USE CASE

Achieve Cyber Asset Attack Surface Management

CAVELO

Swap costly spend and multiple data protection technologies for a simple, single pane of glass

Traditional data protection used to focus on a business's perimeter and the assets (hardware and software) that operated within its "walls". Yet today's borderless workplaces mean the perimeter no longer exists and instead creates almost a limitless attack surface. Every asset is critical for the sensitive data it collects, stores and shares.

THE CHALLENGE

As businesses continually add new assets they stretch their overall attack surface, increasing cyber risk and the likelihood of a data leak or security breach.

Every business uses different methods and technologies to track digital assets and manage data protection. But using multiple technologies silo company data. As a result, businesses often lack complete visibility to the sensitive data they have, where it lives, and how it impacts their risk.

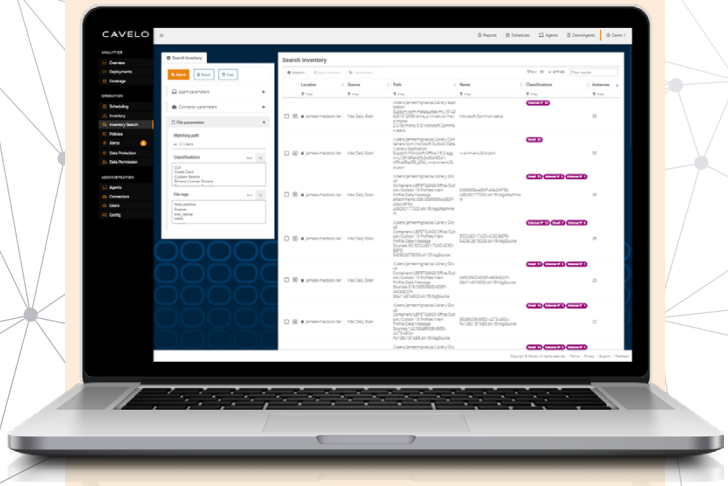
Risks of Limited or Non-existent Cyber Asset Attack Surface Management Capabilities:

- Data Silos
- Poorly Protected Data
- Incomplete Data Inventory
- Regulatory Non-compliance
- Exfiltration of Data
- Ransomware Attacks
- Reputational Risk
- Financial Losses
- Incident Response
- Operational Risk

Let Cavelo handle CAASM with always-on asset discovery, data classification and risk benchmarking.

Here's how:

1. Drive operational and security decision making with real data using Cavelo's query and reporting capabilities.
2. Take advantage of agent-based and remote network scanning that provides you with an accurate and thorough vulnerability report.
3. Customize the Cavelo dashboard and features to match your unique business requirements, use cases and regulatory frameworks.



THE SOLUTION

Cyber Asset Attack Surface Management (CAASM) starts with gaining and maintaining visibility to all of the digital assets the business uses, and the sensitive data they contain. With full visibility, businesses can establish an up-to-date inventory and leverage real data to make critical and time-sensitive response and remediation decisions.

Understanding where sensitive data lives within the business, how it's protected, where it's been used and who has access to it supports regulatory requirements and data governance programs.

CAASM provides:

- ✓ Visibility to the entire environment, all in one centralized location.
- ✓ Data access and management to popular cloud services (including Office365, Google Workspace, Salesforce, Dropbox and more) through built-in API connectors.
- ✓ Data integrity and tighter data access controls to ensure the right people have access to the right data.
- ✓ An asset catalog with classification types that align to the business.
- ✓ Auto-classification that identifies sensitive data types within the data inventory and defines relative data types.
- ✓ Remediation prioritization – ranking items in order of priority to lower the business's risk of a breach.

LEARN MORE