Chest

Agreement Overview

Red Sift

Red Sift OnDMARC

Available to purchase until 30/03/2028

Red Sift is a UK-owned, cloud-based security platform for TLS certificate management and DMARC email protection. Certificates monitors your certificate estate in real time, flags issues early, and guides you through fixing them before they cause an outage. OnDMARC does the same for email, with customisable reporting and compliance tracking to get you to DMARC enforcement faster. Together, they give organisations of any size clear visibility and stronger control across their certificates and email.

Key Facts

Benefits

- Simple preferential pricing using Jisc banding
- Fixed pricing for 1 or 3 year terms
- OnDMARC: No volume limits, unlimited email traffic included
- Rapid time to compliance, designed specifically for education providers
- Free trial available for OnDMARC, free version available for Certificates

Important Dates

Agreement start: 31 March 2025

Agreement end: 30 March 2028

Invoice date: annually one month in advance of the anniversary of the licence start date.

Commitment Period

Institutions may participate in the Agreement at any time during the agreement period, and are bound by its Terms and Conditions, including payments, until the end of the Institution's chosen Commitment (Licence) Period.

Licence Type

Site licence

Eligible Institutions

Higher and Further Education and Research Councils in the United Kingdom, and to Universities and Colleges of Further Education in the Republic of Ireland. Other organisations supporting education, including research bodies and the public sector, may ask to participate in the Agreement. Chest will liaise with the Supplier about any such requests.

Background Information

The National Cyber Security Centre's (NCSC) announcement that its Mail Check DMARC reporting service for the UK public sector was retired

on 24 March 2025. Red Sift's OnDMARC is one such replacement for organisations to consider. Redsift Certificates were added to the agreement June 2026.

Product Information

Supplier Details

Licensor: Red Sift Ltd, 3rd Floor, 1 Ashley Road, Altrincham, Cheshire, United Kingdom, WA14 2DT. 09240956.

Product Description

Red Sift OnDMARC is a UK-owned, cloud-based solution that stops unauthorised use of email-sending domains. With real-time monitoring, customisable reports, and guided remediation, OnDMARC helps organisations reach DMARC enforcement in weeks, not months. While Red Sift OnDMARC simplifies email security, Jisc Banded pricing makes it accessible to organisations of all sizes.

Red Sift Certificates provides full visibility across your public and private certificate estate. With CT log monitoring, automated expiry alerts, and guided issue remediation, Certificates helps organisations reduce risk from expired or misconfigured TLS certificates.

Redsift OnDMARC

- Red Sift OnDMARC is an automated DMARC application that helps organisations take back control of their email reputation. OnDMARC gives step-by-step implementation guidance, hosted email protocol management, and clear reports on sending services and domain health. For more information, click **here**.



- OnDMARC speeds up time to enforcement by making it easy to audit existing email-sending environments, troubleshoot setups with Investigate, and automate the management of DMARC, DKIM, and SPF with Dynamic Services.
- Hosted MTA-STS stops man-in-the-middle attacks, and OnDMARC is the only end-to-end BIMI solution on the market with integrated VMC provisioning.
- DNS Guardian (available with Premier licensing) is the first DNS configuration monitoring feature of its kind offered among DMARC providers, stopping malicious emails that slip through DMARC defences, including threats from domain takeovers and SubdoMailing attacks. Read more at **Red Sift's blog**.
- With the newly embedded Red Sift Radar LLM, OnDMARC enables security teams to find and fix email-related issues up to 10x faster. For more information, **click here**.

There are 3 levels of OnDMARC available to purchase:

Essentials

This includes:

- Automated DMARC and Outbound Email Authentication Suite
- Unlimited Sending Services
- Unlimited Email Sending Volume
- Dynamic DMARC
- Dynamic SPF with Unlimited SPF Lookups
- 1 year of data history
- Investigate
- Forensics Reporting

- Logs
- API Access
- SAML/SSO
- Chat Support
- Unlimited Platform Users
- Unlimited Parked Domains
- Essentials Support

Enterprise

This includes everything in Essentials and the addition of:

- Dynamic BIMI with one VMC included
- Dynamic DKIM
- Dynamic MTA/STS
- Detailed User Permissions
- Domain Compliance Support - Dedicated Success Engineer
- Dedicated Account Manager
- Quarterly Account Review
- Advantage Support

Premier

This includes everything in Enterprise and the addition of:

DNS Guardian.

DNS Guardian is the first DNS configuration monitoring feature of its kind offered among DMARC providers, stopping malicious emails that slip through DMARC defences, including threats from domain takeovers and SubdoMailing attacks.

If you are unsure which level is most appropriate for your institution and needs, please contact **help@chest.ac.uk**

Redsift Certificates

Red Sift Certificates is a is a cloud-based TLS/PKI visibility and monitoring solution that gives full discovery and oversight across your public and private certificate estate. Its dashboard and continuous discovery simplify PKI oversight, and REST API and webhook integrations connect it to your existing security workflows. Its customer success program and support portal, Sift Space, back every customer with expert help along the way.

- Continuous certificate discovery via CT log monitoring keeps every certificate tracked, across both public and private infrastructure.
- Automated expiry alerts and guided issue remediation help security teams prevent outages and fix misconfigurations before they become incidents.
- Integration via REST API and webhooks connects Certificates to existing SIEM, ticketing, and asset management workflows.
- Role-based access control (Owner, Admin, Observer) gives appropriate access across teams and business units.
- PQC readiness baselining prepares organisations for the transition to post-quantum cryptography.

Supported by the **award-winning Red Sift customer success program** and support portal Sift Space.

There are 3 levels of Red Sift Certificates available to purchase:

Certificates Lite

- Dashboard
- Certificate Inventory (All, Issuance & Revocation History)
- Endpoint Monitoring (limited 443 scan)
- Certificate Transparency (limited)
- Domains & Domain Exclusions (limited)
- API Access (limited)
- Notifications & CT Monitoring Settings (limited)

Certificates Essential

- Dashboard
- Certificate Inventory
- Endpoint Monitoring (Ports 443 and 25)
- Certificate Transparency
- Host Discovery
- Host Assessment
- DNS Inspections
- TLS Security posture (incl. PQ readiness)
- WHOIS / RDAP Lookups
- Domains & Exclusions
- Network Ranges
- API Access
- Notifications & CT Monitoring Settings

Certificates Enterprise
This includes everything in Essential and the addition of:

- Teams & Account Management
- Search API
- Issue Tracking
- Network Scanning (beyond 443 and 25)
- Events
- Integrations & Private PKI (AWS, GCP, Azure, CAs, Cloudflare, CSC, etc.)
- Headless Browser
- Technologies Detection

If you are unsure which level is most appropriate for your institution and needs, please contact **help@chest.ac.uk**

Useful Resources

- For product news and industry insights from the Red Sift team, you can find more information on **their blog**.
- Get the latest news in email security through Red Sift's **Email Security Weekly**.
- Need to understand how best to implement email security protocols? Learn more in **this guide**.
- Improve your understanding of High-Assurance Certificate Transparency Monitoring with **this guide**.

Red Sift Launch Webinar

On the 30 April 2025 Red Sift hosted a webinar to celebrate the launch of their Jisc Agreement on Chest. You can access that webinar by clicking on the below image.



Terms and Conditions

Licensor: Red Sift Ltd, 3rd Floor, 1 Ashley Road, Altrincham, Cheshire, United Kingdom, WA14 2DT. 09240956.

The Chest Order, together with the Licence Terms and Conditions, and any exceptions listed below, create a legally binding contract between your institution, organisation or company and the Licensor. Therefore please read the terms and conditions carefully and only submit a Chest Order if its terms and conditions are acceptable to your institution, organisation or company and you have the authority to make the financial commitment shown.

Licence Type

This licence is subject to the terms and conditions for the **Standard Software as a Service (SaaS) Licence (July 2024)**

Payment Terms

Chest is an Enterprise of Jisc. All Purchase orders must be made out to JISC, One Castlepark, Tower Hill, Bristol, BS2 0JA Payments are due within thirty days of invoice date; recipients of late payments are entitled to interest in accordance with UK statutory provisions.

On receipt of a completed Order, and a Purchase Order (if required by the Institution) made payable to Jisc, Institutions will be invoiced depending on the licence and payment term selected. Invoices are payable within 30 days of the date of the invoice.

- For a one-year licence, the invoice will be for the Agreement Year in which the Licence is signed.
- For institutions signing up to three year agreements, subsequent annual invoices will be sent 1 month in advance of the anniversary of the licence commencement date.

Exceptions to the Terms and Conditions

1. Term 1.1(a) (the definition of Authorised Users) is deleted and replaced by the following text: “Authorised Users” means any person affiliated with the Licensee.
2. An additional Definition is added: “Customer Data” means data and information submitted by or on behalf of Licensee to the Licensors Software.
3. An additional Definition is added: “DPA” means Licensors’ data processing agreement available at https://redsift.com/data-processing-agreement which is incorporated in, and forms part of, this Agreement.
4. Term 2.2 is deleted.
5. Term 3.1(d) is deleted