

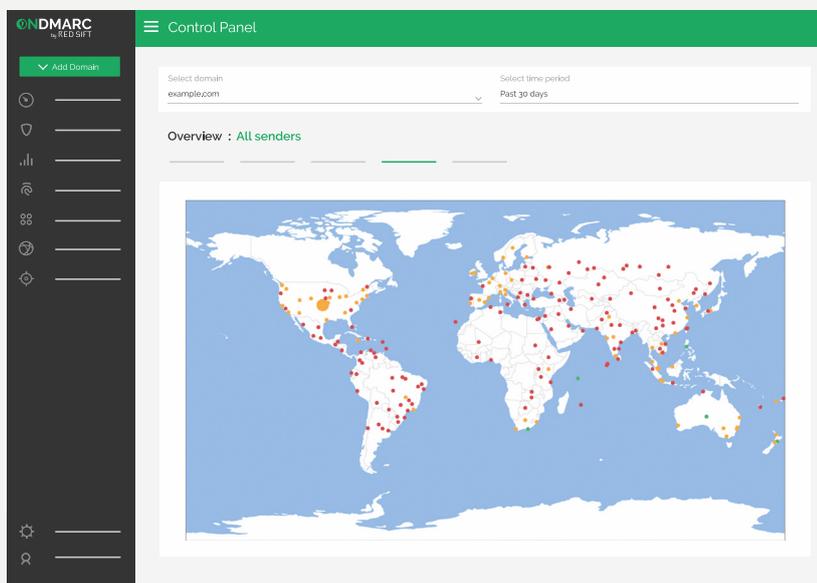
# RED SIFT'S DIGITAL RESILIENCE PLATFORM

RED SIFT

Red Sift's Digital Resilience Platform solves for the greatest vulnerabilities across your complete attack surface, including email, domains, brand, and your network perimeter.

By providing comprehensive coverage of an organization's digital footprint through best-in-class discovery and monitoring, we enable our users to uncover threats within email security, discover lookalike domain abuse, and spot vulnerabilities across their network perimeter. Paired with sophisticated remediation capabilities, we provide you with the tools to shut down phishing, and ensure ongoing compliance with email and web security protocols.

## ONDMARC



Stop domain fraud by blocking **outbound and inbound** email impersonation.

### Key benefits

- ✓ Minimize time to protection
- ✓ Uncover who is using your domain to send unauthorized emails
- ✓ Reduce configuration errors
- ✓ Block phishing attacks by shutting down spoofing and domain fraud
- ✓ Increase email deliverability rates for verified mail sources

## Powerful features



### *Investigate*

Verify your email security setup in seconds.



### *MTA-STS*

Protect emails from man-in-the-middle attacks



### *Dynamic SPF*

Easily and safely overcome the 10 lookup limit without introducing the instability of SPF flattening.



### *Sender Intelligence*

Forensic reporting that delivers granular information on sending sources.



### *Dynamic DMARC*

Manage DMARC, DKIM and SPF records from right inside the OnDMARC interface without needing to access your DNS.

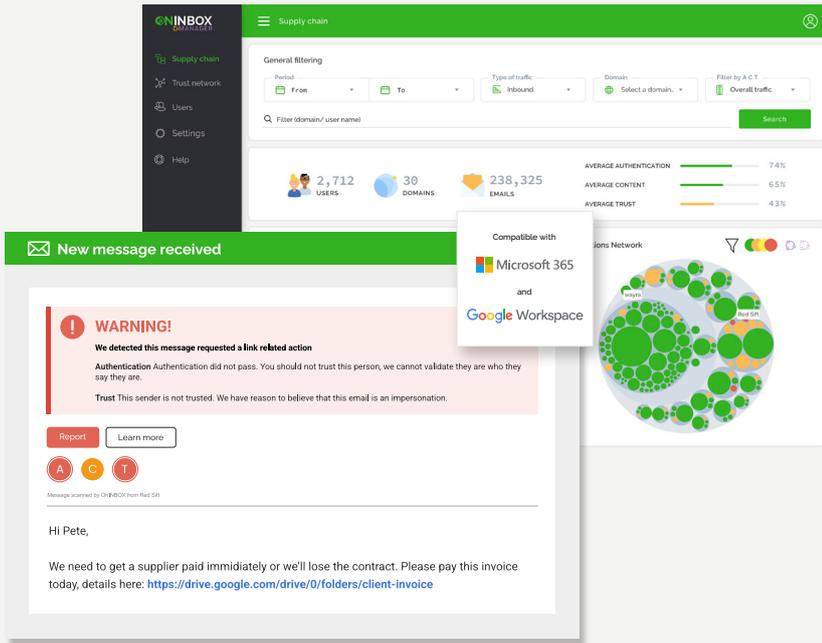


### *BIMI*

Enhance your customers' and clients' brand experience with Brand Indicators for Message Identification (BIMI).

Schedule a meeting with one of our dedicated support team to secure your attack surface.

ARRANGE A DEMO



Protect employees with intelligent **inbound** email threat detection.

## Key benefits

- ✓ Enable your users to spot otherwise impossible to recognize risks at a glance
- ✓ Move away from "train and blame" by empowering your users to confidently interact with email
- ✓ Flag risks to InfoSec teams that bypass your secure email gateway and reach the inbox
- ✓ Identify suppliers who are vulnerable to impersonation and take steps to help them get protected

## Powerful features



### **Out-of-the-box automation**

Rapid deployment for speedy email threat detection.



### **Threats visualized**

In the header of every email, traffic light indicators alert users to the type and level of threats, across all clients, devices, and screens.



### **Deep supply chain insights**

OnINBOX Manager allows InfoSec teams to identify who their organization is talking to and see what email security measures those connections have in place.



### **Customizable warnings**

Add optional text-based banners based on configurable rules.



### **Advanced content scanning**

Natural language processing understands the topic, intent, and level of urgency of the emails your staff receive and warns them of potential threats.



### **Remediation**

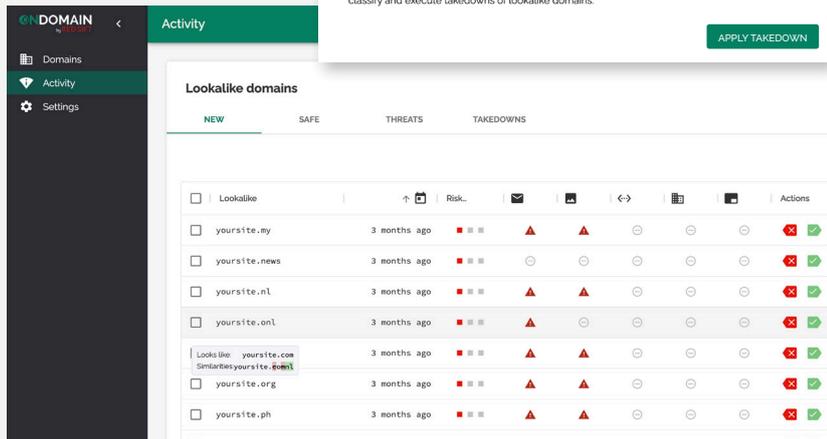
Investigate potential risks prioritized by threat level, then take actions such as marking emails as safe, as a threat, or by blocking and deleting them from employees' inboxes.

**Rentokil  
Initial**

*"Google filters out the malware, OnDMARC protects us from phishing, and ONINBOX is successful in highlighting otherwise impossible-to-spot BEC attacks."*



Peter Shorney, Global Head of Information Security, Rentokil



Uncover and take down lookalike and impersonation domains for enhanced **domain perimeter protection**

## Key benefits

- ✓ See and prevent lookalike attacks
- ✓ Sort threats by their imminence and save time with event-driven alerts
- ✓ Discover and secure legitimate domains that have been forgotten about
- ✓ Defend your brand against abuse and reputational damage
- ✓ Shut down phishing sites using your brand before they're deployed in phishing campaigns to your customers, partners and suppliers

## Powerful features



### Domain and subdomain discovery

OnDOMAIN monitors 150 million newly registered domains and subdomains every day making it easy for you to define and visualize complex domain estates.



### Automated asset discovery and management

Uncover domains that you own that may have been forgotten, parked, or are unknown to IT.



### Machine-vision based logo detection

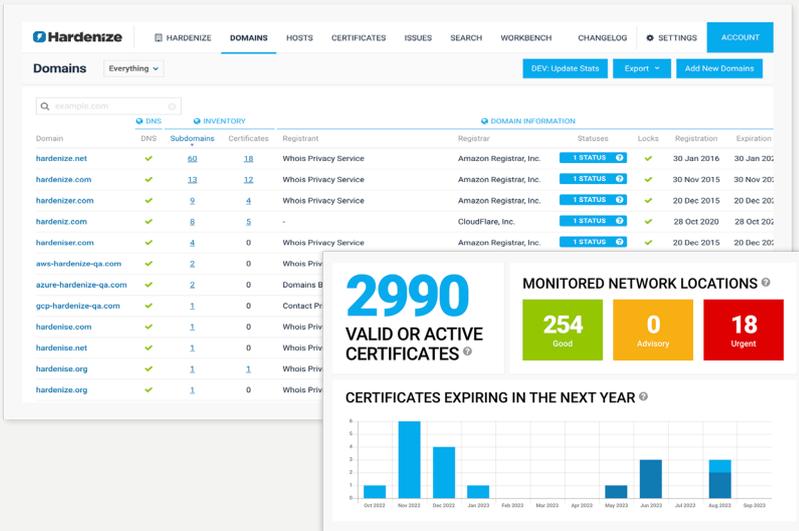
Using computer vision and machine learning, OnDOMAIN scans the web for both legitimate and illegitimate use of an organization's brand assets.



### Integrated takedown

Built-in takedown leverages existing relations with registrars and hosting providers to quickly effect domain takedown.





## Key benefits

- ✓ Quickly find your properties and start monitoring them immediately
- ✓ Find out when certificates are about to expire, avoiding downtime
- ✓ Get a clear breakdown of vulnerabilities so you can prioritize remediation

Continuous discovery and monitoring of network and security configuration, and certificate inventory with support for Certificate Transparency Log analysis.

## Powerful features



### **Comprehensive PKI inventory and monitoring**

Real-time monitoring of newly issued certificates via Certificate Transparency.



### **Discovery of configuration and security issues**

DNS inspection uncovers configuration problems such as dangling DNS problems, and potential subdomain takeover issues.



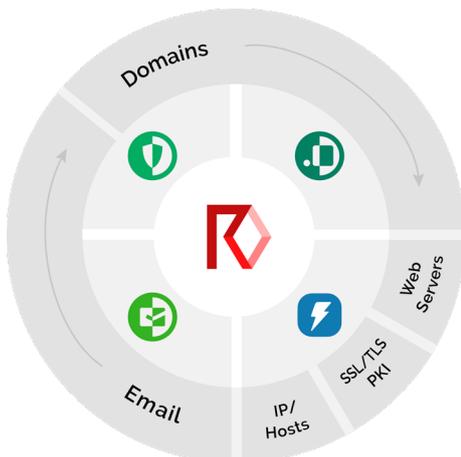
### **Cloud account integration**

Connects to all major cloud providers (AWS, Azure, and GCP), domain name registrars, managed DNS providers, and Certification Authorities providing visibility into assets that otherwise can't be linked to your infrastructure.



### **Semantic search engine**

Discovery and monitoring results are deposited into a semantic search engine that comes with a rich query engine that provides answers about your infrastructure.



## 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.

# The platform advantage

Working in unison, our suite of products provides an integrated, end-to-end solution to close off different avenues of attack and help users manage their business email security and protect their brand reputation.



## In & Outbound Protection with OnDMARC

- Protect all owned domains against exact domain impersonation
- Dynamically manage SPF, DKIM, DMARC, BIMI and MTA-STX
- Increase email deliverability rates for verified mail sources

***Protect your employees, partners and customers***



## Inbound Protection with OnINBOX

- Protect users against BEC attacks with traffic light indicators inside every email
- Investigate and remediate potential risks
- Identify suppliers who are vulnerable to impersonation

***Protect your employees against supply chain attacks***



## Brand Perimeter Protection with OnDOMAIN

- See and prevent lookalike attacks
- Discover, manage and audit the domains you own
- Investigate and take down malicious lookalike sites

***Protect your brand reputation against phishing attacks***



## Network Perimeter Protection with Hardenize

- Quickly find your properties and start monitoring them immediately
- Find out when certificates are about to expire, avoiding downtime
- Get a clear breakdown of vulnerabilities so you can prioritize remediation

***Protect your 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](https://redsift.com)

 [contact@redsift.com](mailto:contact@redsift.com)

 [@redsift](https://twitter.com/redsift)