Simple for customers to adopt and deploy, Red Sift's leading cloud-based technology platform delivers key forensic tooling to reduce the risk of breach for customers, as well as providing Copycat Domain Discovery and Takedown, DMARC email deployment and Cyber Asset Assessment and Remediation.

The benefits of partnering with Red Sift for service providers

Bespoke, personalised approach

As an MSP, we give you the freedom to price and construct services 'powered by' Red Sift. By being flexible in our approach, we can align with your ambitions and provide a high-level of support to match your service offering. Our products are easy to adopt, apply and use since they are agentless and SaaS based.

Three key services which form a platform you can rely on

Red Sift's platform consists of three key applications to keep your clients' cybersecurity posture resilient and protected from various types of attacks:
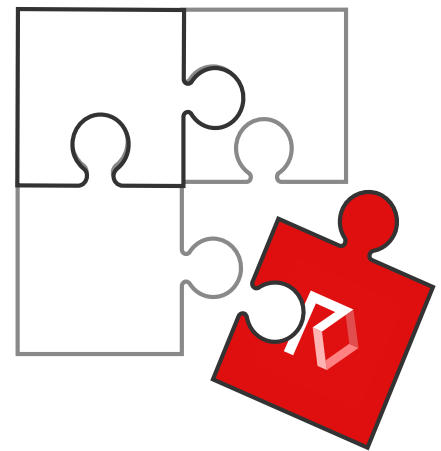
Hardenize

Continuous discovery and monitoring of internet facing assets

> Quickly find your internet-facing assets (domains, hosts, certificates and IPs) properties and start monitoring them immediately.

> Find out when certificates are about to expire in real-time, avoiding downtime.

> Get a clear breakdown of misconfigurations so you can prioritise remediation.

OnDOMAIN

Stop brand impersonation and abuse through domain lookalikes

> See and prevent brand impersonation.

> Discover, manage and audit the domains and subdomains that you own.

> Investigate and take down malicious lookalike sites.

OnDMARC

Stop exact email impersonation attacks through protocol authentication

> Protect all owned domains against exact domain impersonation.

> Dynamically manage SPF, DKIM, DMARC, BIMI and MTA-STS.

> Increase email deliverability rates from verified mail sources.

Market-leading disruptive technologies

Red Sift's portfolio protects organisations from the network perimeter to the inbox. Through cyber attack asset surface management (CAASM), certificate management, domain protection & DMARC, security leaders are able to anticipate and overcome the most important threats. In addition to this, Red Sift's platform is easy to demo, use and understand for your wider team to adopt.

Customers prior to implementing Red Sift	Customers after implementing Red Sift
Siloed security tooling that doesn't interoperate	A unified platform built on REST APIs to fit into their existing stack
Asset discovery is slow and incomplete	Quick, automated discovery of all internet-facing assets
Certificate management is a manual process that is not continuously updated	Automated certificate expiry management to ensure nothing gets missed
Unknown & uninventoried lookalike domains and subdomains present potential for brand abuse	Full visibility of lookalike domains and subdomains so takedown can be actioned before an attack.
Email is unprotected from impersonation opening brand up to risk	Email is protected from exact impersonations with DMARC.

A superior Professional Services opportunity

Red Sift helps your customers build their cyber resilience program via a thorough process:

❯ **Automated Asset Discovery –** Automatically discover external-facing assets across multiple attack surfaces. Red Sift's AI-powered discovery tool finds relationships across assets that other tools miss.

❯ **Continuous Visualisation of your Attack Surface –** Get a consolidated view into all external-facing assets. Have confidence the view is accurate thanks to continuous, real-time updates; no more waiting days or weeks.

❯ **Prioritisation with Ai –** Know what issues require the most urgent attention at a glance. Red Sift ingests thousands of data points to determine what needs to be fixed first so your customer can better run their security team at scale.

❯ **Taking action on what's most important –** Red Sift goes beyond prioritised lists and gives security and non-security teams the information they need to rapidly fix the most important issues.

It is with this process that Red Sift helps your customers anticipate and overcome attacks to their organisations and it closely aligns with Gartner's new Continuous Threat and Exposure Management (CTEM) methodology.

Build flexible services for your end-users with Red Sift

As an MSP, we give you the ability to construct any number of managed services using Red Sift's platform as your foundation. The diagram opposite illustrates just a few ways that some leading customers have leveraged our product offering.
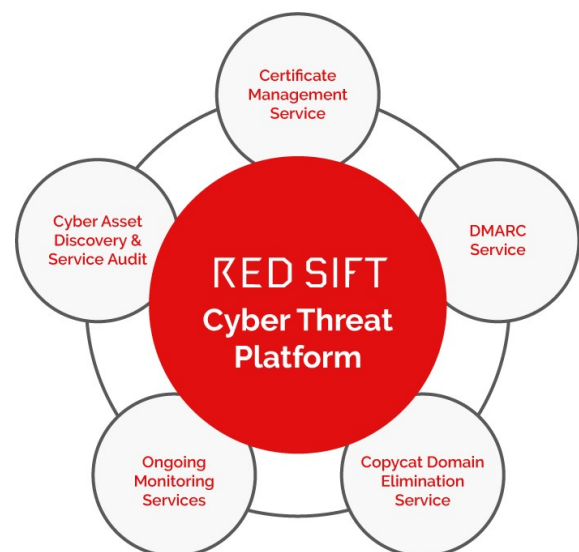
Image: Red Sift's flexible Cyber Threat Platform capabilities

Hands-on enablement to drive early revenue growth

We act as an extension to your business by providing ongoing support and guidance to any of your growth or revenue focused activities. This includes but is not limited to:

❯ In-person training and advice sessions across both sales and technical teams

❯ Full onboarding program backed up by self-paced online training

❯ Account mapping

❯ Call-out days

❯ Demos and enablement tools to grow your business quickly

❯ Marketing collateral and packaged campaigns-in-a-box

❯ Co-branded activities, campaigns, events and webinars

❯ Full access to our newly launched partner portal

❯ A dedicated EMEA team focused purely on channel relations and enablement

❯ A monthly SaaS model with flexible pricing and multi-year discounts

Perfect tool for pre-sales initiative

With Red Sift, you can discover a prospect's internet-facing assets, certificates, domains and DMARC status as part of a pre-sales effort. This allows you to understand the insights the platform can deliver during prospecting in order to provide a highly-personalised presentation to the customer when you land the call.
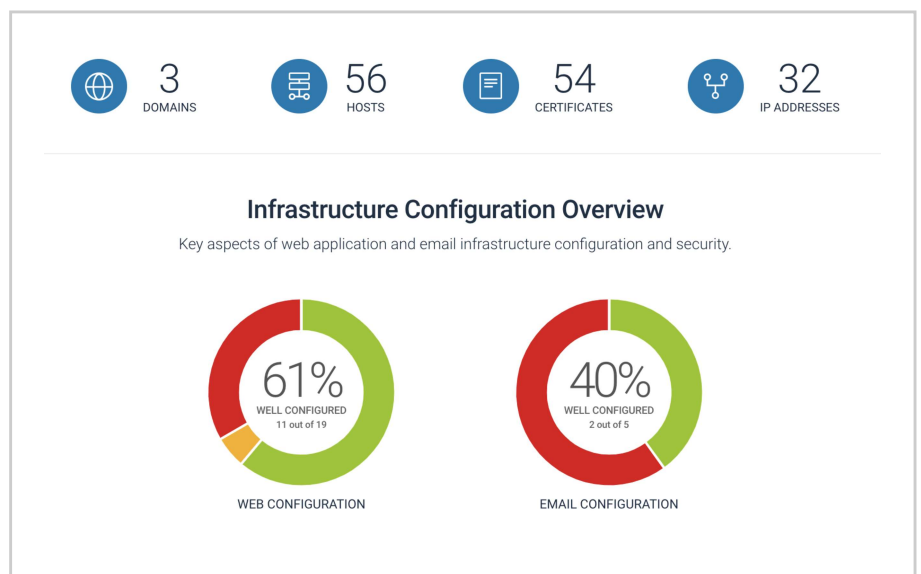

Image: Screenshot of a Hardenize dashboard showing an Infrastructure Configuration Overview

Get In Touch

If you'd like to learn more about the services opportunity with Red Sift, please contact our EMEA channel team **channels@redsift.io**

RED SIFT

redsift.com

contact@redsift.com

@redsift