DATA SHEET

Securin

External Attack Surface Management (EASM)

The Need for External Attack Surface Management

Every external asset is being scrutinized with literally thousands of eyes, both physical and emulated by AI. Yet organizations do not understand their attack surface, whether on premises or in the cloud:

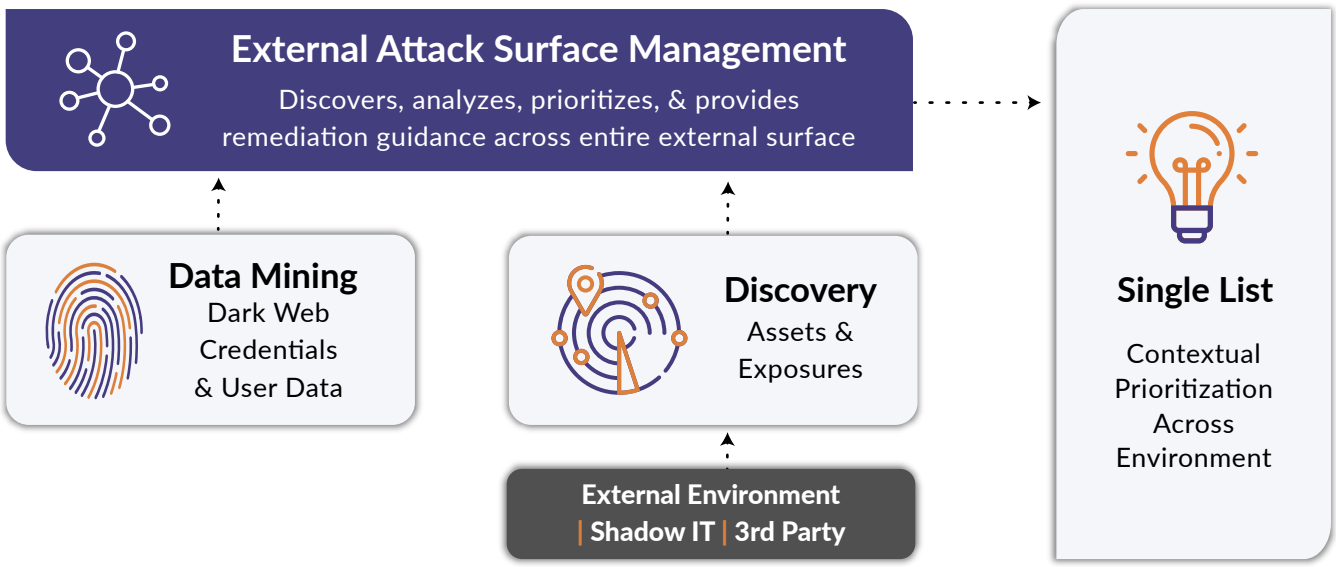
- **Undefined Attack Surface:** Today, organizations rely on a hodgepodge of approaches that even as a whole do not fully characterize all assets and environments.
- **Incomplete Enumeration:** Even if the assets and environment are fully characterized, most organizations lack the vulnerability intelligence needed to detail the most critical exposures, including compromised credentials available on the Dark Web.
- **Too Many Exposures:** Most organizations do not take the adversary's view of how best to exploit that environment and so instead present too many exposures for the organization to handle.
- **Lack of Validation:** Organizations often flag mitigations and remediations as complete then find out that the exposure is still present, often weeks after the fact.

To protect the entire attack surface - including the cloud - organizations need robust discovery of all assets and environment characteristics, full enumeration of exposures, prioritization from the adversary's view, and validation of mitigation and remediation efforts prior to closing the issue. Security teams need an approach that spans the entire lifecycle of exposures and can be baked into both IT operations and DevSecOps practices.

Introducing Securin EASM

Delivered as a software as a service (SaaS) application, Securin External Attack Surface Management (EASM) provides a single, prioritized list of vulnerabilities across the entire attack surface – external environment, Dark Web, shadow IT and 3rd party – all from an adversary's point of view. Securin EASM is powered by researching the entire web, crawling the organization's environment, and data mining the Dark Web. Securin EASM algorithms continuously evaluate the severity of risks and balance them against asset priority. The result is a single list of vulnerabilities, prioritized in the context of that unique overall environment.

Product Overview



Features

Leveraging intelligence from Securin Vulnerability Intelligence (VI), Securin EASM provides leading-edge capabilities for security teams and applications.

Discovery	Securin EASM conducts continuous crawling for discovery of the external environment, Dark Web, cloud (ingest AWS periodically for in-depth scans)/ shadow IT, 2nd party (lateral domains), and 3rd party (vendors and suppliers). On average, EASM discovery yields 20-30% previously unknown assets.
Credential Intelligence	Even the best security is bypassed by a leaked System Administrator User ID and password. Securin EASM provides over 40x the Dark Web information versus open-source intelligence (OSINT), such as leaked credentials used in direct attacks. Also, Securin EASM identifies plaintext passwords exposed in the Dark Web.
Exploit Intelligence	Leveraging Securin VI's rich data, Securin EASM provides information about exploits, tracking: proof of concept (POC) exploits, remote code execution (RCE), privilege escalation (PE), public exploits, exploitation in the wild, exploitation by threat actors, exploitation by ransomware, and exploit code.
Web Crawling	Securin EASM crawls the entire web to detect potentially vulnerable systems and attacker command & control (C2) infrastructure. Securin EASM detects customer IPs that are part of a C&C (AKA Botnet) and flags as an exposure.
Contextual Prioritization	Generates a single, normalized, prioritized list of vulnerabilities. An Adversary's view prioritizes the vulnerabilities most likely to be exploited in that unique environment.
Remediation Validation	Validates that the exposure is still present (e.g. remediation was not applied), checking three times before closing. To minimize cycle time, security teams can manually flag the remediation as closed.
Environment Risks	Securin EASM gathers and assesses information about the infrastructure, network, web application, and cloud environment, including application programming interfaces (APIs), and the tech stack. Exposures such as open ports and unsecured services are identified. Problematic issues such as misconfigurations and expired certificates are pinpointed.
Implementation	Readily onboarded in less than an hour, Securin EASM provides full attack surface and asset information via REST APIs. Information is also available via the user interface (UI) for interactive exploration. For formal integrations, Securin EASM fully interoperates with IT service management (ITSM) applications, network scanners, and public clouds. In addition to being fully embeddable, Securin EASM is also available as an OEM product.

Usage Modes

Each vulnerability's history, association with threat actor groups, use in the MITRE ATT&CK framework, and mitigation or remediation is detailed in user-friendly drill down and drill through formats. Securin EASM is accessible via UI for interactive exploration and and via REST APIs for embedding in applications and for OEM arrangements.

- **Direct Access:** Via an intuitive user interface (Figure 1 and Figure 2), security analysts can explore vulnerabilities interactively. Vulnerability information is shown by assets, but analysts can search, filter, drill down, and drill aside to explore all information.

- **Embedded in Applications:** Securin EASM is designed to be leveraged by other applications and tools. SaaS delivery and robust APIs ensure that Securin's model of intuitive exploration is available within the organization's customized applications and original equipment manufacturer (OEM) applications including those delivered by managed security service providers (MSSP).

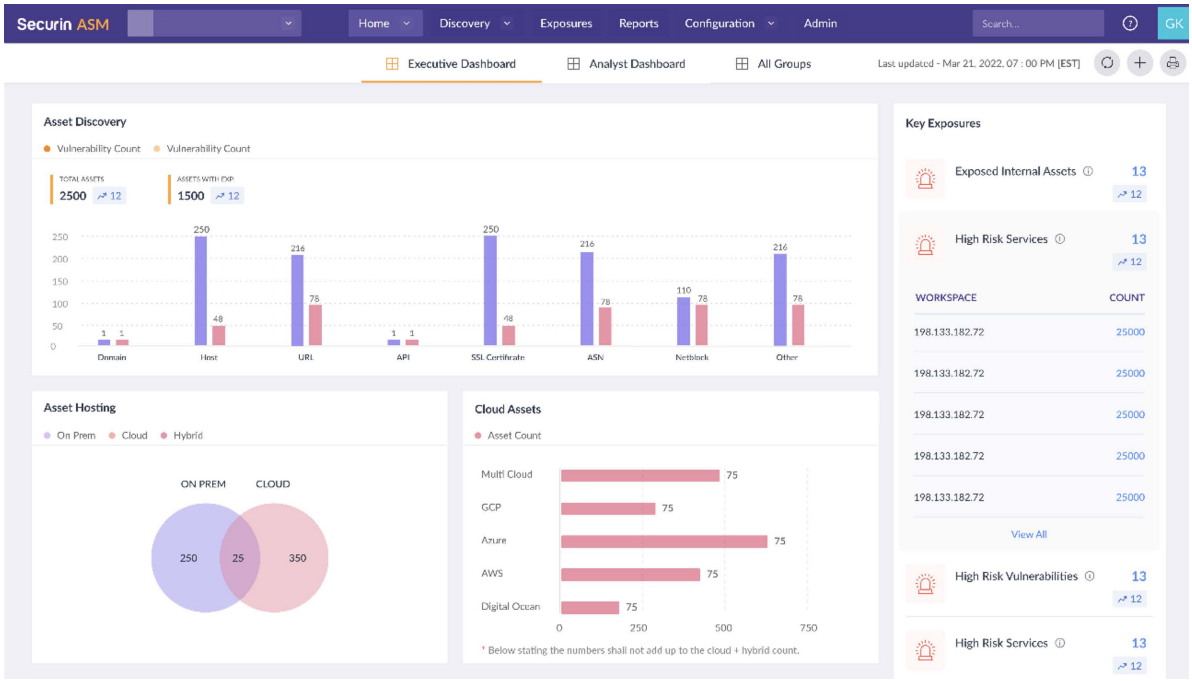
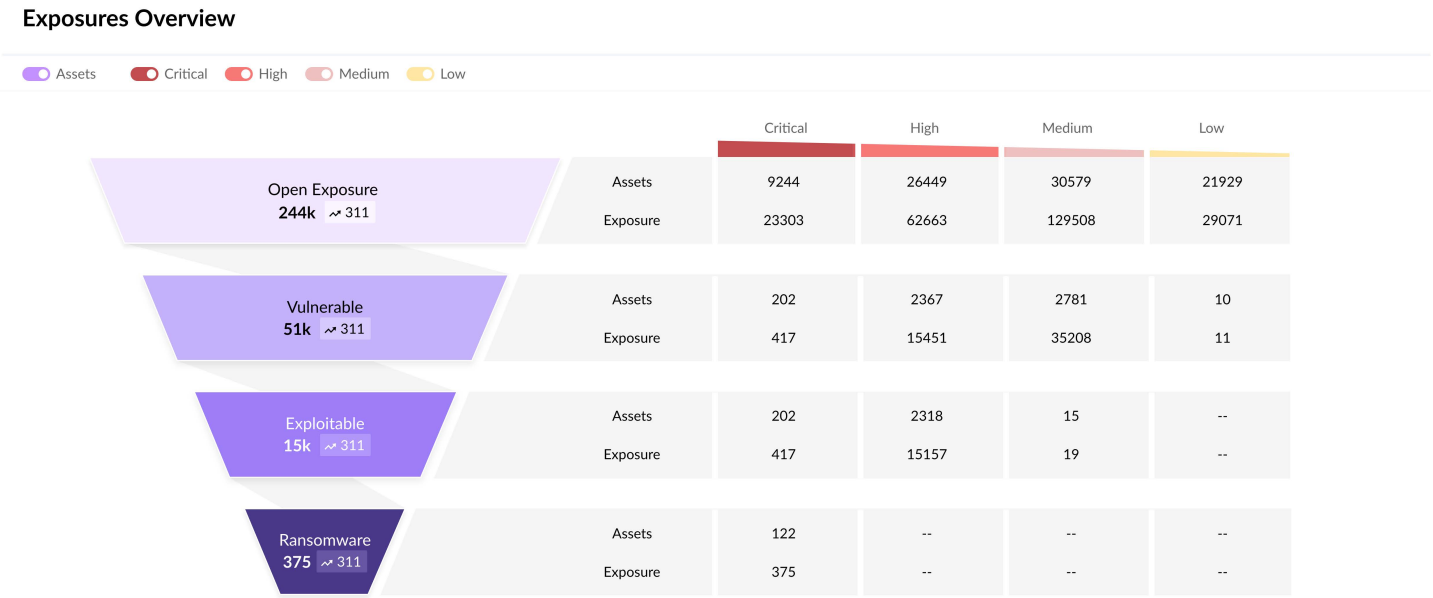


Figure 1: Securin EASM provides intuitive attack surface management across the external environment.



		Critical	High	Medium	Low
Open Exposure 244k 311	Assets	9244	26449	30579	21929
	Exposure	23303	62663	129508	29071
Vulnerable 51k 311	Assets	202	2367	2781	10
	Exposure	417	15451	35208	11
Exploitable 15k 311	Assets	202	2318	15	--
	Exposure	417	15157	19	--
Ransomware 375 311	Assets	122	--	--	--
	Exposure	375	--	--	--

Figure 2: Securin EASM has powerful display and filtering capabilities available via UI and API.

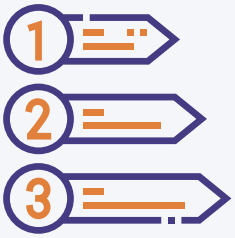
Unique Capabilities

Securin EASM provides unmatched capabilities including:

- **Discovery:** Discover 20-30% of assets previously hidden to the organization (shadow IT).
- **Credential Intelligence:** Securin EASM provides over 40x more Dark Web information versus open-source intelligence (OSINT) approaches including both leaked credentials and network passwords sent in clear text.
- **Contextual Prioritization:** Contextual prioritization ranks vulnerabilities from an adversary's perspective in terms of ease of exploitation in that unique environment. With this focus, security teams have been able to reduce overall issues by 71% in just a few months.
- **Environment Risks:** Gather and assess information about the computer, network, and cloud environment, highlighting misconfigurations, certificate issues, open ports, and more.

Benefits

These benefits apply both to direct use via the UI and embedded use via APIs.



Provides Single Source of Prioritization

Compiles a single, prioritized list of vulnerabilities – with asset values factored into the analysis - for that customer's external environment including Dark Web, shadow IT, and 3rd party.

Supports Business Initiatives Proactively

Provides proactive risk assessment before acquisition, integration into corporate network, or migration to a new environment, supporting business initiatives.

Addresses Needs of All Groups

Delivers a full range of information and automation-ready background to maximize the effectiveness of groups such as development, security, and remediation.

About Securin

At Securin, we empower teams and organizations to minimize their business risk with our comprehensive range of offensive cybersecurity solutions. These solutions are carefully crafted to be intuitive, adaptable, and scalable, catering to organizations of all sizes in today's ever-changing digital landscape. Securin's human-augmented intelligence approach to cybersecurity empowers organizations to thrive by proactively addressing emerging threats and uncertainties, ensuring their security.

Securin
securin.io

Follow Us On