covert threats are detected.

Report

Our approach transcends automated detection by incorporating context-sensitive manual analysis conducted by our T.R.T. team. Our security analysts examine endpoint and agent surveys to identify and capture elusive hacker strategies, ensuring even the most covert threats are detected.

Remediate

Our detailed incident reports are designed to help our partners respond swiftly,
and many of the remediation steps we outline can be automated and executed
in a single click. Plus, we'll provide detailed recommendations for any other work
that should be completed and can step in to help isolate ongoing attacks and
minimize damage.

Our distinguishing features

Endpoint Detection and Response

The key to identifying sophisticated threats lies in having clear visibility. Maverc's Managed EDR (Endpoint Detection and Response) facilitates faster detection and removal of hackers through almost instantaneous endpoint monitoring. By keeping an eye on malicious processes and integrating data from other Maverc services, Managed EDR offers exceptional insight, allowing for the prompt identification and elimination of cyber threats as they emerge.

Key Benefits :

- Persistent observation of process executions and their related metadata enhances visibility, making it increasingly difficult for hackers to conceal their activities.
- Ability to identify attacks right at their origin and track threat actor behaviors from the point of initial access to the intended impact.
- In case of a security incident, Maverc's Threat analysts are equipped to perform near real-time forensic analysis and actively search for threats within your network.

LEARN MORE

MAVERC

Our distinguishing features

Attack Surface & Vulnerability Management

The key to staying resilient from a cyber attack is taking action before an attacker can. Our Threat Response Team meticulously scans and identifies vulnerabilities across your entire digital footprint, including often-overlooked areas like shadow IT, OT, and cloud services. By offering real-time insights and analytics, Maverc empowers you to understand and reduce your attack surface before cybercriminals can exploit it. With intuitive interfaces and seamless integration into your existing security infrastructure, Maverc's Attack Surface Management technology becomes a strategic asset in your cybersecurity arsenal. Make the smart choice for your security with Maverc, and transform your cyber resilience from reactive to proactive.

Key Benefits :

- Enhanced Visibility and Control: ASM provides a comprehensive view of an organization's entire digital footprint, including on-premises, cloud, and remote assets. This enhanced visibility helps in identifying and managing all potential entry points for cyber attackers, thereby reducing blind spots and increasing control over the organization's security posture.

- Proactive Threat Identification and Mitigation: By continuously monitoring and analyzing the attack surface, allowing organizations to proactively identify vulnerabilities and potential threats. This enables timely remediation of security gaps, such as unpatched software, misconfigurations, or exposed sensitive data, before they can be exploited by attackers.

- Improved Compliance and Risk Management: Maverc aids in maintaining compliance with various industry standards and regulations by ensuring that all parts of the IT environment are secure and vulnerabilities are addressed. This proactive approach to identifying and mitigating risks significantly contributes to an overall robust risk management strategy, helping to protect against data breaches and other security incidents.

MAVERC

LEARN MORE

Our distinguishing features

Ransomware Protection

In the fight against ransomware, time is of the essence to prevent its spread. Our Ransomware protection functions by providing early warning signals for potential ransomware incidents. Should an indicator be triggered, our dedicated Threat Response team promptly verifies the threat. Once confirmed, they work diligently with you to contain and prevent the further spread of the infection, ensuring swift and effective response to these critical cybersecurity threats.

Key Benefits :

- Swift detection and elimination of ransomware, minimizing risk and ensuring maximum system uptime.
- Accurate identification of compromised endpoints in a ransomware attack, allowing for a better evaluation of the attack's extent and facilitating appropriate responses.
- Enhanced capability to promptly and effectively tackle potential ransomware threats, leading to quicker resolution and removal of ransomware.

LEARN MORE

MAVERC

Other Valuable Tools

Console Enabled Host Isolation

This feature enables rapid blocking of both incoming and outgoing network traffic on compromised hosts, greatly diminishing the likelihood of a widespread cyberattack across the network. Isolation, which can be activated either manually or automatically, severs the host's connection from the organization’s network while maintaining a link solely between Maverc and the isolated host. Once isolation is in effect, the Threat and Response team steps in to offer guided remediation measures to address the incident and restore the affected host(s) to normal operation.

Automated Response Workflows

This feature equips our customers with a powerful tool to counteract hacker activities instantly. Automated response workflows enhance our incident reporting by offering customers the convenience of executing remediation steps recommended by Maverc through a single click, whenever automation is possible. This capability enables customers to react more swiftly to incidents, particularly in scenarios involving unfamiliar threats, ensuring a rapid and efficient response.

Custom Reporting and Metrics

In cybersecurity, there's an inherent paradox: the more effectively you defend your clients, the less visible the benefits of your services become to them. To address this, Maverc provides customizable threat reports that illuminate all the unseen, behind-the-scenes work being done. These comprehensive summaries and reports enable customers to not only accurately assess but also effectively communicate the value they derive from Maverc's services. These reports are delivered Weekly, Monthy, and Quarterly enabling you to make informed decisions related to your security posture

Committed to Solving the Toughest Cyber Security Challenges

Maverc's mission is driven by a fundamental principle that "Cyber Security has everything to do with everything we do". dedication to the wider cybersecurity community plays a significant role in our team's goal of providing affordable solutions to SMBs. This involves extending our efforts beyond just our infrastructure, and actively responding to incidents and developments within the industry as they occur. We collaborate and form partnerships with others committed to enhancing the cybersecurity landscape. Additionally, we offer comprehensive cybersecurity training and education, catering to enthusiasts across all levels of expertise. Our motivation is inspired by a commitment to defending critical industries and infrastructure and to support and strengthen the capabilities of present and future cyber defenders.

> Everyone is linked to cyber in some manner, be it through daily activities like commuting via the subway, or through essential services like the electric grid that powers our homes and keeps them functional. Cyber Security has everything to do with everything to do

Resource Library

Blog & Newsletter

If you're seeking educational materials, our blog is an excellent starting point. Particularly, our cybersecurity education section hosts a diverse collection of **blog** posts addressing various aspects of cybersecurity. For those interested in understanding active incidents in more depth, our threat analysis category offers insightful content. Additionally, business owners will find valuable resources in our business growth category, which focuses on strategies for selling cybersecurity services and expanding your business.

Ebooks & Educational Materials

If you're seeking educational materials, our blog is an excellent starting point. Particularly, our cybersecurity education section hosts a diverse collection of blog posts addressing various aspects of cybersecurity. For those interested in understanding active incidents in more depth, our threat analysis category offers insightful content. Additionally, business owners will find valuable resources in our business growth category, which focuses on strategies for selling cybersecurity services and expanding your business.

TableTops and Live Webinars

Our range of **webinars and live events** offer insights on everything from peer-recommended best practices to effective responses during active cyber incidents. These sessions provide valuable guidance on preparing your business and team for current and emerging threats, including strategies for developing a comprehensive incident response plan or business continuity plan.

Customer Portal

Manage your cybersecurity service seamlessly with the Maverc Customer Portal, an online tailored for Maverc users. This portal simplifies your interaction with Maverc's cutting-edge security solutions, offering an intuitive interface for monitoring and managing your cybersecurity infrastructure. Enjoy direct access to technical support, detailed incident reports, and real-time updates on your security status. With features like customized dashboards, easy access to new updates, and a wealth of educational resources

Why Us?

- Exceptional Customer Support: While the Maverc solution is user-friendly and straightforward, our team remains dedicated to offering exceptional support and hands-on assistance whenever required. Beyond our comprehensive support documentation, we actively collaborate with partners to thoroughly investigate specific incidents and reports. We also provide tailored security advice, recommendations, and more, ensuring you have the support you need to navigate any cybersecurity challenge.

- Transparent and Fair Pricing: Our pricing structure is straightforward and gimmick-free, grounded in two fundamental principles: offering a top-tier cybersecurity solutions at a cost accessible to SMBs, and implementing a tiered licensing system. This approach allows our partners to achieve suitable margins by adding extra services and value in their efforts to secure their customers, ensuring clarity and fairness in our pricing model.

- Innovation Focused: Our customers are the central focus of our product and service strategy. The features we develop and the methods we employ to create them are tailored to meet the challenges and needs our customers encounter as cyber threats evolve. We engage in ongoing dialogue, gather feedback, conduct rapid prototyping tests, and more, to ensure our solutions are staying ahead of the curve.

Customers

Solutions Partners

MAVERC

Committed to Forging the Future of Cyber Security

Swiftly Detect, Effectively Respond, and Confidently Recover from cyber attacks.

maverc.com

Info@Maverc.com
(888) 948-1468

NAICS CODES

541511
541512
541513
541519
541611
541618
541620
541690
611420
511210
518210
541430
541720