HALO SECURITY

The Halo Security External Attack Surface Management Platform

See your organization like an attacker

Attackers constantly look for security weak points to exploit. Often, these are the assets that businesses have forgotten about or lack complete visibility into. These assets are likely to have weaker defenses, making them the easiest and fastest to breach.

Halo Security's attack surface management services help organizations eliminate the risk of the unknown. Our platform provides a clear, comprehensive map of web security risks and vulnerabilities across the organization, prioritizing risk by the severity of the threat. This allows security teams to quickly identify and remediate the most urgent issues. Continuous monitoring ensures instant alerts when new issues arise.

Key Features

- Continuous Asset Discovery
- Agentless External Vulnerability Scanning
- Risk-Based Issue Prioritization
- Integrated Manual Penetration Testing
- Customizable Alerting

Gain deep visibility into your full attack surface

Our automated discovery solutions identify and catalog known and unknown domains, hostnames, and IP addresses exposed to the internet.

Contextualize, search, and categorize assets

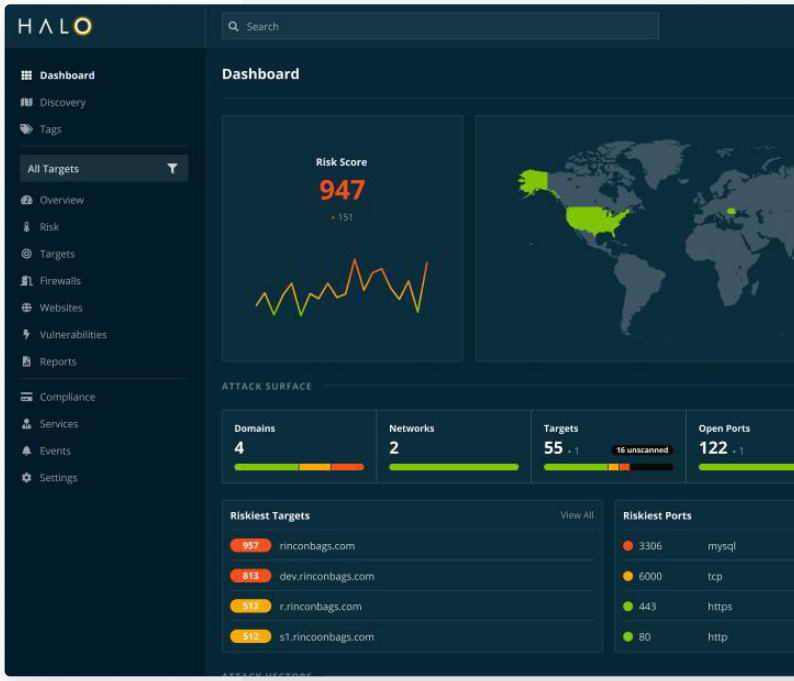
The rich data we collect provides the context needed to understand each asset and automatically group and categorize them for better management.

Uncover risks and vulnerabilities

Our agentless vulnerability detection is tuned for internet-facing assets, detecting known vulnerabilities (CVEs) and other security gaps.

Measure and eliminate risk

Measure and report on your external risk posture, prioritizing the issues that matter most for quick remediation.



Discover Halo Security's suite of attack surface management services.

Attack Surface Discovery

Using a seed domain, our agentless and recursive discovery engine reveals forgotten or unknown assets, eliminating blind spots on your attack surface. Maintain an up-to-date inventory including subdomains, subnets, alive IPs, alternate TLDs, and connected assets.

Firewall Scanning

Gain insight into exposures on your attack surface and identify areas of greatest risk. Scan for open ports, services, products, and risky exposures like SQL databases. Visibility into website and application hosting helps determine necessary controls and scanning requirements. DNS record detection identifies third-party platforms, connected hostnames, and IP addresses.

Website Scanning

Gain deep visibility into your websites and applications. Monitor the security configurations of your TLS certificates, HTTP security headers, third-party scripts, cookies, and download to ensure your websites are protected and properly configured.

Technology Scanning

Detect and catalog the platforms, libraries, software, and systems running on your external assets. Advanced fingerprinting enables precise classification and version detection, ensuring your technology is up to date and accounted for.

Server Scanning

Detect known vulnerabilities and misconfigurations across your servers. Our constantly updated vulnerability database helps you identify the latest threats. Critical vulnerabilities are prioritized for quick remediation.

What You'll Find

- Subdomains & hosts
- Alive IPs
- Connected domains
- Shadow infrastructure

- Ports
- Services
- Products
- DNS records

- Certificates
- Scripts
- Cookies
- HTTP headers

- Third-party software
- JavaScript libraries
- Web hosting platform
- Firewall services

- Known vulnerabilities
- Out-of-date software
- Missing security patches

Add-On Services

Application Scanning

Our Dynamic Application Security Testing (DAST) identifies web application vulnerabilities including OWASP Top 10 Security Risks and SANS CWE TOP 25 Most Dangerous Software Errors.

Dark Web Monitoring

Monitor the deep and dark web for compromised credentials or company mentions. Receive alerts to stay informed and take immediate action to protect your digital assets.

Manual Penetration Testing

Our experienced team of ethical hackers identifies vulnerabilities that automation alone can't find and surfaces them within the platform for a consistent workflow.

Compliance Reporting

Achieve PCI compliance quickly with our integrated PCI compliance reporting. Effortlessly draft and submit reports to us, a PCI DSS Approved Scanning Vendor (ASV), for approval.

What You'll Find

- OWASP Top 10 flaws
- SQL injection
- Cross-Site Scripting

- Leaked credentials
- Leaked emails
- Ransomware mentions

- Business logic flaws
- Chained vulnerabilities
- Application flaws

PCI Security Standards Council
APPROVED SCANNING VENDOR™

Agentless & Production-Safe

We assess your organization from the outside—no installations or configurations required.

Expert Guidance

Our security experts are available to answer your questions and provide the advice you need to succeed.

Integrate With Your Stack

Seamlessly integrate Halo Security with web platforms like AWS or Azure, and workflow tools like Jira or ServiceNow.

HALO SECURITY

Discover how Halo Security can help your organization gain deep visibility and protect your attack surface.

Learn more at **halosecurity.com**

sales@halosecurity.com
(800) 940-2375