ANOMALI

ANOMALI ATTACK SURFACE MANAGEMENT

FIND AND MAP ASSETS AGAINST POTENTIAL VULNERABILITIES

Organizations are collecting and storing more data than ever, driven by digital transformation and other shifting priorities. Many organizations lose track of their assets, failing to update policies and their security infrastructure, leaving them susceptible to attacks that exploit known vulnerabilities.

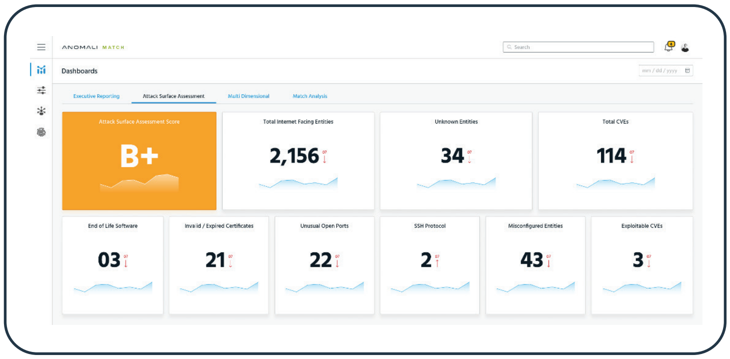
Protecting your environment starts with an Attack Surface Assessment that provides insights into an organization's infrastructure to uncover exposed assets to stop breaches and attackers.

The Attack Surface Assessment provides visibility into ALL external facing assets, either managed or unmanaged (shadow IT) by the organization's IT group, and identifies those exposed.

With this information, organizations are able to understand impact based on (a) asset criticality, (b) asset vulnerability, and (c) potential attack severity. This enables analysts to prioritize investigations and perform remediation of mis-configured assets and/or security controls and patching of vulnerable, exposed assets.

KEY BENEFITS

- Visualize your environment through the eyes of the attacker
- Accelerate mean time to detect (MTTD) and mean time to respond (MTTR) to active threats
- Gain increased visibility into exposed assets and infrastructure
- Leverage real-time insights to understand risks and prioritize response activities
- Monitor for emerging threats to alert on new vulnerabilities
- Prioritize risks and vulnerabilities based on insights and analytics
- Understand asset diversity to establish a baseline to determine risks



ANOMALI MATCH

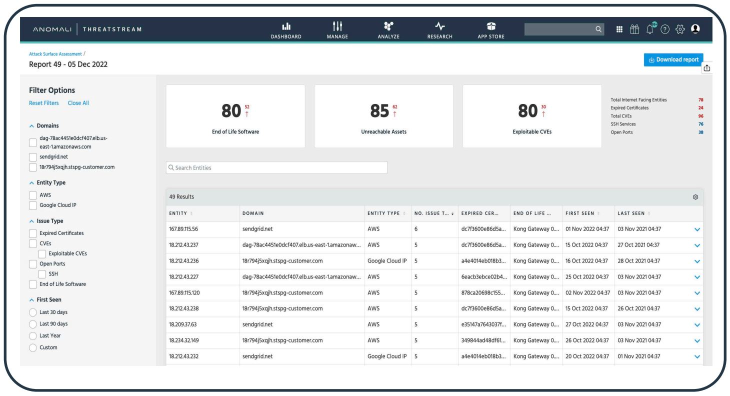
Search

Dashboards

mm / dd / yyyy

Executive Reporting | Attack Surface Assessment | Multi Dimensional | Match Analysis

Tile	Value
Attack Surface Assessment Score	B+
Total Internet Facing Entities	2,156 07 ↓
Unknown Entities	34 07 ↓
Total CVEs	114 07 ↓
End of Life Software	03 07 ↓
Invalid / Expired Certificates	21 07 ↓
Unusual Open Ports	22 07 ↓
SSH Protocol	2 07 ↑
Misconfigured Entities	43 07 ↓
Exploitable CVEs	3 07 ↓



Attack Surface Assessment /

Report 49 - 05 Dec 2022

Download report

Filter Options

Reset Filters Close All

Domains

- □ dag-78ac4451e0dcf407.elb.us-east-1.amazonaws.com
- □ sendgrid.net
- □ 18r794j5xqjh.stspg-customer.com

Entity Type

- □ AWS
- □ Google Cloud IP

Issue Type

- □ Expired Certificates
- □ CVEs
  - □ Exploitable CVEs
- □ Open Ports
  - □ SSH
- □ End of Life Software

First Seen

- ○ Last 30 days
- ○ Last 90 days
- ○ Last Year
- ○ Custom

80 52 ↑ End of Life Software

85 62 ↑ Unreachable Assets

80 30 ↑ Exploitable CVEs

Total Internet Facing Entities	78
Expired Certificates	24
Total CVEs	96
SSH Services	76
Open Ports	38

Search Entities

49 Results

ENTITY	DOMAIN	ENTITY TYPE	NO. ISSUE T...	EXPIRED CER...	END OF LIFE ...	FIRST SEEN	LAST SEEN
167.89.115.56	sendgrid.net	AWS	6	dc7f3600e86d5a...	Kong Gateway 0....	01 Nov 2022 04:37	03 Nov 2021 04:37
18.212.43.237	dag-78ac4451e0dcf407.elb.us-east-1.amazonaw...	AWS	5	dc7f3600e86d5a...	Kong Gateway 0....	15 Oct 2022 04:37	27 Oct 2021 04:37
18.212.43.236	18r794j5xqjh.stspg-customer.com	Google Cloud IP	5	a4e4014eb018b3...	Kong Gateway 0....	16 Oct 2022 04:37	28 Oct 2021 04:37
18.212.43.227	dag-78ac4451e0dcf407.elb.us-east-1.amazonaw...	AWS	5	6eacb3ebce02b4...	Kong Gateway 0....	25 Oct 2022 04:37	03 Nov 2021 04:37
167.89.115.120	18r794j5xqjh.stspg-customer.com	AWS	5	878ca20698c155...	Kong Gateway 0....	02 Nov 2022 04:37	03 Nov 2021 04:37
18.212.43.238	18r794j5xqjh.stspg-customer.com	AWS	5	dc7f3600e86d5a...	Kong Gateway 0....	15 Oct 2022 04:37	26 Oct 2021 04:37
18.209.37.63	sendgrid.net	AWS	5	e35147a7643037f...	Kong Gateway 0....	27 Oct 2022 04:37	03 Nov 2021 04:37
18.234.32.149	18r794j5xqjh.stspg-customer.com	AWS	5	349844ad48df61...	Kong Gateway 0....	26 Oct 2022 04:37	03 Nov 2021 04:37
18.212.43.232	sendgrid.net	Google Cloud IP	5	a4e4014eb018b3...	Kong Gateway 0....	20 Oct 2022 04:37	01 Nov 2021 04:37

Anomali Attack Surface Management

Security teams are stretched thin, managing multiple tools across various hybrid cloud environments – including public clouds, private clouds, and on-premises.

This creates critical blind spots, leaving security teams struggling to prioritize efforts in areas that will minimize damage and disruption.

With Anomali's Attack Surface Management, organizations receive ongoing visibility, scanning, and discovery to help locate entities outside their firewalls, including:

- Internet facing hosts
- Unreachable Assets
- SSH Services
- Open Ports
- CVEs
- CVE Exploits
- End of Life Software
- Expired Certificates

The Anomali Difference

By marrying all ingested security telemetry with the world's largest global intelligence repository, Anomali is able to connect an organization's internal attack surface with its global threat landscape to minimize risks and prioritize investigation and response activities.

Anomali's Attack Surface Management provides a contextual inside-out and outside-in view that enables organizations to not only see what's exposed, but understand the who/what/how of an attack and the additional context needed on how to fix any vulnerabilities.

Anomali's proprietary data provides a point in time as well as a historical view with insights that others can't. This includes identifying vulnerable assets and informing on how long they've been vulnerable, and if they've been compromised.

Organizations can uncover vulnerabilities and continuously monitor their environment to alert on new or emerging threats and respond quickly.

KEY USE CASES

DISCOVER
Uncover assets that are part of your attack surface and understand their vulnerabilities

MONITOR
On-demand and scheduled scans to identify known and hidden vulnerable assets

ANALYZE
Compare progress and activities completed since the previous scan to understand gaps and trends

PRIORITIZE
Determine what assets are most at risk to prioritize response efforts

ANOMALI