PRAETORIAN

WHITE PAPER

Attack Surface Management

A Free Enablement Technology for Effective Continuous Threat Exposure Management

INSIDE THIS REPORT

- The Foundation of Modern Security
- Why Attack Surface Management Matters
- The Cost of Ignoring Your Attack Surface
- Free vs. Paid: Making the Right Choice
- Integration with CTEM
- Implementation Best Practices
- Getting Started

INTRODUCTION

The Foundation of Modern Security

Attack Surface Management (ASM) has emerged as a foundational capability for modern cybersecurity programs. At its core, ASM provides visibility into the assets and exposures that make up your organization's digital footprint.

In today's rapidly evolving threat landscape, organizations struggle to maintain an accurate inventory of their internet-facing assets. Cloud migrations, shadow IT, and the proliferation of SaaS applications have exponentially increased the complexity of tracking what systems exist, where they reside, and how they're configured.

This whitepaper explores why Attack Surface Management should be considered a free enablement technology—a foundational layer that enables more advanced security capabilities like Continuous Threat Exposure Management (CTEM)—rather than a premium add-on or standalone product category.

> **Key Insight:** Organizations that treat ASM as a foundational, freely available capability build stronger security programs than those who view it as a premium feature locked behind expensive vendor contracts.

WHY ASM MATTERS

Why Attack Surface Management Matters

You cannot secure what you cannot see. This fundamental truth underpins the importance of Attack Surface Management. Before any vulnerability assessment, penetration test, or security control can be effective, you must first know what assets exist in your environment.

1. **Complete Visibility**
   ASM discovers assets across cloud providers, on-premises infrastructure, and third-party services, giving you a comprehensive view of your digital footprint.

2. **Shadow IT Discovery**
   Uncover unauthorized or forgotten systems that may have been deployed outside formal IT processes, often representing significant security gaps.

3. **Continuous Monitoring**
   Unlike point-in-time assessments, modern ASM provides ongoing visibility as your environment changes, alerting you to new exposures as they emerge.

The Attack Surface Has Exploded

Modern organizations operate across multiple cloud providers, leverage dozens of SaaS applications, and maintain complex hybrid infrastructures. Each new service, each new integration, each new deployment potentially expands the attack surface. Without continuous ASM, security teams are essentially flying blind.

THE RISK

The Cost of Ignoring Your Attack Surface

Organizations that lack comprehensive attack surface visibility face significant risks. Breaches often occur not through sophisticated zero-day exploits, but through simple misconfigurations or forgotten systems that attackers discover through basic reconnaissance.

67%
OF BREACHES INVOLVE UNKNOWN ASSETS

197
DAYS AVERAGE TIME TO IDENTIFY A BREACH

Common Attack Surface Blind Spots

- **Orphaned cloud resources** - Compute instances and storage buckets created for temporary projects that were never decommissioned
- **Shadow SaaS** - Cloud applications adopted by business units without IT oversight or security review
- **Misconfigured services** - Databases, storage, or APIs inadvertently exposed to the internet
- **Expired certificates** - TLS certificates that have lapsed, potentially exposing traffic to interception
- **Subdomain takeover risks** - DNS entries pointing to resources that no longer exist, which attackers can claim

THE CHOICE

Free vs. Paid: Making the Right Choice

The security industry has seen a proliferation of ASM vendors, many charging premium prices for capabilities that are increasingly available at no cost. Understanding what you truly need versus what vendors want to sell is critical for making informed decisions.

> **Free ASM capabilities include:** Basic asset discovery through OSINT, certificate transparency log monitoring, DNS enumeration, IP range scanning, and cloud provider inventory integration. These foundational capabilities provide significant value and should be table stakes for any security program.

When Does Paid ASM Make Sense?

While basic ASM should be free, there are scenarios where premium capabilities provide genuine value:

- **Advanced correlation** - Connecting disparate data sources to identify complex attack paths
- **Prioritization intelligence** - Context-aware risk scoring that goes beyond simple vulnerability counts
- **Remediation workflows** - Integration with ticketing systems and automated response capabilities
- **Managed expertise** - Human analysts who can interpret findings and provide actionable guidance

INTEGRATION

ASM as an Enablement Technology for CTEM

The true value of Attack Surface Management becomes apparent when viewed not as a standalone product, but as an enablement layer for Continuous Threat Exposure Management (CTEM). ASM provides the foundational visibility upon which all other security activities depend.

ASM is the foundation. CTEM is the structure built upon it.

How ASM Enables CTEM

1. **Scoping**
   ASM data feeds directly into the CTEM scoping phase, ensuring testing programs cover all relevant assets.
2. **Discovery**
   Continuous ASM ensures the discovery phase always works with current asset inventories, not outdated snapshots.
3. **Prioritization**
   ASM context—such as asset criticality and exposure level—enables more intelligent risk prioritization.

BEST PRACTICES

Implementation Best Practices

Successfully implementing Attack Surface Management requires more than just deploying tools. Organizations should follow established best practices to maximize value and avoid common pitfalls.

Start with the Basics

- **Inventory your known assets first** - Before seeking unknowns, ensure you have a complete list of what you already know about
- **Integrate with cloud providers** - Direct API integrations provide more accurate and complete data than external scanning alone
- **Establish baseline monitoring** - Set up continuous monitoring to detect changes as they occur, not weeks later

Avoid Common Mistakes

- **Don't chase perfection** - 100% asset visibility is aspirational; focus on covering critical systems first
- **Don't ignore context** - Raw asset lists are less useful than inventories tagged with business context
- **Don't silo ASM data** - Ensure ASM feeds into broader security workflows and tools

CONCLUSION

Getting Started

Attack Surface Management should not be viewed as a premium product category requiring significant budget allocation. The foundational capabilities—asset discovery, inventory management, and basic monitoring—are increasingly available through free tools and open-source solutions.

> **The key is to start.** Even basic ASM visibility provides significant value over operating blindly. As your program matures, you can evaluate whether premium capabilities justify their cost based on your specific needs and constraints.

At Praetorian, we believe that ASM is a foundational enablement technology that should be freely available to all organizations. That's why we include comprehensive attack surface discovery as a core component of our platform—no additional licensing, no hidden fees.

By treating ASM as a foundational layer rather than a profit center, we enable organizations to build more effective security programs that deliver real risk reduction, not just compliance checkboxes.

Ready to See Your Attack Surface?

Start with a free assessment and discover what you're missing.

Get Started

© Copyright 2024 Praetorian Group, Inc. All rights reserved.