ARCTIQ

Attack Surface Management as a Service

Powered by

MANDIANT

⋈ Enterprise Security

Over time, IT environments have evolved organically into complex ecosystems — often without adhering to organizational security policies. As a result, security teams struggle to comprehensively assess their rapidly expanding attack surface and tackle growing threat vectors that include cloud assets, apps & services, internal & external assets, a growing supply chain, and a diverse and remote workforce.

Critical Visibility & Monitoring of Your Attack Surface

Arctiq's Attack Surface Management (ASM) as a Service offering, powered by Mandiant, helps organizations identify, monitor, and minimize their digital attack surface and potential entry points for attackers. By merging extensive enterprise visibility, continuous monitoring capabilities, and the latest threat intelligence, we assist organizations in identifying vulnerabilities and analyzing their online exposure effectively.

Our ASM as a Service Encompasses:

Active Vulnerability Checking

Actively checks assets for vulnerability exposure, allowing organizations to stay informed about potential security risks.

Identification of Unsanctioned Resources

Identifies unmanaged or unknown assets as they enter the environment, helping organizations maintain visibility and control over their digital assets.

Searchable Inventory

Maintains a searchable inventory of an organization's technology ecosystem, helping security teams gain a comprehensive view of their assets.

Subsidiary Monitoring

Offers centralized visibility across subsidiary entities and will monitor security policy adherence while standardizing tools and practices.

Attack Surface Management (ASM)

How can ASM help organizations answer fundamental, but critical questions such as:

• What do we have?

• What is it running?

• What are our vulnerabilities?

ASM answers these questions by automatically taking inventory and mapping the extended enterprise to show what the organization has. Through integrations, ASM can show security teams what is running on those assets. ASM can also show security teams what and where the vulnerabilities exist in the environment to help reduce risk.

Real-World Coverage

Provides coverage for fast-breaking vulnerabilities, such as the Log4j, and aligns with recognized databases like NIST National Vulnerability Database (NVD) and CISA's Known Exploited Vulnerability catalog.

Digital Supply Chain Monitoring

Identifies and assesses the supply chain ecosystem, extending beyond third- and fourth-party providers. It will also assess the external security posture of each vendor.

Merger & Acquisition Support

Assesses the external security posture and risks associated with potential acquisitions, facilitating due diligence and post-acquisition integration.
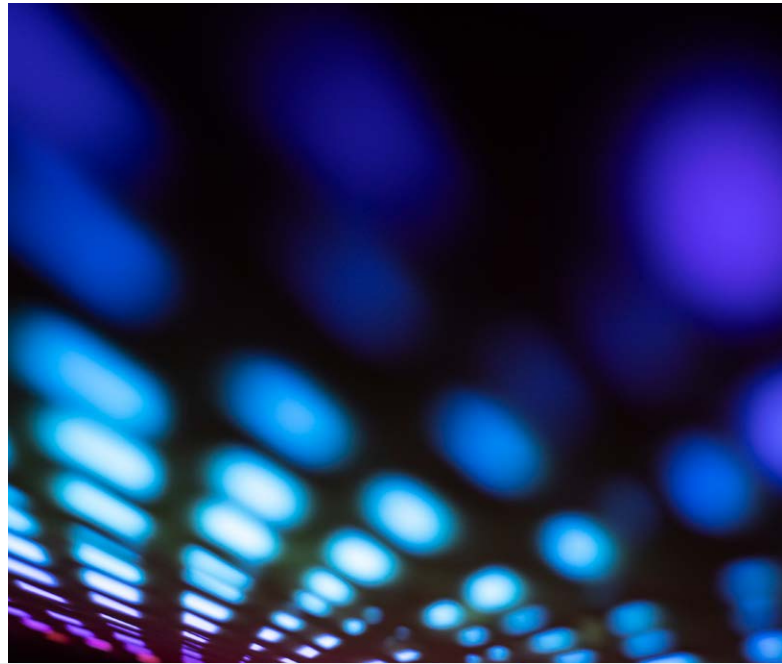
Security Expertise 24x7x365

Delivered as a fully managed service through our three North American Security Operations Centers, our ASM as a Service provides a 24x7x365 coverage through a team of security experts that provide:

Deployment and Integration

We seamlessly deploy and integrate ASM into your organization's infrastructure, ensuring a smooth onboarding process.

Onboarding

For new customers, we provide the necessary groundwork by populating initial data to kick-start the ASM process.

Issues

We distinguish between true positives (TP) and false positives (FP), helping your organization prioritize real security concerns.

Remediation

We provide recommendations for remediation and can take action to address issues within the purview of our service.

Reporting

Our service provides both basic and granular reporting on an ongoing basis, offering insights into your organization's security posture.

Ownership Confirmation

We confirm ownership of newly discovered assets, ensuring accurate identification and management.

Our service provides continuous asset discovery, vulnerability assessment, monitoring, and risk reduction through activities such as patching, security configuration, and access control adjustments. We also include incident response planning, compliance management, third-party assessments, and user training to ensure a holistic and proactive approach to cybersecurity, helping organizations safeguard their systems, data, and networks in an ever-evolving threat landscape.

Key Benefits

Arctiq's ASM as a Service assists customers in managing their attack surface by providing comprehensive visibility into their extended enterprise, starting from DNS data and iteratively discovering assets, services, application technologies, and cloud resources. We continuously monitor assets for exposure, identifying vulnerabilities and misconfigurations while cross-referencing data with Mandiant Threat Intelligence for prioritization. In order to transform this intelligence into practical insights, we emphasize the significance of continuous, real-time management, given the ever-changing nature of the attack surface. Daily activities and alerts enable continuous risk monitoring, with integration into existing workflows via platforms like ServiceNow, JIRA, and Splunk, ensuring that security operations teams can efficiently investigate and respond to critical exposures.

Broad Asset Visibility

We categorize 15+ asset types, providing broad visibility across an organization's external ecosystem.

Extensive Vulnerability Coverage

We cover 170K+ vulnerabilities, actively confirming vulnerabilities, misconfigurations, and exposure.

Comprehensive Asset Mapping

We provide comprehensive visibility through asset mapping, discovering assets and cloud resources through various integrations and techniques.

Real-Time Asset Monitoring

We monitor your infrastructure in real time, detecting changes and exposures to stay ahead of threats.

Risk Management

We automatically apply expertise and intelligence to your attack surface, helping identify vulnerabilities, misconfigurations, and exposures.

Integration

Our platform integrates with various security programs, third-party security tools, and external repositories to streamline security efforts. With 250+ data source integrations, we automatically leverage discovery techniques and enrich assets.

Advanced Threat Intelligence

Our experts constantly monitor the threat landscape to provide you with up-to-date intelligence on emerging threats and vulnerabilities.

Our Managed Extended Detection and Response (MXDR) and ASM as a Service collaborate to fortify your organization's cybersecurity defenses. ASM as a Service offers comprehensive visibility by identifying and monitoring digital assets and the attack surface, supplying vital context for MXDR solutions. MXDR utilizes this context to prioritize alerts, enhance threat detection, and execute incident response efficiently. ASM as a Service continuously monitors for changes in the attack surface, promptly sharing insights with MXDR for adaptive detection strategies. Furthermore, ASM as a Service contributes to vulnerability management, and MXDR leverages vulnerability data to focus threat detection efforts. The combined approach ensures a well-rounded security posture, reducing potential attack vectors while improving threat detection and response capabilities.

Next Gen Security with Managed XDR + ASM as a Service

Get in touch with us today to schedule a free consultation and demonstration.

Attack Surface Management is paramount in today's cybersecurity environment, given the ever-expanding and evolving attack surface with cloud adoption, SaaS applications, and mobile devices. Our ASM as a Service empowers organizations to safeguard their perimeter, adapt to emerging technologies, and strengthen security governance in a swiftly evolving digital landscape. Contact us now to explore how this solution can benefit your organization or to witness it in action.

Arctiq is a dominant force in the IT services and cybersecurity industry, combining extensive experience, top-tier partnerships, and unmatched technical expertise. With advanced Security Operations Centers and a commitment to innovation, Arctiq delivers cutting-edge cybersecurity solutions to clients throughout North America, reinforcing their security in the digital era.

Business Drivers and Challenges

We're here to align your IT strategy with your business objectives and tackle the challenges that matter most to you.

Ransomware Attacks

Data Breaches

Cloud Security

Compliance and Regulatory Requirements

Phishing and Social Engineering

Insider Threats

Security Skills Shortage

Infrastructure Recoverability

Patch Management

Contact Arctiq Today

At Arctiq, we are dedicated to ensuring the highest level of cybersecurity for your organization. Our tailored solutions, combined with our commitment to innovation, empower you to navigate the digital landscape securely, confidently, and with resilience.

▶ Partner with Arctiq to protect your digital assets and stay ahead of emerging threats
Book a consult.

Book a consultation