BRACKISH SECURITY

ATTACK SURFACE MANAGEMENT PLATFORM

PINCHER

https://brackish.io
https://pincher.io

Executive Summary

Pincher is a full-fledged Attack Surface Management (ASM) platform which offers a comprehensive solution for identifying, assessing, and mitigating vulnerabilities across an organization's digital footprint. In today's digital age, where cyber threats are increasingly sophisticated and pervasive, an ASM platform serves as the cornerstone for proactive security measures. By continuously discovering and inventorying all accessible assets across on-premises, cloud, and third-party environments, the platform ensures that every facet of the attack surface is accounted for and monitored. This includes not only traditional IT infrastructure but also emerging technologies and services that expand an organization’s exposure, such as IoT devices, web applications, and API endpoints.

The core strength of the Pincher platform lies in its ability to provide real-time visibility into the security posture of these assets, identifying vulnerabilities, misconfigurations, and at-risk data that could be exploited by adversaries. Through advanced scanning and analysis techniques, the platform detects changes in the attack surface, enabling security teams to prioritize risks based on their potential impact. This empowers organizations to shift from a reactive to a proactive security strategy, focusing on preventative measures rather than merely responding to incidents after they occur.

An Attack Surface Management platform is an indispensable tool for organizations aiming to fortify their defenses against the evolving threat landscape.

What is Pincher?

Pincher is the future of Attack Surface Management (ASM) that stands at the forefront of cybersecurity innovation. Designed with unparalleled adaptability, Pincher is not just a tool; it's a highly customizable platform that is engineered to meet the unique needs of each client, ensuring that your specific security challenges are addressed with precision and efficiency.

What sets Pincher apart is its scalability and flexibility. Whether you're a small business or a large enterprise, our platform molds to your environment, growing as you grow. Our intuitive interface and advanced analytics are tailored to provide solutions that align with your business objectives, enhancing your security posture while optimizing your resources.

Capabilities

- Advanced Subdomain Enumeration
- Vulnerability Detection
- Password Dumps
- Service Enumeration
- Port Discovery
- Web Application Misconfigurations
- Directory Fuzzing
- Secrets Scanning

Flexibility

Our clients drive their own experience with Pincher. If your attack surface increases as the business grows, we can easily adjust to include the new in scope items. Pincher can be setup to scan monthly, quarterly, annually or ad-hoc. Pincher is most frequently configured to run on nights and weekends.

What Pincher is Not?

Although we think Pincher is pretty great, it does not fully replace the human aspect of penetration testing.

- It is not a penetration test, however, our penetration testers will validate any findings from the tool prior to alerting the customer of a potential vulnerability.
- Pincher is not a vulnerability scanner. Sure, it scans for vulnerabilities, but where it truly shines is the collection and parsing of data for organization that an attacker could abuse.
- Pincher is not available for internal security audits or assessments. It was designed specifically help our clients monitor external perimeter.
- Pincher does have some web application testing capabilities, such as cross site scripting and SSL configuration scanning, it is not intended for targeted web or mobile application penetration testing.

67% of organizations saw their attack surfaces expand in the past 12 months, while 69% were compromised by an unknown or poorly managed internet-facing asset in the past year.*

Results

Since its inception, Pincher has assisted several large and small organizations strengthening their security posture by collecting and aggregating data from external host devices and abandoned domains all while actively monitoring the environment for new CVEs.

- In a real life example, Pincher discovered a .env file on an exposed production server. The file contained credentials that allowed the tester to manually SSH into the server and access a database. This finding prevented a full production environment compromise that would have resulted in a loss of PII and monetary damages to the client.

- For another client, Pincher identified a server that had been stood up after the last discovery scan. The server was utilizing a legacy platform with a known remote execution CVE. Pincher’s automated notification system notified a Brackish penetration tester who validated the finding.

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.*

Source: IBM*

How Does It Work?

Pincher operates by continuously discovering, monitoring, and managing the external facing assets of an organization to identify and mitigate vulnerabilities before they can be exploited by attackers.

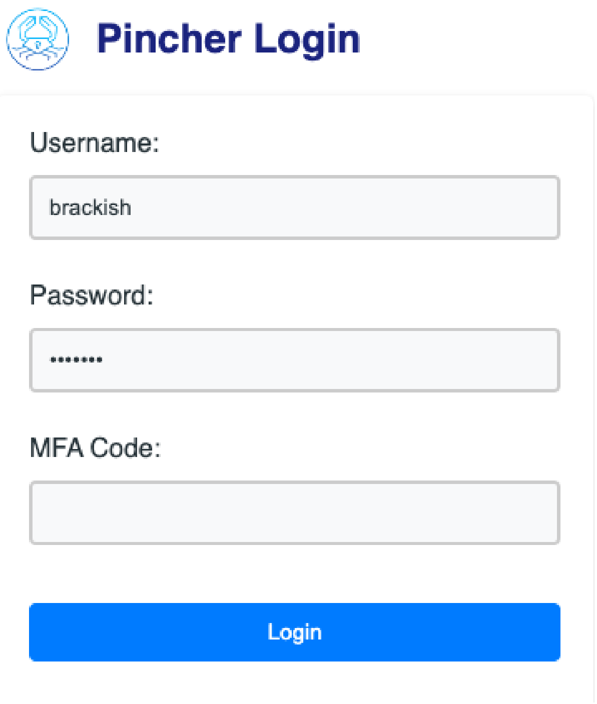
Pincher works a multi-phase approach, the first is discovery, it casts a wide net, obtaining as much data as possible on a target.

Secondly, we have implemented large language models (LLMs) to comb and parse the output from our scanners. Brackish receives alerts on anything of value where one of our penetration testers will review the alert(s) and will conduct a proof of concept assessment to verify the legitimacy of the vulnerability.

The team will then provide a summary report of the finding(s) and immediately alert the client of critical and high severity findings.

While the team focuses on report writing, Pincher continues it's efforts to monitor client attack surface and discover new areas of weakness.

Clients are provided access to their Pincher portal to view data collected, obtain reports and to download password dump files.



Pincher Login

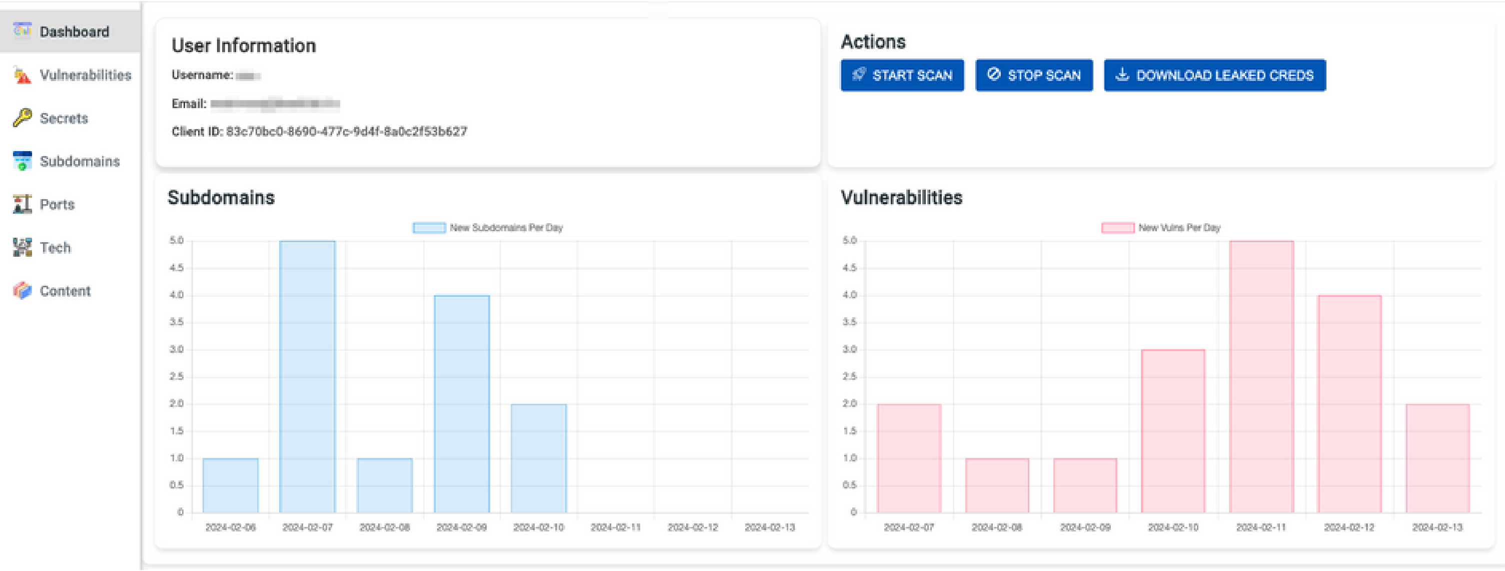
Username: brackish

Password: •••••••

MFA Code:

Discovery

- Enumeration of Domains and Subdomains
- IP Address Mapping
- Vulnerability Detection
- Detecting Web Applications
- Finding Associated Cloud Resources
- Identifying Open Ports and Services



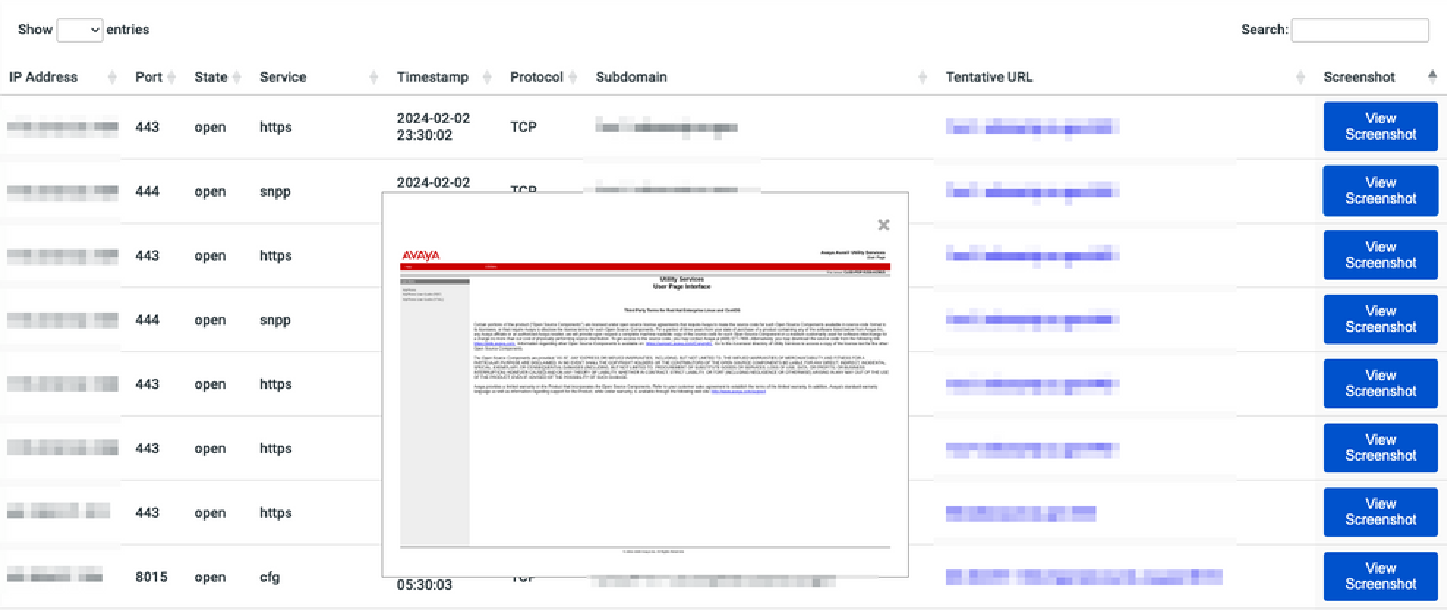
Username: [redacted]

Email: [redacted]

Client ID: 83c70bc0-8690-477c-9d4f-8a0c2f53b627

Parsing

Once assets are discovered, Pincher utilizes artificial intelligence to categorize assets based on type (e.g., web server, VPN, API endpoint) and criticality to the business.

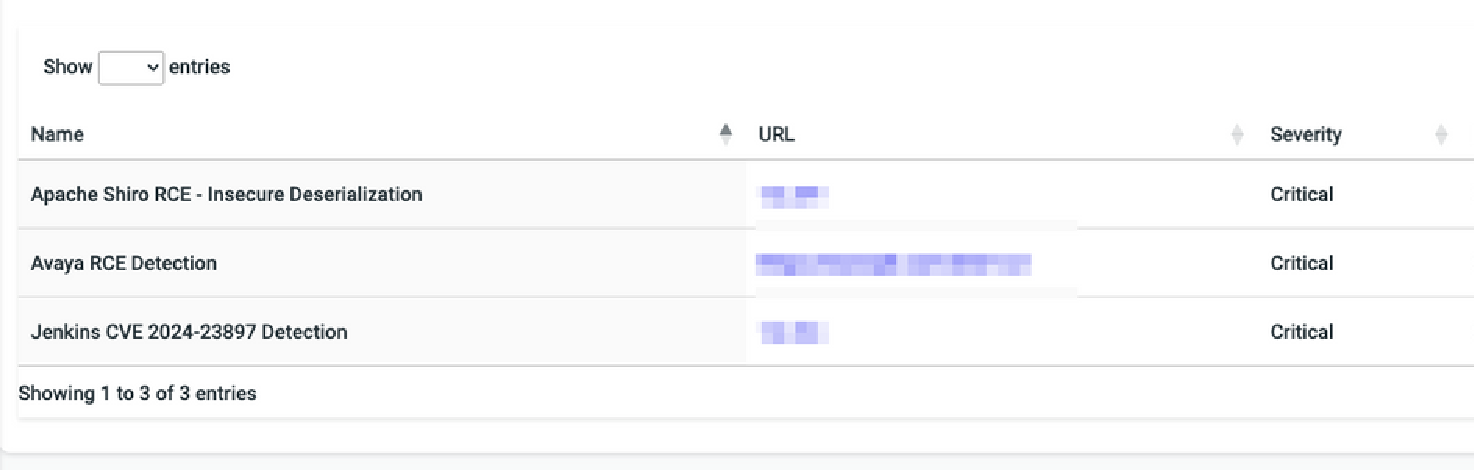


IP Address	Port	State	Service	Timestamp	Protocol	Subdomain	Tentative URL	Screenshot
[redacted]	443	open	https	2024-02-02 23:30:02	TCP	[redacted]	[redacted]	View Screenshot
[redacted]	444	open	snpp	2024-02-02	TCP	[redacted]	[redacted]	View Screenshot
[redacted]	443	open	https				[redacted]	View Screenshot
[redacted]	444	open	snpp				[redacted]	View Screenshot
[redacted]	443	open	https				[redacted]	View Screenshot
[redacted]	443	open	https				[redacted]	View Screenshot
[redacted]	443	open	https				[redacted]	View Screenshot
[redacted]	8015	open	cfg	05:30:03	TCP	[redacted]	[redacted]	View Screenshot

Vulnerability Identification

Pincher scans the assets for known vulnerabilities, misconfigurations, and security weaknesses.

The Brackish Security team manually reviews, confirms vulnerabilities and conducts proof of concept testing to remove false positives



Name	URL	Severity
Apache Shiro RCE - Insecure Deserialization	[redacted]	Critical
Avaya RCE Detection	[redacted]	Critical
Jenkins CVE 2024-23897 Detection	[redacted]	Critical

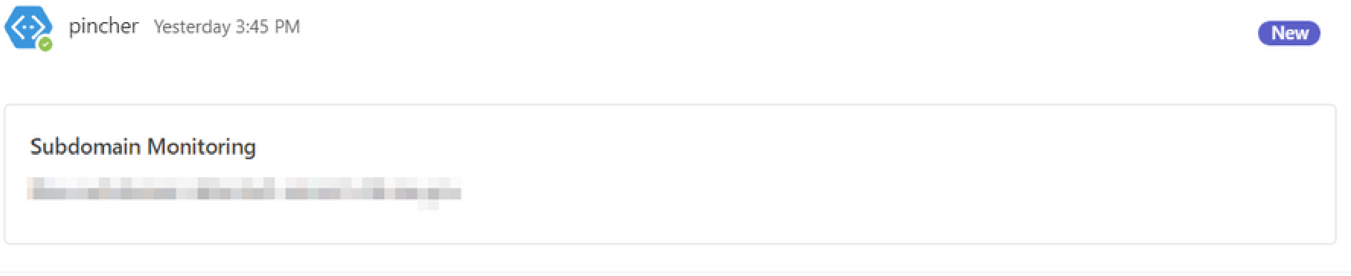
Showing 1 to 3 of 3 entries

Monitoring and Alerting

Continuous monitoring for changes in the attack surface, including the addition of new assets or changes to existing ones.

The Brackish Security team alerts clients as specified in the agreed upon SLA to new findings, vulnerabilities, or changes that require attention.

Brackish receives real-time updates through various channels when new artifacts are discovered.



pincher Yesterday 3:45 PM

Subdomain Monitoring

[redacted]

Reporting

Brackish Security notifies clients immediately if any critical or high severity vulnerabilities are discovered through various channels (e.g. Teams, Email, Text, Slack). Monthly or quarterly reports are provided to clients, including any differences in their attack surface.

Use Cases

Compliance and Regulatory Requirements

Organizations are required to comply with various industry regulations and standards that dictate how data should be protected.

Use Case: ASM platforms assist in maintaining compliance by identifying unprotected assets that could lead to data breaches that would violate regulations like GDPR, HIPAA, or PCI-DSS.

Mergers and Acquisitions

When a company acquires or merges with another, it inherits the acquired company's digital assets and potential vulnerabilities.

Use Case: An ASM platform can quickly provide a comprehensive inventory of the newly acquired digital assets, identify security gaps, and help integrate and secure the expanded attack surface.

Security Posture Assessment and Benchmarking

Organizations need to regularly assess their security posture to understand how well they are protected against potential threats.

Use Case: An ASM platform provides a comprehensive view of an organization's external security posture, allowing it to assess vulnerabilities and misconfigurations, and benchmark its security posture against industry standards and best practices.

Reducing the Attack Surface

An expansive attack surface increases the likelihood of a successful cyber attack.

Use Case: By continuously identifying and classifying assets, ASM platforms enable organizations to systematically reduce their attack surface—either by securing vulnerable assets or eliminating unnecessary ones.

About Us

Brackish Security, LLC was founded by former Big 4 and FAANG security engineers that see security differently. Brackish believes that security is not simply a static snapshot, but an ongoing effort between both you and Brackish. While assessing security, we also take a holistic approach to identifying vulnerabilities.

Continuing education is important for us, that's why our testers have industry standard certifications including the OSCP, OSEP, OSWE, OWSP, CEH, CCNA, CCISO, GSLC, ITIL, PMP, CISSP, A+, Net+, Sec+, and multiple security clearances. Additionally, as proponents of proactive security, we are constantly engaged in independent research and have reported numerous vulnerabilities to organizations worldwide which has resulted in our testers receiving multiple CVEs and bounties. It isn't all about accolades here, though. Part of our process is reaching out to affected organizations and informing them of issues - without the expectation of anything in return. We just want **To Make the Bad Guys Salty!**

Services We Offer:

- Internal/External/Wireless Penetration Testing
- Web Application/API Testing
- Phishing Engagements
- Source Code Analysis
- Vulnerability Assessments
- Mobile Application Testing
- IoT Testing

BRACKISH SECURITY