Hardenize

HARDENIZE INTERNET ASSET DISCOVERY AND MONITORING

Hardenize provides a managed service that combines automated discovery of Internet and Cloud assets with continuous network, configuration, and security monitoring.

Automated discovery of your network infrastructure globally

Maintaining the visibility of your network infrastructure has never been more difficult. Between rapid technology changes, IT decentralization and outsourcing, and mergers and acquisitions, too much is happening too quickly. Organizations often operate blind or rely on incomplete data because keeping track of the constant changes is too much work.

Key benefits

Fresh data

- Hardenize was built on the belief that information is only useful if it's fresh. We update our data continuously and in real time. Every asset is reviewed on a daily basis.

Runs in the cloud

- There's nothing to install or manage. You can get started in minutes and will always have access to the latest and best version.

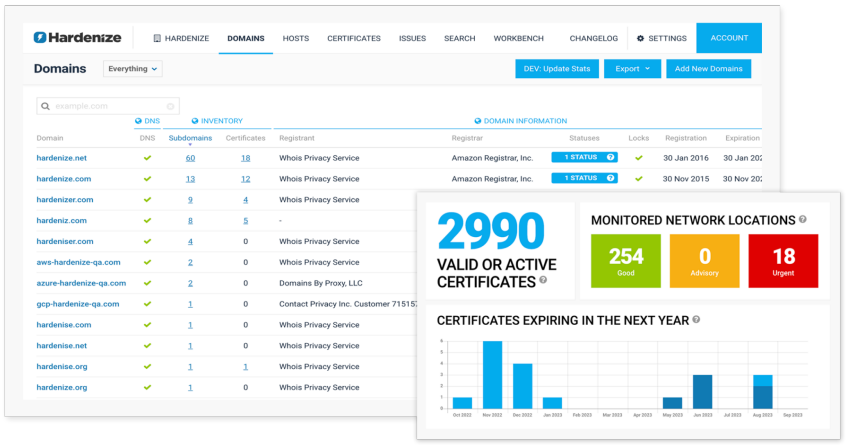
APIs

- Programmatically manage all aspects of your account. Fetch your data when you need it, or get new events in real time.

Private

- Your data is yours. Every Hardenize account is private and fully separate from everything else we host.

In a world where infrastructure changes are made by machines, every minute of every day, Hardenize provides a machine-powered, automated, and continuous discovery service, giving you the ultimate visibility into what resources you're exposing on the Internet. We can find all your assets, including your domains, subdomains, network ranges, Cloud IP addresses and providers, and certificates.



Continuous service and configuration monitoring

We also continuously monitor the discovered assets to understand what services you are providing. At the network level, that means tracking all open ports and server information. Higher up, we collect detailed domain policy and server configuration.

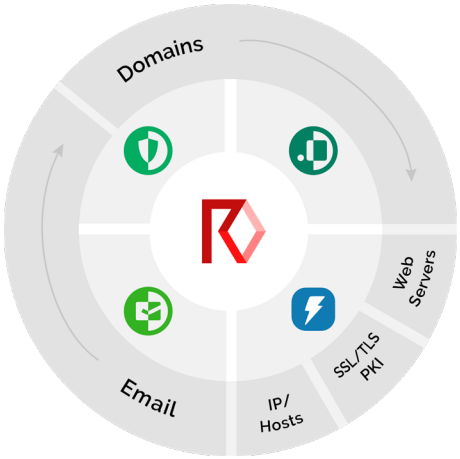
With more than a decade of experience building tools for deep security and network configuration analysis, we support a wide range of standards and services, including everything related to DNS, SMTP, SPF, DMARC, HTTP, HSTS, TLS, PKI, application security, and many other standards. Our coverage includes established as well as emerging technologies.

We assemble all the collected data and transform it into a semantic data model, from which we then build a search engine of your network infrastructure and services.

Technical capability	Description
Automated domain and subdomain discovery	Designed to find the account holder's own infrastructure.
Cloud integrations	Connecting to all three major cloud providers (AWS, Azure, GCP), domain name registrars, infrastructure providers, managed DNS providers and certificate authorities.
Host inventory building	Used as a basis for all our monitoring services and for integration with other tools.
Domain registration monitoring	Reviews registrant information, locks, and expiration.
DNS configuration monitoring	Ensures correct and robust operation. Domain and subdomain takeover protection through detection of dangling DNS issues.
Service configuration monitoring for correctness and security	Most network and security standards (e.g., DNS, SMTP, HTTP, TLS, PKI).
Network range and IP address monitoring	For open ports, banners, TLS, PKI, and services. We scan the top 1,000 ports on a daily basis and test for a variety of popular protocols.
Web application monitoring	E.g. CSP, HSTS, SRI, other security headers, third-party resources.
Certificate inventory	Built via import from our database and combined with those observed via network scanning.
Certificate expiration and revocation monitoring	Including distributed monitoring of your entire estate.
Certificate Transparency monitoring	We monitor CT Logs in real-time, discovering and validating all new certificates that belong to you.
Infrastructure search engine	With a semantic data model and rich query language.
Comprehensive APIs	With support for batch and real-time integration.

A Digital Resilience Platform built for an evolving attack surface

The integration of Hardenize's unique ASM capabilities enables the Red Sift platform to gain a comprehensive view of an organization's digital footprint, allowing customers to better understand and protect their entire critical attack surface area in the face of an ever-evolving threat environment.



Products on the Red Sift platform include:

- **OnDMARC -** blocks outbound phishing attacks
- **OnINBOX -** analyzes the security of inbound emails
- **OnDOMAIN** - uncovers and takes down lookalike domains
- **Hardenize** - discovers and monitors all public-facing assets

RED SIFT

Red Sift's Digital Resilience Platform solves for the greatest vulnerabilities across the complete attack surface. By providing comprehensive coverage of an organization's digital footprint through best-in-class discovery and monitoring, Red Sift enables users to proactively uncover threats within email, domains, brand, and the network perimeter. Paired with sophisticated remediation capabilities, Red Sift provides organizations with the tools to shut down phishing and ensure ongoing compliance with email and web security protocols.

Red Sift is a global organization with offices in North America, Australia, Spain, and the UK. It boasts an impressive client base across all industries, including Domino's, ZoomInfo, Athletic Greens, Pipedrive, and top global law firms. Red Sift is also a trusted partner of Entrust, Microsoft, and Validity, among others.

redsift.com
contact@redsift.com
@redsift

v2.0 | Feb 23