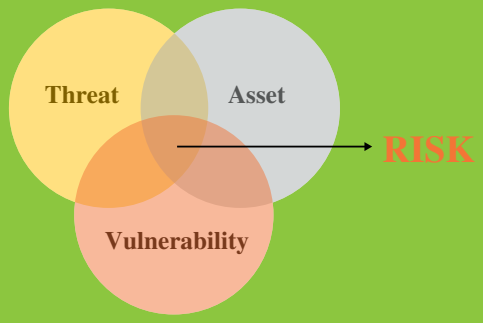
Unlock External Exposure Management with Ridge Security

How to Grow MSSP and MDR Adjacent Service Offerings

Traditional vulnerability management approaches can no longer keep up with today's dynamically changing business needs. Attack surfaces are vastly expanding across multiple clouds, on-premise locations, remote workers, mobile users and IoT. Cyber attackers employ increasingly sophisticated tools and methods to breach assets. Conventional security practices that focus on internally defending assets are inadequate; additionally viewing assets from the outside—as an attacker does—is essential to achieve comprehensive security protection.



Managed Security Service Providers (MSSP) and Managed Detection and Response (MDR) providers are building out adjacent service capabilities to help customers manage this increasingly complex and distributed landscape. Ridge Security's MSSP program is designed to help you achieve these business benefits with award-winning tools, targeted exposure management capabilities and easy API integration.

MSSPs and MDRs On the Rise in Security Operations (SOC)

This burgeoning complexity—accompanied by a dearth of skilled security industry professionals, as well as a field of cybersecurity tools that have grown intricate and fragmented—compel many customers' SOC teams to seek relief from service providers to strengthen their security protection with both offensive and defensive strategies. By outsourcing to MSSPs and MDRs, security teams can gain up-to-date protection for all endpoints, applications, networks, and clouds without enlarging their in-house team.

MSSPs can address these security gaps for large and small organizations alike, while at the same time lowering costs and streamlining processes. A fast-growing, competitive segment of this market is MDR providers who maintain their own multi-function technology stacks, along with other integrated security capabilities, all delivered as cloud services.

Gartner projects that by 2025 50% of organizations will use MDR services for their threat detection and response operations. Successful MSSP and MDR offerings fully integrate the appropriate offensive and responsive protections to meet customer needs.

What is External Exposure Management

360-degree protection of expanding attack surfaces requires exposure management—in addition to detection and response—to discover and validate asset vulnerabilities before bad actors find them. The concept is to detect security risks from an outside-in perspective. Organizations often have neither comprehensive visibility into their internet-connected assets, nor a thorough assessment of the connectivity paths between those assets that allow for lateral movement after a breach.

Modern organizations contain numerous attack surfaces in need of External Exposure Management.

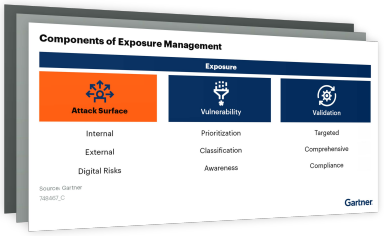
- Cloud-based applications and web services
- Partner/Contractor applications and web services
- Corporate-owned and employee-owned endpoints
- On-premise networks
- Mobile and remote user network connectivity
- Cloud and on-premise databases and data center servers
- IoT devices and sensors
- Industrial control systems
- Physical security entrance and alarm systems

The Three Major Components of External Exposure Management

Gartner's synopsis of External Exposure Management outlines three pillars.

Vulnerability Management: Routine scanning of software and configurations of known assets. This component detects, identifies, raises awareness, quantifies and prioritizes risks based on common vulnerabilities and exposures.

Attack Surface Management: Takes an attacker's view of assets—searching for a vulnerable or overlooked point to breach an asset. This pillar discovers internal, external and digital risks in internet-connected assets to identify gaps in security controls and existing vulnerability assessments.



Vulnerability Validation: Validates the effectiveness of current security controls on internet-connected assets, and includes tools and methods such as penetration testing and attack simulation. This pillar achieves a targeted, comprehensive and compliance view of risks.

Continuous Threat Exposure Management (CTEM)

Ad hoc measures, emergency patches, and even comprehensive asset and vulnerability inventory management programs must evolve into multi-functional security strategies. This layered security must include not only traditional preventative-only controls, but also mature and robust detection and response capabilities. Existing approaches to managing the attack surfaces are no longer keeping up with digital velocity—in an age where organizations can neither fix everything, nor be completely sure what vulnerability remediation can be safely postponed.

Continuous Threat Exposure Management (CTEM) is a pragmatic and effective systemic approach to continuously refine security management and priorities, and replaces blind trust in slow-adapting cybersecurity tools and procedures. Continuous Threat Exposure Management (CTEM) is a five-step program for achieving long-term sustainable cyber resilience, and describes a cycle of five iterative stages: scoping, discovery, prioritizing, validation, and mobilization.

Continuous Threat Exposure Management (CTEM) programs with automated pentesting and red teaming—when combined with External Exposure Attack Surface Management—enables a strong external-facing cybersecurity posture. Organizations can also approach exposure management in a somewhat less structured way than a full implementation of CTEM, by taking specific actions on each of the three components of External Exposure Management.

The Value of Integrating Exposure Management into MSSP and MDR Security Stacks

Risk self-assessment is often suboptimal due to organizational rigidity or tool-specific myopia. Security and risk management teams must initiate a mature Continuous Threat Exposure Management program (CTEM) to stay ahead of today's threats.

External Exposure Management—in conjunction with a full CTEM implementation, or as a separate pre-CTEM action—is becoming a popular adjacent service that MDRs integrate into their portfolios. This includes Exposure Management solutions like breach and attack simulation (BAS), attack surface management, and automated penetration testing. These tools identify and analyze risks within an organization's digital infrastructure to determine asset vulnerabilities, potential loss exposures, and the steps needed to minimize risk. Competitive MDR offerings in the marketplace include capabilities such as continuous security testing, ad-hoc penetration testing, attack surface management, compliance audits and security incident response.

Britt Norwood, Senior VP, Global Channels and Commercial at Trellix emphasizes that security operations are constantly responding to threat alerts from multiple sources and need holistic solutions that minimize the impact threats have on their customers. "Critical to any MDR's business is the ability to reduce security event response times and streamline overall management," he said. "This requires a comprehensive security stack with diverse functions and capabilities all accessible and viewable from a single interface. The ability to identify and validate risk vulnerabilities within apps, systems, storage, and networks, in addition to detecting anomalies and mitigating threats across all attack vectors from endpoints to clouds is a huge advantage."

Unlock Exposure Management with RidgeBot

Ridge Security RidgeBot, an award-winning enterprise security scanning, exploitation and validation tool, seamlessly fits into MSSP or MDR organizations' security stacks and offers tools in all three of the components of External Exposure Management.

- **Vulnerability management:** Continuous vulnerability discovery, providing detailed vulnerability descriptions as well as suggestions and steps for remediation.
- **Attack surface management:** Ongoing asset discovery and inventory, discovery of OS and app types and versions, listing of open ports, listing of external facing URLs, folders and subfolders, scanning of infrastructure connectivity and attack path mapping.
- **Vulnerability validation:** Automated and ongoing validation of security posture to discover vulnerabilities within newly deployed assets, assets updated with code changes, reconfigurations, untested backups, patches and changes in infrastructure connectivity. Internal and external auto-pentest, attack simulation, exploitation of vulnerabilities found, description of risk findings, reporting and automatic prioritization of the vulnerabilities and risks found.

All these capabilities are essential to maintain offensive security protection. Testing through simulation and direct exploit practices in an automated red team fashion can continuously verify and validate that IT infrastructure components, processes, connections, and procedures are working and secure, without opening new vulnerabilities and risks. RidgeBot's RESTful API enables easy integration with SOAR, SIEM and XDR solutions such as Trellix Helix, Splunk Phantom, Stellar Cyber, Nessus Professional and more.

RidgeBot mobilizes External Exposure Management in numerous ways.

- Helps CISO understand overall internal and external cyber risks
- Reduces workload pressure on the security team by automatically prioritizing critical risks and providing suggestions of actions to take to remediate them
- Alleviates staff and resources shortages with automation
- Continuously validates security posture to ensure compliance and to catch newly introduced risks when changes to assets are made

Business Benefits of Ridge Security as your External Exposure Management Technology

The capabilities of Ridge Security RidgeBot can help you grow your security services portfolio for External Exposure Management technology. By offering automated pentesting within an External Exposure security stack enables managed services to:

- Discover, validate and manage vulnerabilities within active assets
- Scan/report on assets and network infrastructure to find attack surfaces and lateral movement
- Provides branded reports organized by business risk
- Conduct automated exploits using ethical hacking skills learned from human testers
- Conduct post-exploit verification with testing techniques like privilege escalation or Pass-the-Hash
- Integrate automated pentesting into MSSP and MDR technology stacks with APIs

There are many business benefits to offering External Exposure Management within your portfolio.

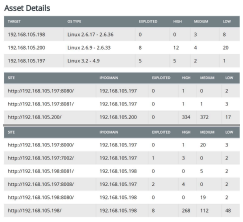
- Fuel business growth and increase revenue streams with adjacent services
- Expand your service delivery portfolio for competitive differentiation and advantage
- More fully meet customer requirements with automation for 360-degree protection across on-premise, cloud, and hybrid environments
- Enable customers to justify their MSSP and MDR spending by reducing risk and improving their business outcomes
- Complement detection and recovery capabilities with exposure management to proactively discover and fix vulnerabilities before bad actors find them

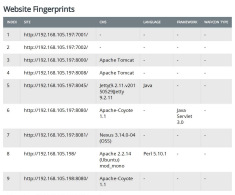
Best Practises for Integrating RidgeBot into MSSP/MDR Service Offerings

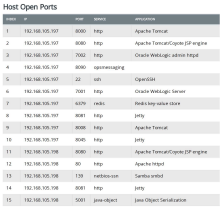
MSSPs and MDRs can package Ridge Security RidgeBot into several innovative service offers.

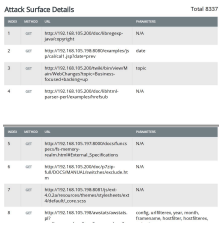
Option 1: Offer Continuous Attack Surface Monitoring

The RidgeBot Attack Surface Identification test launches asset profiling to identify a number of key attributes of each target machine. The service could be priced at a fixed amount per month per customer.









Option 2: Offer a Website Pentest Service

The RidgeBot Website Penetration test launches attacks against websites and web applications including:

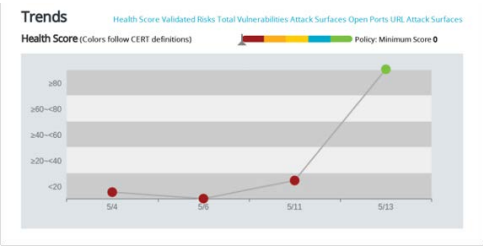
- Authenticated website testing
- Dynamic application security testing
- All popular frameworks are supported
- Testing for the OWASP Top 10 web application security risks

The service could be priced at a fixed amount per test per website.

Option 3: Continuous Vulnerability Management

The RidgeBot Penetration test includes up-to-date trending and historical information on vulnerabilities detected.

- A count of all IP devices with open ports such as servers, IP printers, IP cameras, IP phones, IoT
- Monthly Trending Report
- Monthly Differential Report
- Historical Report that includes asset details, the health score trend, the validated risk trend, the total vulnerability trend, the attack surface trend, and a risk list of every test run



Option 4: Offer a Full Pentest as a Service

The RidgeBot automated Penetration test offers numerous valuable capabilities including:

- Complete asset profiling
- Complete vulnerability reporting
- Exploitation of vulnerabilities detected with exhaustive probing of every attack surface and every attack path
- Deep pentest with post-exploitation and lateral movement
- Remediation suggestions
- Realtime reporting

An MSSP/MDR service offering can advance a customer's manual testing practices by leveraging the efficiency and scalability of an automated platform.

- Increased number of IP destinations, including IP phones, cameras, printers, and IoT devices
- Increased testing frequency

Choose Ridge Security as your External Exposure Management Technology Partner

RidegBot offers automated and continuous penetration testing and validation that easily integrates as an adjacent service within MSSP and MDR platforms or security software stacks. This integration streamlines orchestration and improves efficiency, effectiveness, and productivity, continuously providing clear risk visibility across the customer's entire IT environment.

MSSPs and MDRs that integrate automated pentesting into their security stacks can discover unknown attack surface vulnerabilities using AI-powered algorithms with real-time information to generate dynamic attack strategies. When exploitable risks are uncovered, they are scored to better understand the issues, and to prioritize those that might have the severest impact.

The conventional practice of testing only when required by compliance, annually or on an ad hoc basis, exposes security vulnerabilities introduced by IT changes in between testing cycles. Frequent, ongoing automated testing provides reliable assessments that allow red teams to focus on the higher priority items, reduces effort identifying and prioritizing attacks, and shortens the triaging of false positives.

Security operations technologies are converging toward a broad, cloud-delivered platform that feeds the growth of MDR as an adjacent service in MSSP portfolios. The broad scope of MDR offerings in the marketplace requires compelling differentiation to grow a business.

Ridge Security can help you grow your service offering with award-winning security tools and capabilities that tightly integrate into your security software stack or platform. Ridge Security has a dedicated team of MSSP/MDR partner support staff that can assist you with questions, integration options and deploying RidgeBot to your best advantage.

Ridge Security Technology Inc.

www.ridgesecurity.ai