Anomali Attack Surface Management

Identify, prioritize, and address security risks—fast

A single security gap can leave your organization's data open to attack. To fortify your attack surface, you need to discover all your exposed assets, prioritize them based on the risk they pose to your business, and remediate them quickly.

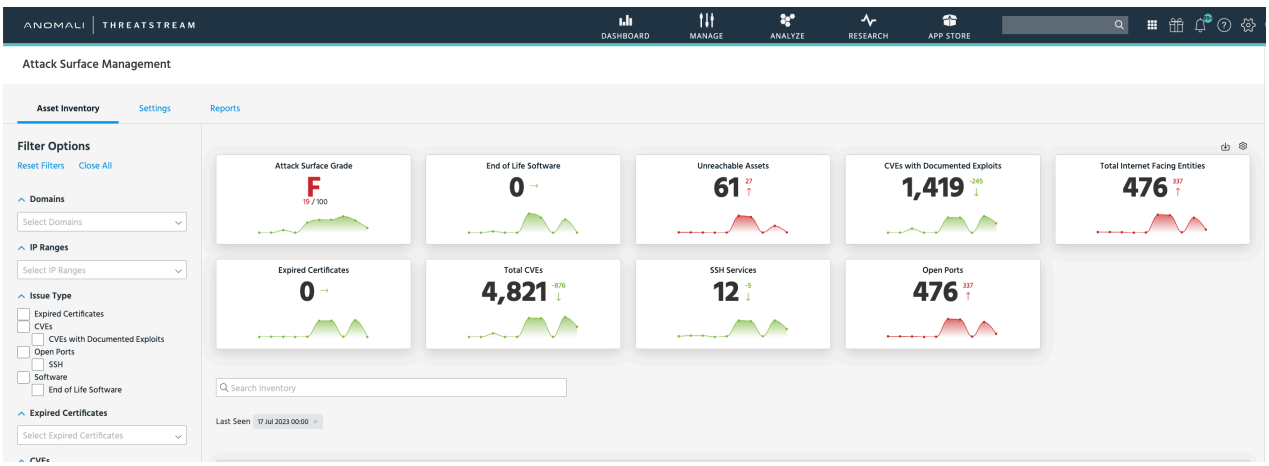
Anomali Attack Surface Management provides comprehensive visibility into all your IT assets, including shadow IT, to fuel actionable security analytics. Real-time monitoring flags outdated policies, misconfigured assets, and other at-risk entities. A real-time dashboard and drill-down details provide insight into asset criticality and vulnerability as well as potential attack severity.

Armed with complete information and context, security teams can work quickly to fix the most important gaps first and enable fast, effective remediation across your organization.

As part of the Anomali security operations platform, Anomali Attack Surface Management connects your internal security telemetry with the world's largest threat intelligence repository, industry-leading detection and response, and data-driven automation to help security teams to minimize cyber risks and strengthen your security posture.

BENEFITS

- Visualize your environment through the eyes of the attacker
- Detect and respond immediately to exposures in your attack surface
- Share information, context, and drill-down details easily with other teams
- Gain full visibility into exposed assets and infrastructure—including shadow IT
- Leverage real-time insights to understand risks and prioritize responses
- Monitor for new exposures and vulnerabilities
- Provide management with high-level visibility on your current attack surface



Eliminate blind spots, prioritize risks, and enable fast remediation

Modern hybrid environments, distributed workforces, multi-vendor security, and shadow IT make it hard to gain complete visibility and understanding across the enterprise attack surface. To work faster and smarter, security teams need both comprehensive visibility and data-driven insight into each vulnerability and the risk it presents.

Anomali Attack Surface Management continuously inventories and monitors your entire digital footprint, including hardware, applications, SaaS deployments, cloud resources, websites, subdomains, IP addresses, social media accounts, and vendors' infrastructures—as well as the shadow IT assets that leave many organizations exposed.

Ongoing visibility, scanning, and discovery on both sides of the firewall help you track:

- Internet-facing hosts
- Unreachable assets
- SSH services
- Open ports
- CVEs
- CVE exploits
- End-of-life software
- Expired certificates

View your attack surface through the eyes of an attacker

Working with Anomali Security Analytics, Anomali Attack Surface Management quickly identifies the most desirable exposed assets for an attacker. Security teams can understand not only what's at risk, but also what an attack might look like—and how to prevent it.

Discover and remediate unknown assets and vulnerabilities

What you don't know will hurt you. Anomali Attack Surface Management helps you find and proactively secure internet-facing assets that you might not have been aware of—before attackers get there first. On-demand and scheduled monitoring enable continuous visibility into vulnerabilities. Alerts on new and emerging threats help you respond quickly to incidents.

Prioritize efforts to work faster and smarter

Real-time insight into the risk posed by each vulnerability helps you prioritize investigation and remediation. Point-in-time and historical views show how long assets have been vulnerable, whether they've been compromised, and how your attack surface changes over time. An understanding of potential attack vectors reduces the risk posed by digital transformation projects.

Key Use Cases

Understand risk

Assess exposures and prioritize remediation by criticality

Avoid blind spots

Gain comprehensive asset visibility—including shadow IT

Close potential attack paths

Prioritize security control deployment and configuration where it's most needed

Respond effectively to attacks

Use integrated intelligence and context on exploits and actors

Monitor security over time

Track both historical and real-time changes to your external surface

ANOMALI