# Spoofing del dominio, social engineering e spearfishing? Una sola risposta: DMARC

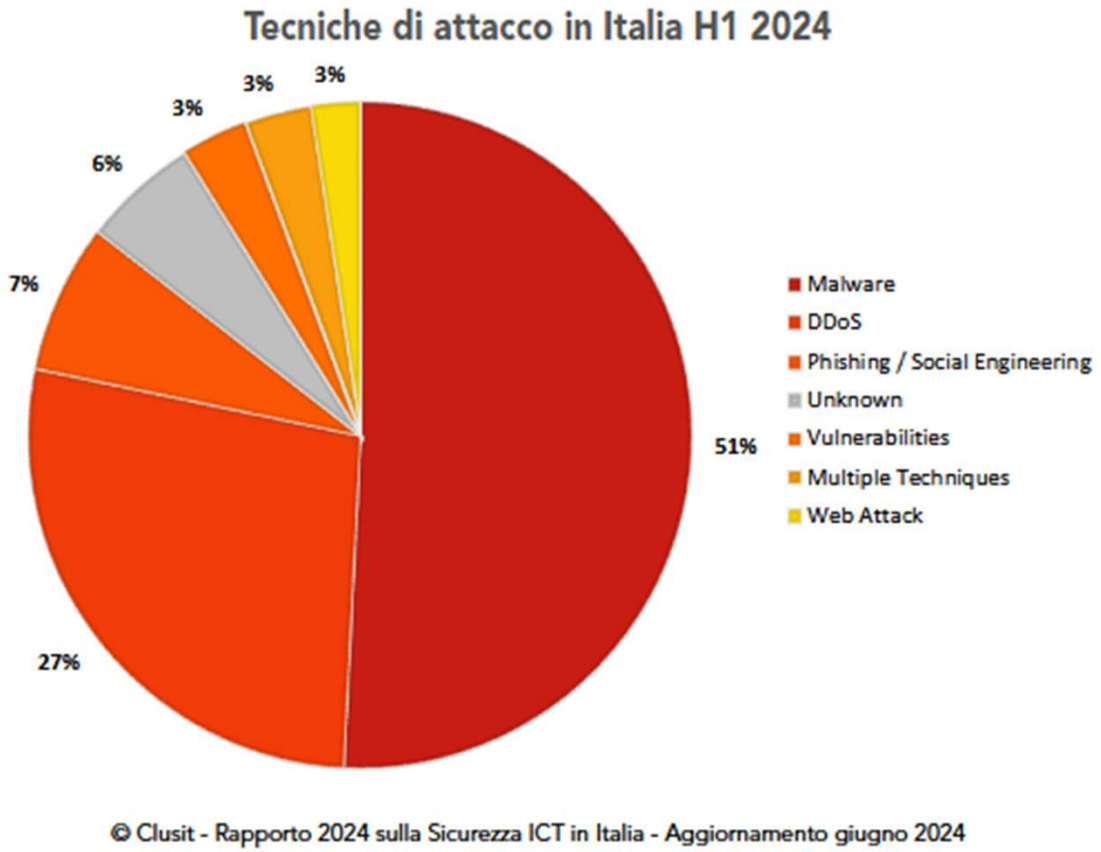
**Angelo Biamonte** | Sales Engineer, *Bludis*
**Jorge Montiel** | Head of Presales – EMEA, *Red Sift*

## Agenda

- **Introduzione e contesto**
  - Social Engineering, spoofing e Phishing: i numeri
  - Tecniche di phishing più diffuse: BEC & CEO Fraud
  - Quanto è difficile riconoscere la mail fraudolenta?
  - Quanto è difficile riconoscere il sito fraudolento?
  - Danni del Phishing all'immagine aziendale
  - Direttive e regolamentazioni
  - DMARC: La soluzione
  - DMARC: Difficoltà di implementazione e manutenzione
- **Red Sift**
  - Overview
  - Platform
  - Moduli
- **Perché Red Sift?**
- **Q&A**

# Introduzione e Contesto

# Social Engineering, spoofing e Phishing: i numeri

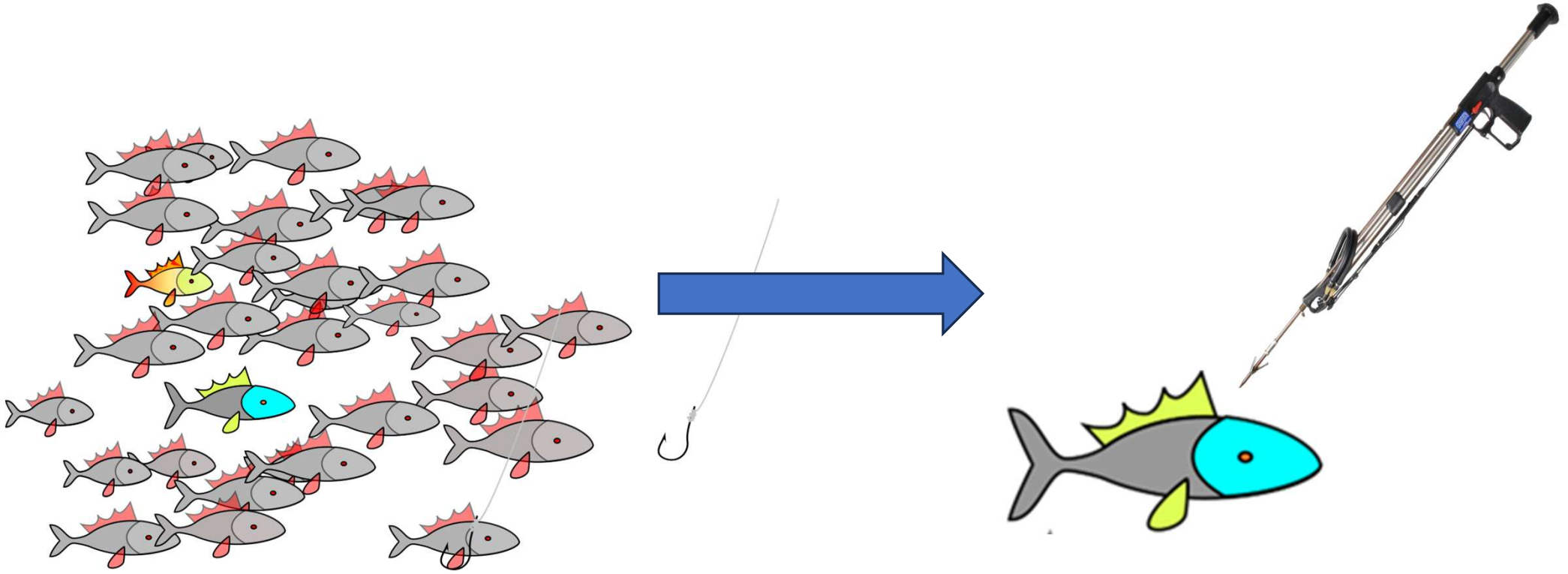



(per quanto riguarda il) malware [...] (è) **la mail come vettore di attacco che la fa ancora da padrone**

© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024


Report sulla difesa digitale Microsoft 2024

# Social Engineering, spoofing e Phishing: i numeri



**Phishing**

**Spear - Phishing**

# Tecniche di phishing più diffuse: BEC & CEO Fraud

**BEC: Business Email Compromise**

**Furto di dati**


**False fatture**


**Frode del CEO**

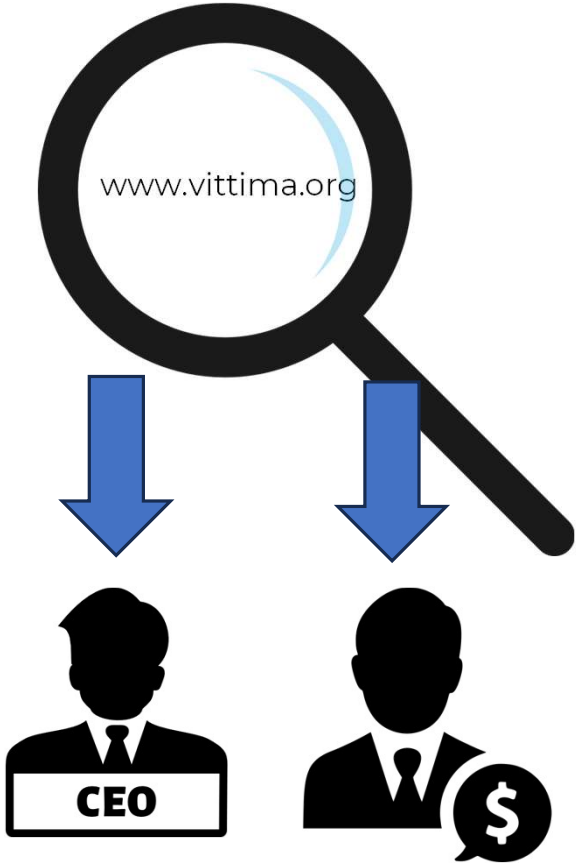
**Human Resources**

**Nuovi Assunti**

**Esecutivi**

**Amministrativi**

# Tecniche di phishing più diffuse: BEC & CEO Fraud




## Frode del CEO

Urgente - Acquisizione Segreta Posta in arrivo ×

**Ceo, della Azienda** <ceodellaazienda@vittima.org> 16:56 (20 minuti fa)

a me

Ciao Amministrativo,

Mi dispiace disturbarti, ma sto per prendere un volo e non so come altro fare, è urgente.
Siamo in chiusura per l'acquisizione di unaacaso.org, ma naturalmente il mercato non deve saperne nulla fino a cose fatte. Ho bisogno che mandi 50k a questo Iban il prima possibile:xxxxxxxxxxxxxx. Mi raccomando non farne parola.

Mr. Ceo

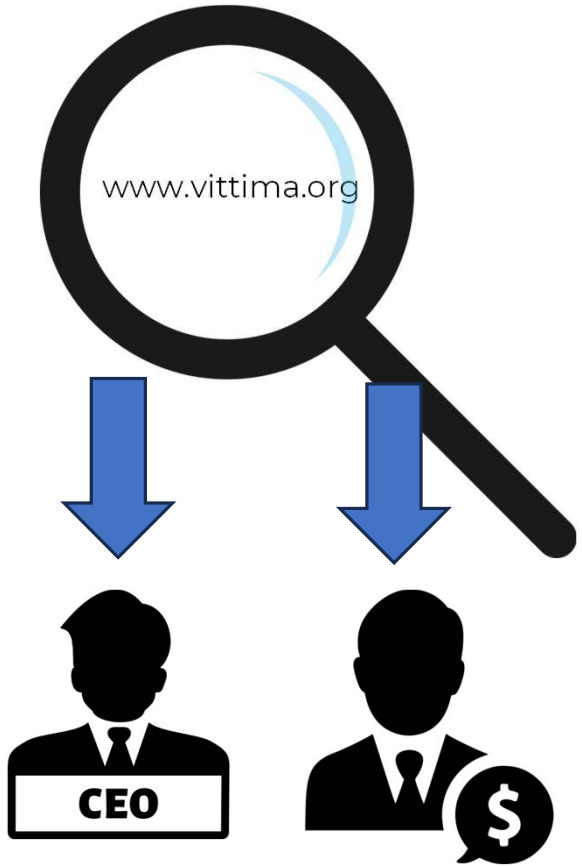
**Ceo della Azienda**
Ceo
ceodellaazienda@vittima.org
Telefono: +3906xxxxxxx
Mobile: +393452xxxxxx

Vittima S.r.l. a socio unico

www.vittima.org

*Roma Piazza di Spagna*

# Tecniche di phishing più diffuse: BEC & CEO Fraud




## Frode del CEO

da: **Malfattore** <Malfattore@malfattore.org>
a: "amministrativo@vittima.org" <amministrativo@vittima.org>
data: 3 mar 2025, 16:56
oggetto: Urgente - Acquisizione Segreta
proveniente da: malfattore.org
firmato da: malfattore.org
sicurezza: Crittografia standard (TLS) Scopri di più
: Importante secondo Google.

**Ceo della Azienda**
Ceo
ceodellaazienda@vittima.org
Telefono: +3906xxxxxxx
Mobile: +393452xxxxxx

Vittima S.r.l. a socio unico

www.vittima.org

*Roma Piazza di Spagna*

# Tecniche di phishing più diffuse: BEC & CEO Fraud

**Frode del CEO**

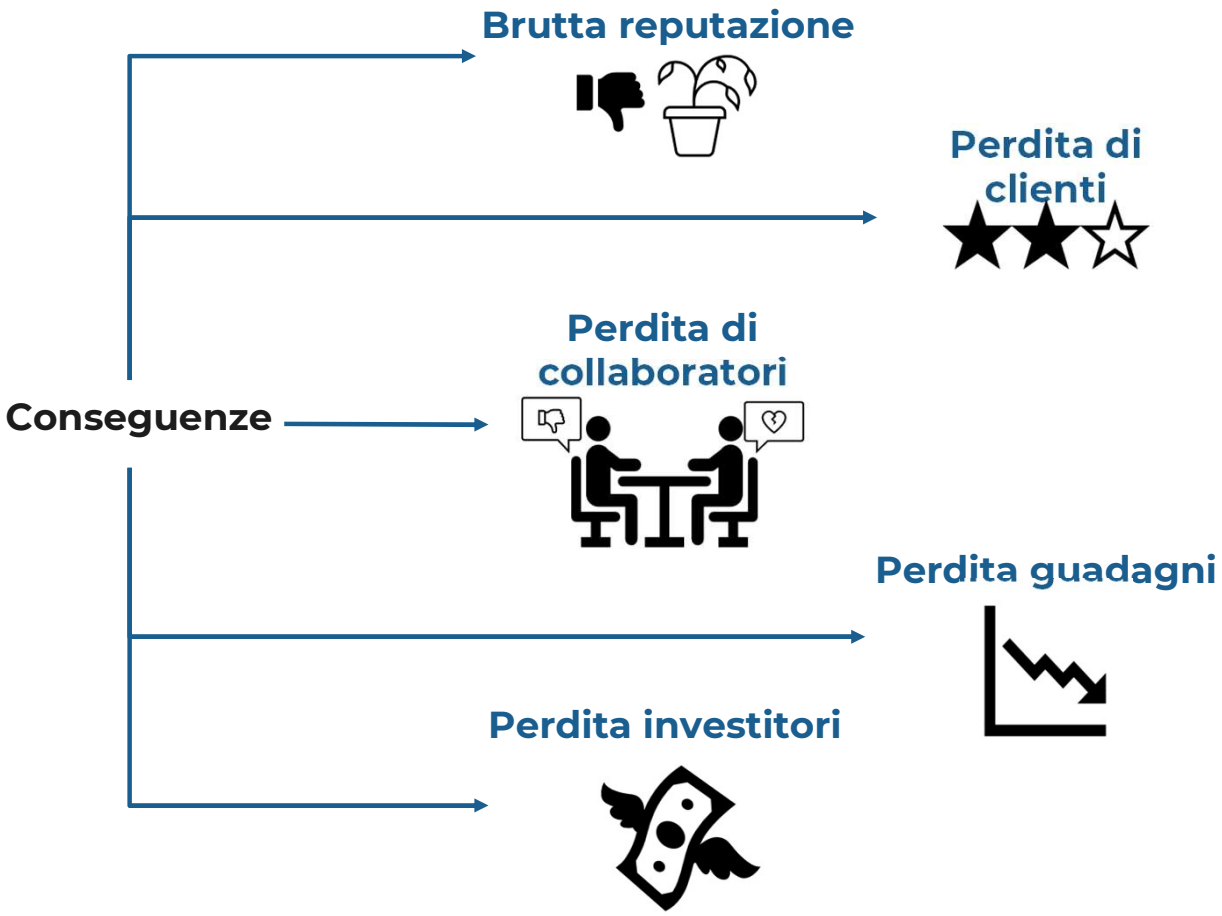

**By-pass verifiche**

**Pagamenti**

**Backdoor e Shadow IT**

**Rubare informazioni**

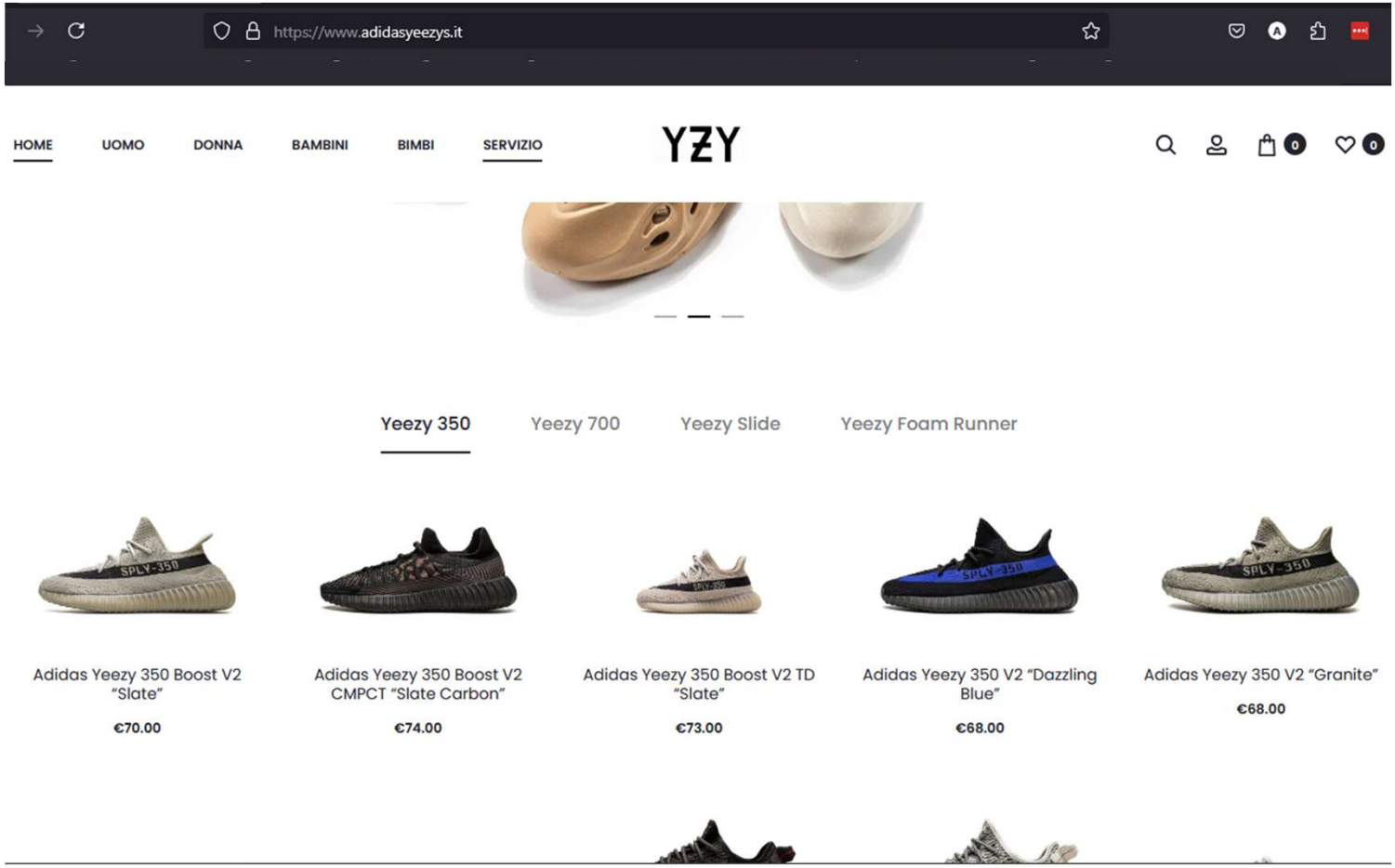
# Danni del Phishing all'immagine aziendale




La grande maggioranza dei consumatori **(83%) afferma che la protezione dei propri dati personali è uno dei fattori più cruciali per la** capacità delle aziende di guadagnarsi la **fiducia**. [...] **80% chiede** anche garanzie che le loro **informazioni personali non saranno condivise**.

https://www.pwc.com/gx/en/issues/c-suite-insights/voice-of-the-consumer-survey.html

# Danni del Phishing all'immagine aziendale



# Quanto è difficile riconoscere la mail fraudolenta?

DHL Shipment Notification : 1942710291 Posta in arrivo × Aggiornamenti ×

**DHL Customer Support** <support@dhl.com> lun 7 dic 2020, 08:39

a me

Notification for shipment event group "Out for delivery" for 07 Dec 20.

AWB Number: 1942710291
Pickup Date: 2020-12-03 14:01:03
Estimated Delivery Date: 2020-12-04 23:59:00

| Ship From: | Ship To: |
|---|---|
| Lancashire, GB | ROME, IT |

EVENT CATEGORY
**07 Dec 20 8:38 AM - With delivery courier - ROME,ITALY**

Shipment status may also be obtained from our Internet site in Italy under http://www.dhl.it/en/express/tracking or Globally under http://www.dhl.com/track

Please do not reply to this email. This is an automated application used only for sending proactive notifications

You are receiving this email because a notification is configured to receive notifications from ProView. If you prefer not to receive future notification email of this type, click here to unsubscribe. Please note this URL is only valid for 1 day.

# Quanto è difficile riconoscere la mail fraudolenta?

angelo.[redacted], Hai (1) messaggio da parte nostra. Work × Aggiornamenti ×

**DHL** KwzKyVlk@zlljxwy.us tramite 187179.irpf9bg05234zau.ca4gybhpo8j30d9.e0snz279g1ibyta.z9qjrl4bvmxsg2a.wildernessexp.com ven 21 f

a me

**CONSEGNA DEL**

**PACCO SOSPESO!**

**Status:** Fermo presso il centro di distribuzione (**Imposta doganale in sospeso**)

**Potrebbero essere applicati costi di consegna**

Il tuo codice di tracciamento:

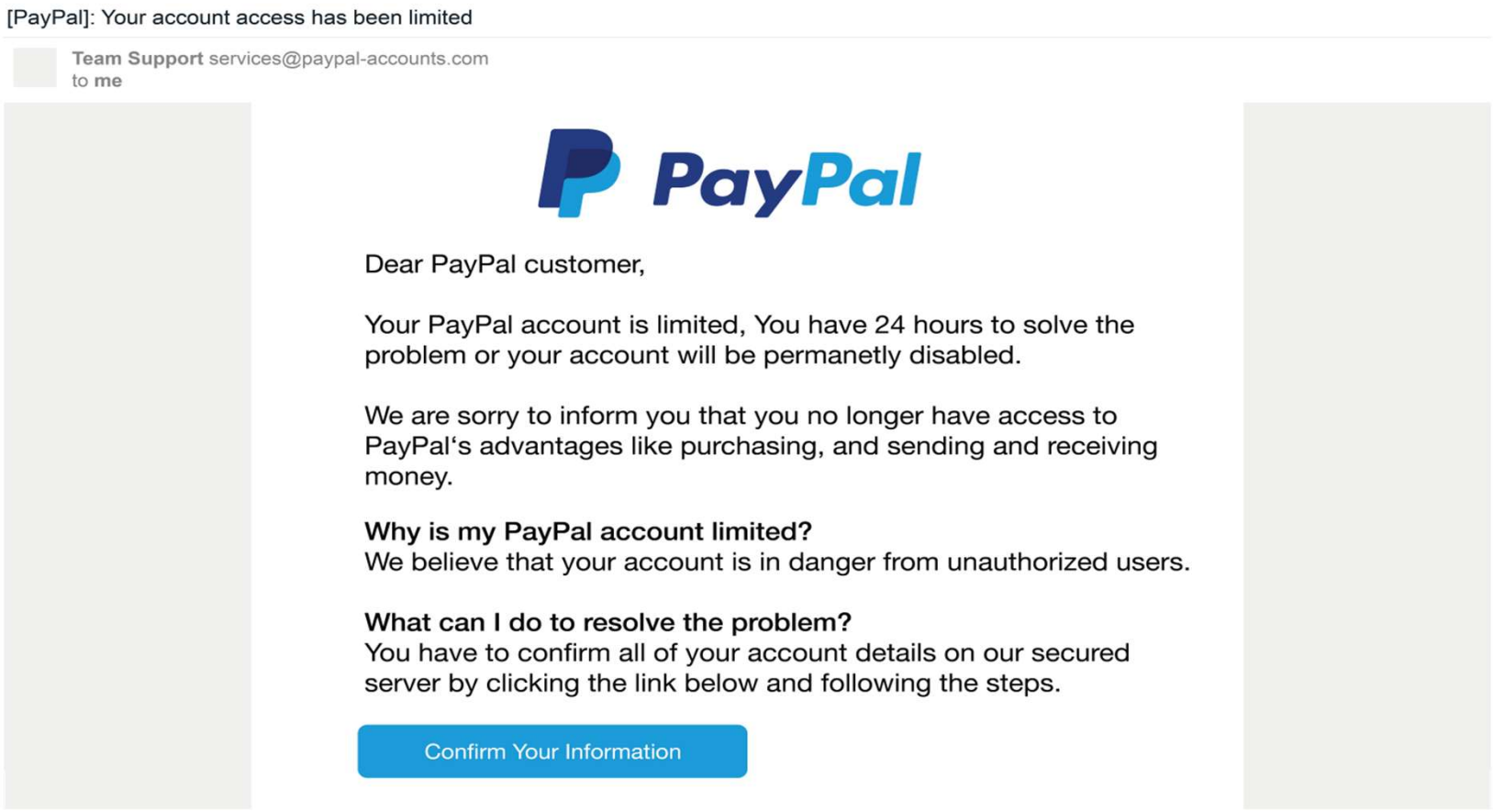
**D541472056IT**

**Programma La Consegna Ora**

If you no longer wish to receive these emails, you may unsubscribe by clicking here.

da: **DHL <KwzKyVlk@zlljxwy.us>**
tramite 187179.irpf9bg05234zau.ca4gybhpo8j30d9.e0snz279g1ibyta.z9qjrl4bvmxsg2a.wildernessexp.com
a: [redacted]
data: 21 feb 2025, 20:25
oggetto: [redacted], Hai (1) messaggio da parte nostra.
proveniente da: 187179.irpf9bg05234zau.ca4gybhpo8j30d9.e0snz279g1ibyta.z9qjrl4bvmxsg2a.wildernessexp.com
sicurezza: Crittografia standard (TLS) Scopri di più

# Quanto è difficile riconoscere la mail fraudolenta?



[PayPal]: Your account access has been limited

**Team Support** services@paypal-accounts.com
to **me**

PayPal

Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

**Why is my PayPal account limited?**
We believe that your account is in danger from unauthorized users.

**What can I do to resolve the problem?**
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

# Quanto è difficile riconoscere la mail fraudolenta?

**PayPal Communications** <no_reply@communications.paypal.com>
a me

mer 13 mar 2024, 09:49

Ciao Marco Ciotola

## Stiamo apportando alcune modifiche ai nostri accordi legali che ti riguardano

È possibile visualizzare le informazioni relative a questi accordi, quando e come vengono modificati e cosa è possibile fare se si desidera rifiutare tali modifiche visitando la pagina Aggiornamenti delle regole su PayPal.com.

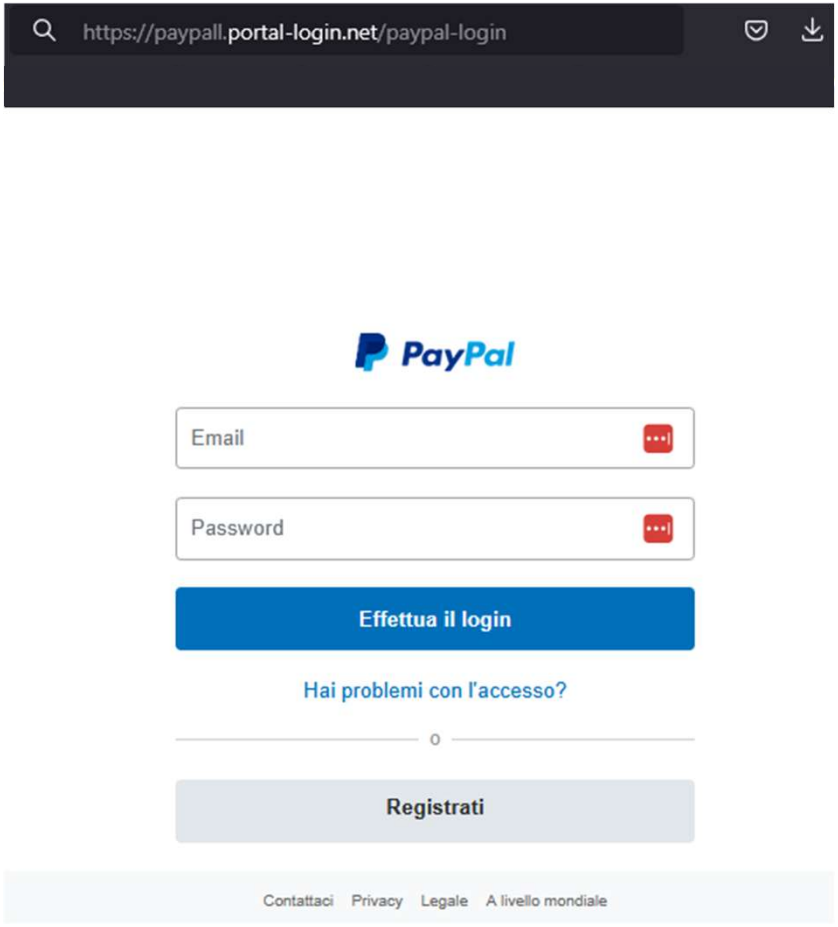
I dati vengono forniti anche nel Centro messaggi PayPal.

**Usi l'app PayPal?**
Accedi all'app PayPal, tocca l'icona Puoi toccare l'icona Impostazioni, quindi toccare il Centro messaggi, oppure selezionare il tuo profilo, tocca "Accordi legali" e "Aggiornamenti delle regole".

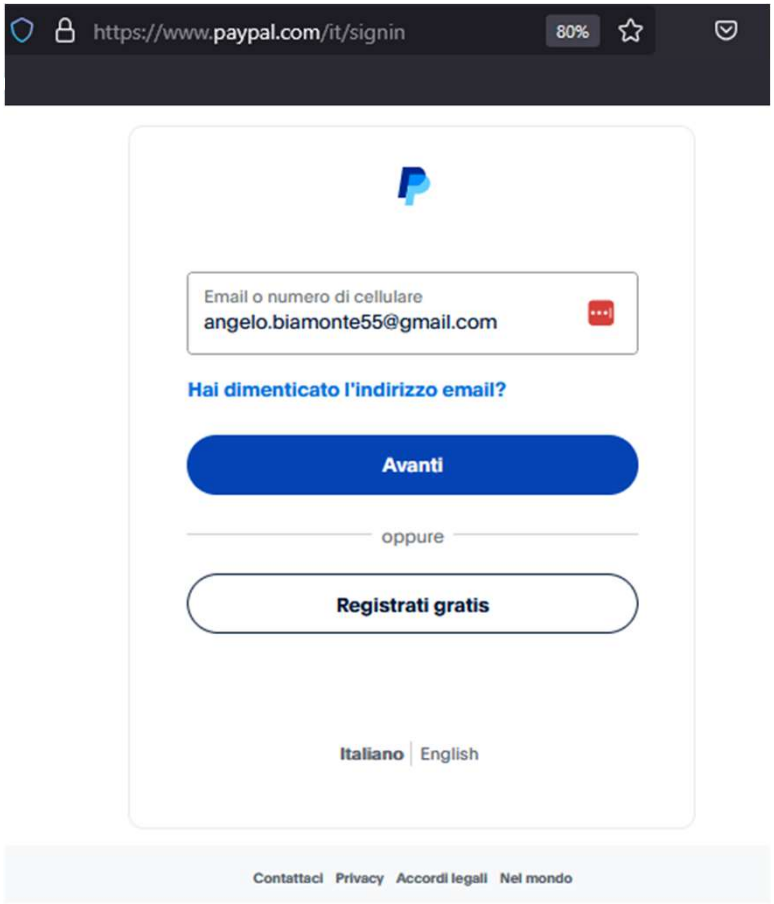
In caso di domande su una qualsiasi di queste modifiche o sul tuo conto, non esitare a contattarci.

Grazie per avere scelto PayPal.

# Quanto è difficile riconoscere il sito fraudolento?



# Quanto è difficile riconoscere il sito fraudolento?



# Direttive e Regolamentazioni – NIS2 & Dora

## Nis2

- Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi
- Best practices di igiene informatica di base e formazione in materia di sicurezza informatica

**What?**

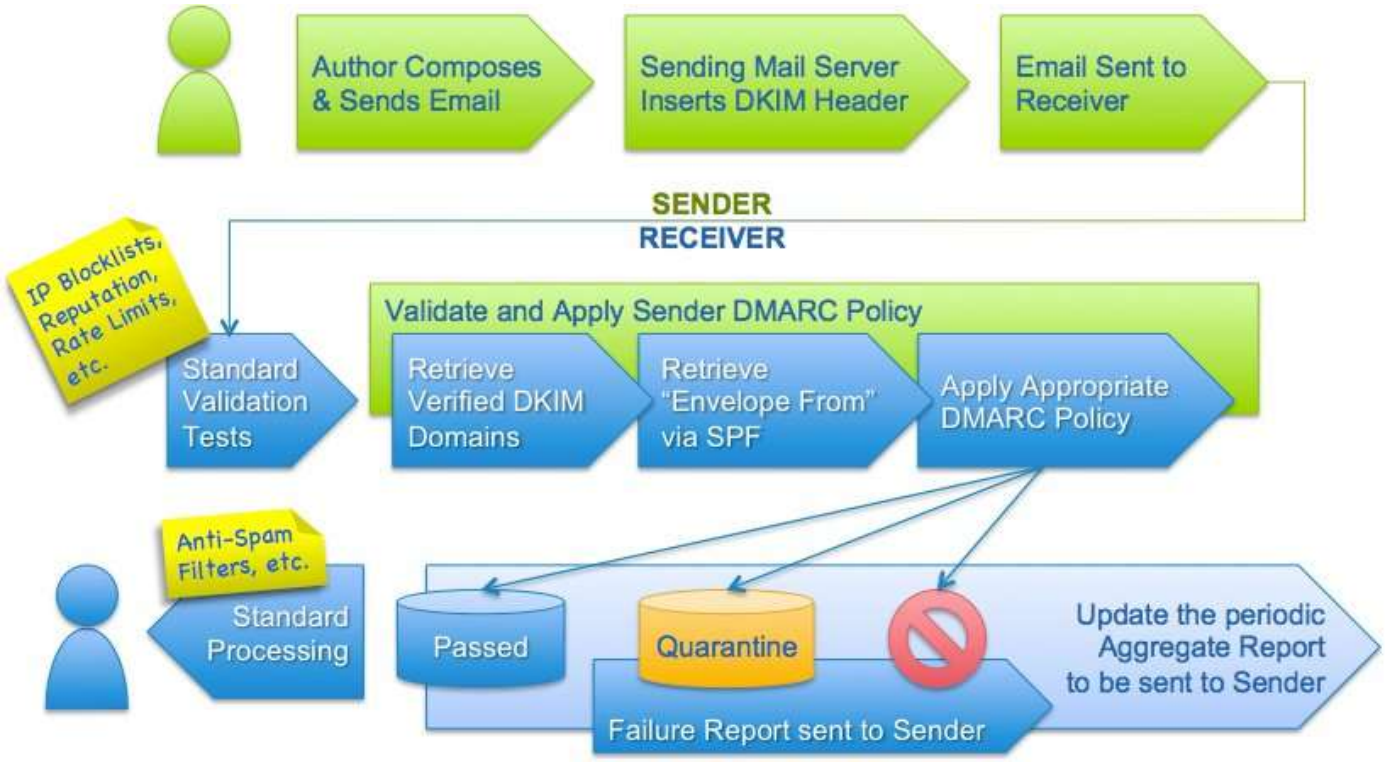
## Dora Act

- Riduzione dell'impatto del rischio ICT applicando le politiche e le misure pertinenti.
- I meccanismi (di cybersecurity) dovrebbero rilevare tempestivamente le anomalie e le attività sospette e rispondere in modo rapido ed efficace per attenuare i rischi.
- Protezione delle comunicazioni digitali contro attacchi e frodi

# DMARC: La Soluzione

## Domain-Based Message Authentication, Reporting, and Conformance

**Come funziona**



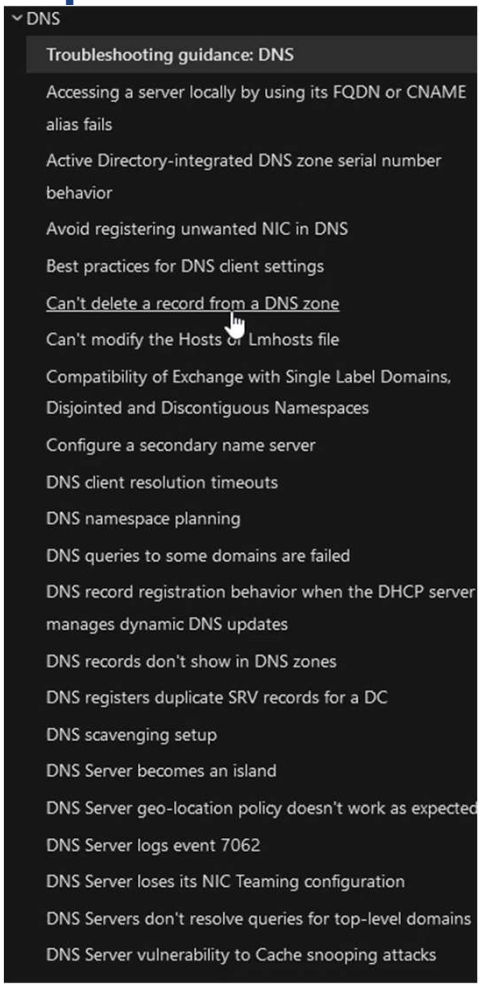
# DMARC: La Soluzione

## Domain-Based Message Authentication, Reporting, and Conformance

**Come si configura**

1. **Distribuisci DKIM e SPF. Devi coprire le basi, prima.**
2. **Assicurati che i tuoi mailer stiano allineando correttamente gli identificatori appropriati.**
3. **Pubblicare un record DMARC con "none" impostato come policy, che richiede i report dei dati.**
4. **Analizza i dati e modifica i flussi di posta in base alle esigenze.**
5. **Modifica i contrassegni dei criteri DMARC da "none" a "quarantine" a "reject" man mano che acquisisci esperienza.**

# DMARC: Difficoltà di implementazione e manutenzione




**Learn / Troubleshoot / Windows / Windows Server / Networking / DNS**

https://dmarc.org/overview/

# DMARC: Difficoltà di implementazione e manutenzione

**Anatomia di un record DMARC**

| Tag Name | Purpose | Sample |
|---|---|---|
| v | Protocol version | v=DMARC1 |
| pct | Percentage of messages subjected to filtering | pct=20 |
| ruf | Reporting URI for forensic reports | ruf=mailto:authfail@example.com |
| rua | Reporting URI of aggregate reports | rua=mailto:aggrep@example.com |
| p | Policy for organizational domain | p=quarantine |
| sp | Policy for subdomains of the OD | sp=reject |
| adkim | Alignment mode for DKIM | adkim=s |
| aspf | Alignment mode for SPF | aspf=r |

## Esempio di record TXT DMARC:

v=DMARC1; p=reject; pct=100; v=DMARC1; p=reject; pct=100;
rua=mailto:1234@inbox.ondmarc.com,mailto:dmarc@example.com;
ruf=mailto:1234@inbox.ondmarc.com,mailto:dmarc@example.com;

https://dmarc.org/overview/

# DMARC: Difficoltà di implementazione e manutenzione

## Esempio report DMARC

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>example.com</org_name>
    <email>dmarc-reports@example.com</email>
    <report_id>123456789</report_id>
    <date_range>
      <begin>1705795200</begin>
      <end>1705881599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>192.0.2.1</source_ip>
      <count>25</count>
      <policy_evaluated>
        <disposition>reject</disposition>
        <dkim>pass</dkim>
        <spf>fail</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
        <result>pass</result>
      </dkim>
      <spf>
        <domain>example.com</domain>
        <result>fail</result>
      </spf>
    </auth_results>
  </record>
  <record>
    <row>
      <source_ip>198.51.100.2</source_ip>
      <count>10</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
```

# About Red Sift

A suite of cybersecurity applications built on a unified, internet scale platform.

Rapid deployment SaaS apps, API-led for easy integration.

Proactive, continuous and automatic interoperable applications.

**Offices in North America, Australia, Spain, Germany and the UK**

**120+ employees**

**$69.8 Million investment**

SANDS CAPITAL

HIGHLAND EUROPE

iqt IN-Q-TEL

RED SIFT

RED SIFT OnDMARC | RED SIFT BRAND TRUST | RED SIFT ASM | RED SIFT CERTIFICATES

Your data sources

Cloud assets

Domains

Certificates

RED SIFT PULSE

RED SIFT RADAR

**Shared data layer**

**Unified asset inventory**

**Narrow, generative AI applications**

**Redundant & scalable cloud architecture**

**API-first foundation**

Red Sift data sources

- Email authentications
- Spam trap feeds
- CT Logs
- Domain and subdomain registrations
- Passive DNS & DNS records
- Who is records
- Zone transfers & zone file uploads and more!

Integrate with all your tools, including

Email

SOC Tools

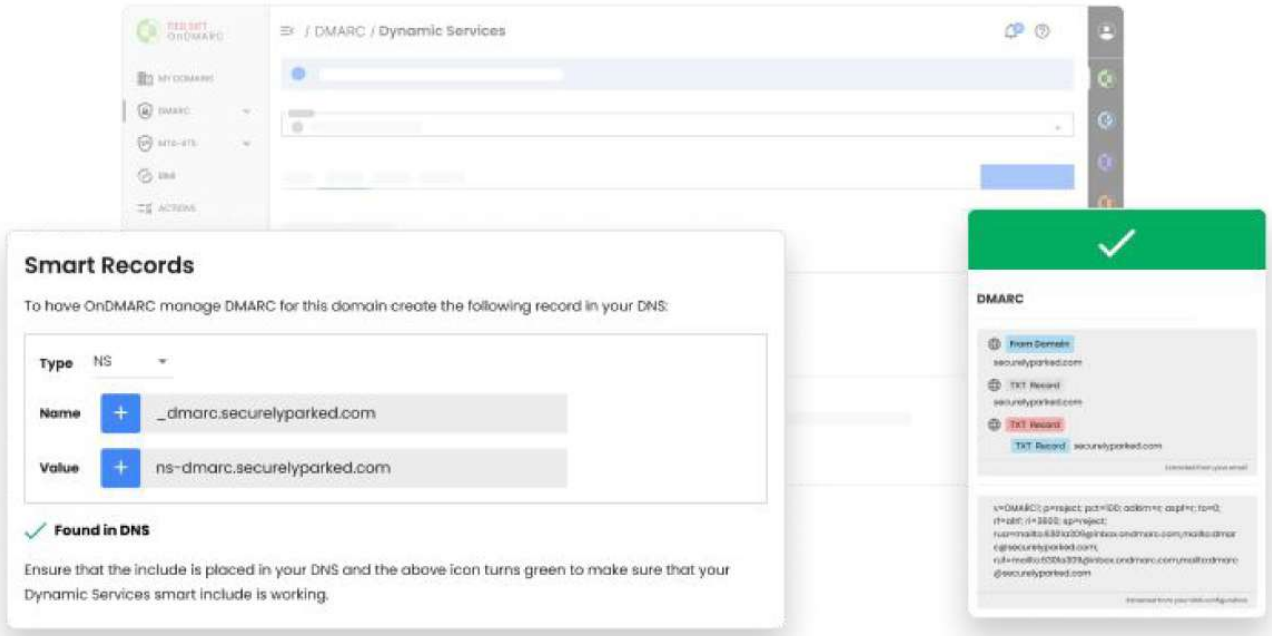
Alerts & Ticketing

RED SIFT
OnDMARC

**Award-winning, cloud-based DMARC, DKIM, SPF and MTA-STS configuration and management platform**

## Simplify management of SPF, DKIM, DMARC & MTA-STS

Make a **one-time DNS change and manage all of your email authentication from OnDMARC's UI**.
Save time, avoid manual configuration
errors and quickly add, authenticate or
remove services.

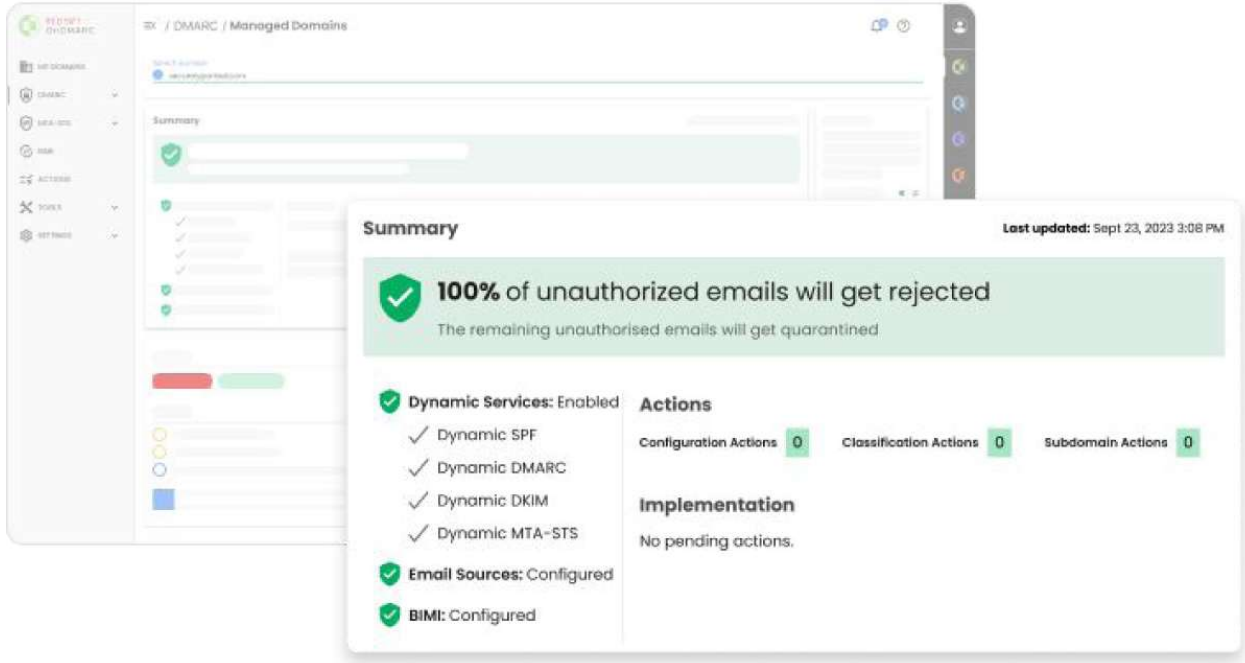


RED SIFT
OnDMARC

**Award-winning, cloud-based DMARC, DKIM, SPF and MTA-STS configuration and management platform**

## The fastest path to DMARC enforcement

Our customers see a **6-8 week average time to full DMARC enforcemen** (p=reject or p=quarantine) including large enterprises with broad networks of sending domains.

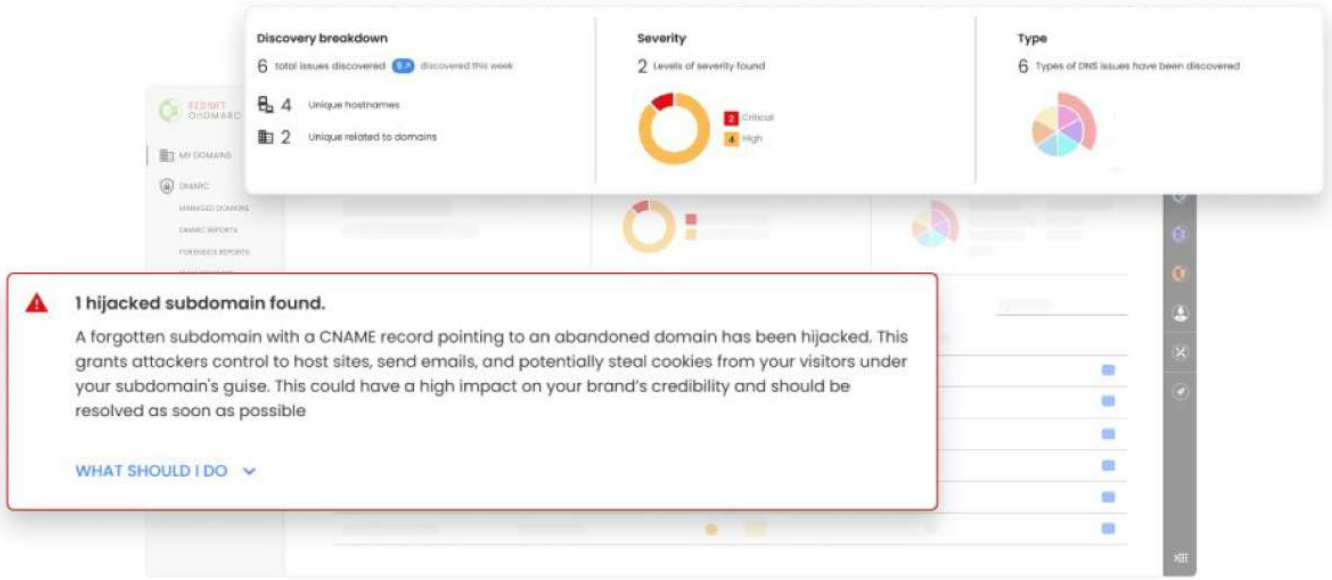


RED SIFT
OnDMARC

**Award-winning, cloud-based DMARC, DKIM, SPF and MTA-STS configuration and management platform**

## DNS Guardian

Ensure better hygiene with **continuous monitoring of your DNS configuration** to prevent SubdoMailing, dangling DNS, and CNAME takeovers.

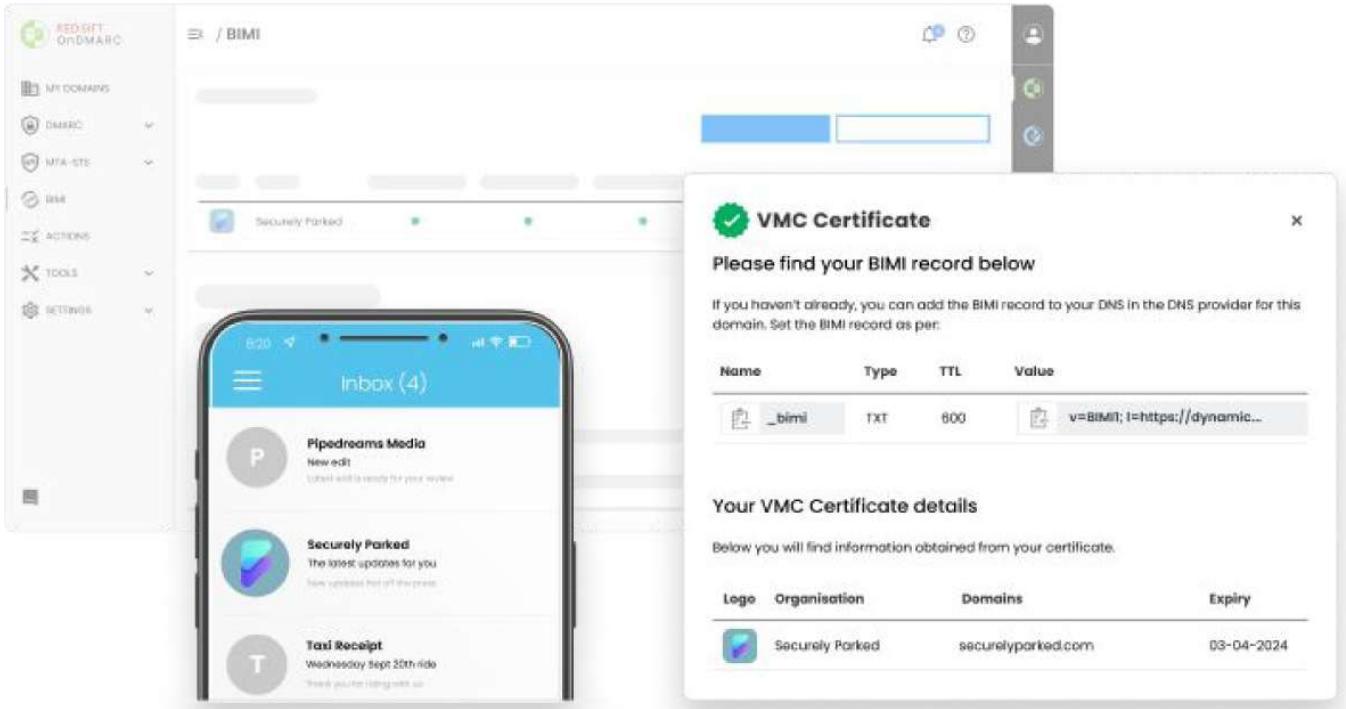


RED SIFT
OnDMARC

**Award-winning, cloud-based DMARC, DKIM, SPF and MTA-STS configuration and management platform**

## Boost brand recognition and deliverability with BIMI

**Red Sift OnDMARC** is the only BIMI solution on the market with integrated
VMC provisioning. **Improve open rates
by 39% and increase brand recall by
44%**.

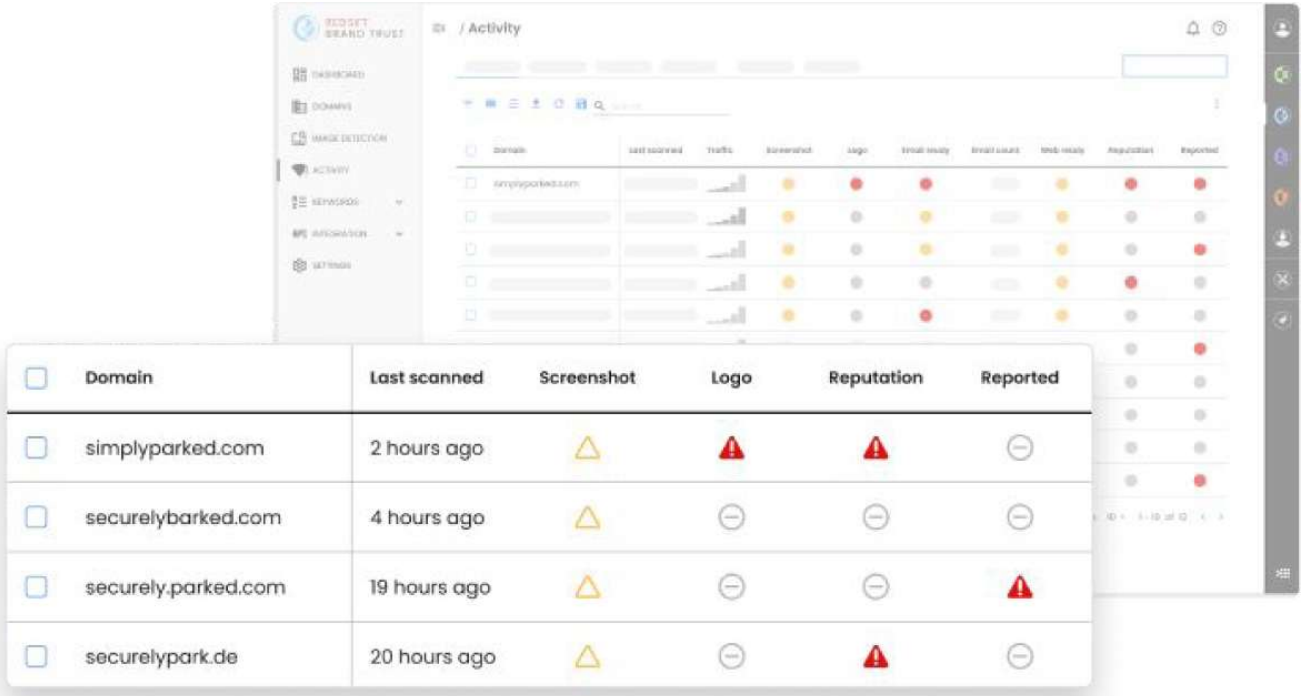


RED SIFT
BRAND TRUST

**Unmatched, AI-driven brand impersonation discovery and monitoring**

## Quickly determine a domain's risk level

Deep DNS query information and metadata are surfaced for every potential lookalike domain to determine
which sites are most likely to be fraudulent.

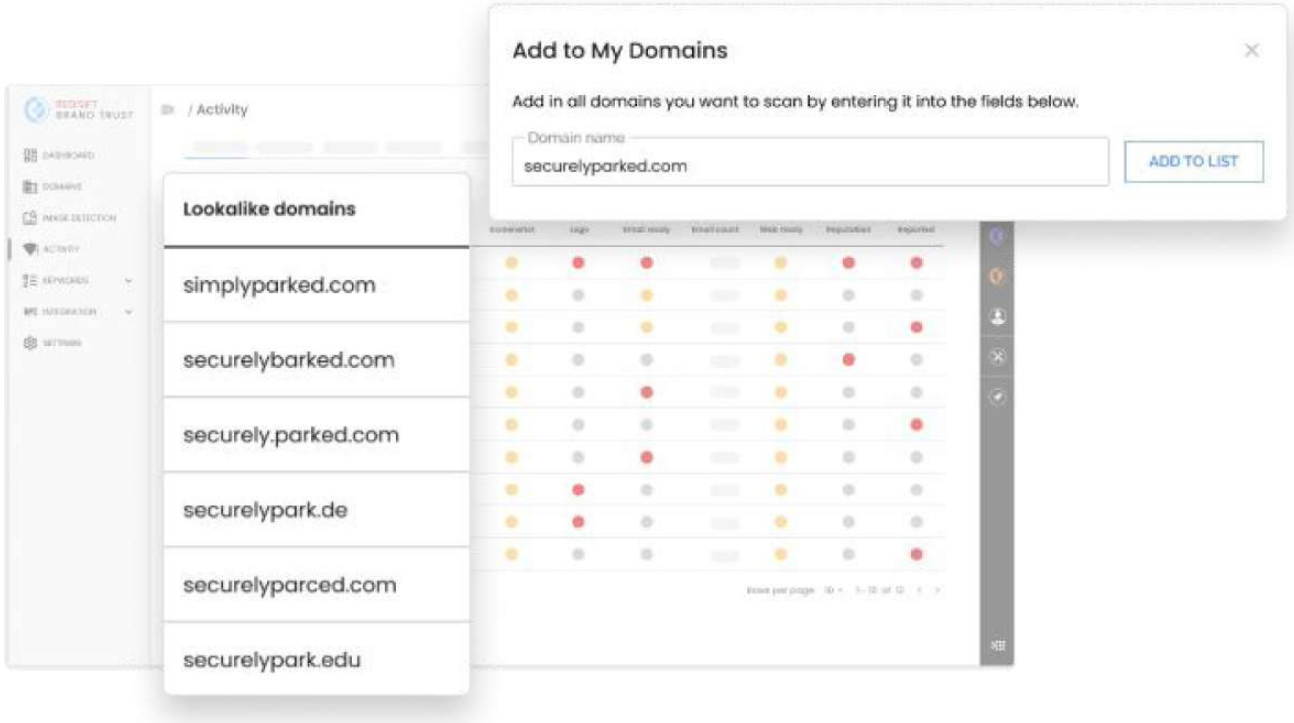


RED SIFT
BRAND TRUST

**Unmatched, AI-driven brand impersonation discovery and monitoring**

## Leverage unmatched discovery power for your brand

Begin **with a single URL and get a complete picture of your brand**.
Proprietary name-matching algorithms
find potential lookalike domains in real-time.

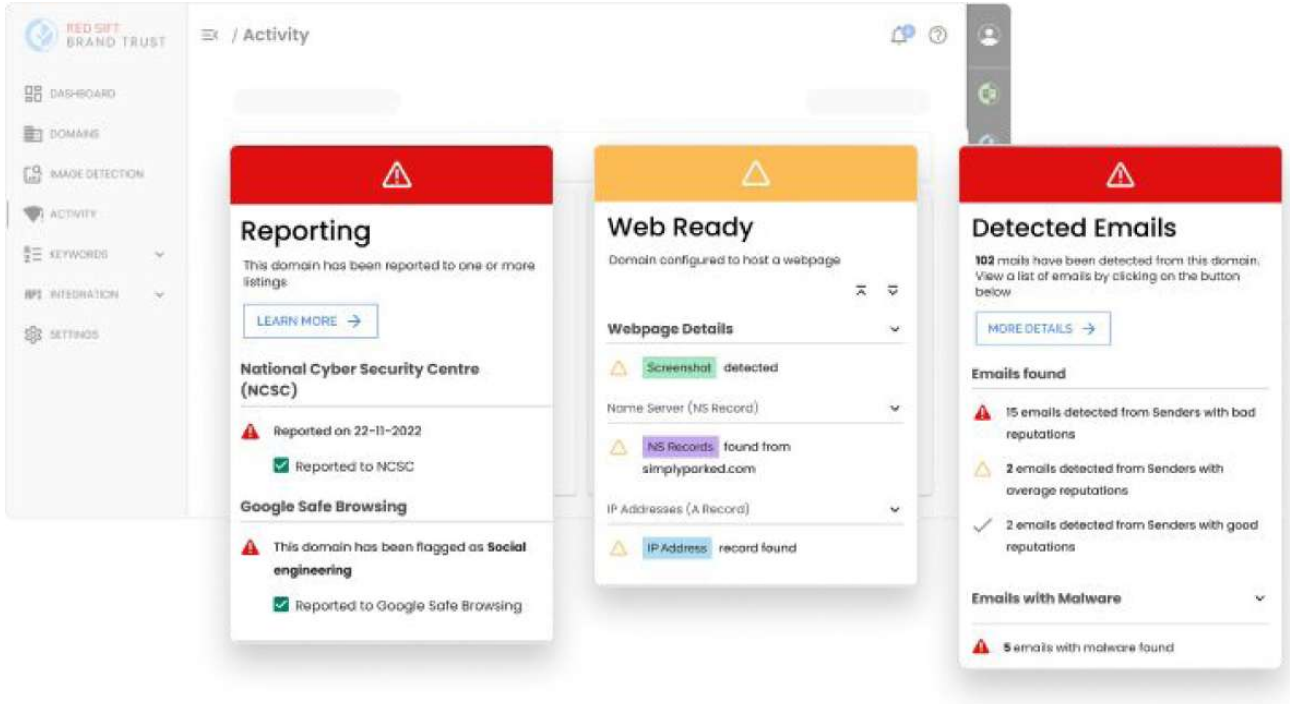


RED SIFT
BRAND TRUST

**Unmatched, AI-driven brand impersonation discovery and monitoring**

## A unified view for every domain

WHOIS data, rasterized web snapshots,
certificate registration, DNS signals, live
spam data, and more are surfaced on
every domain and refreshed daily to drive informed decisions.

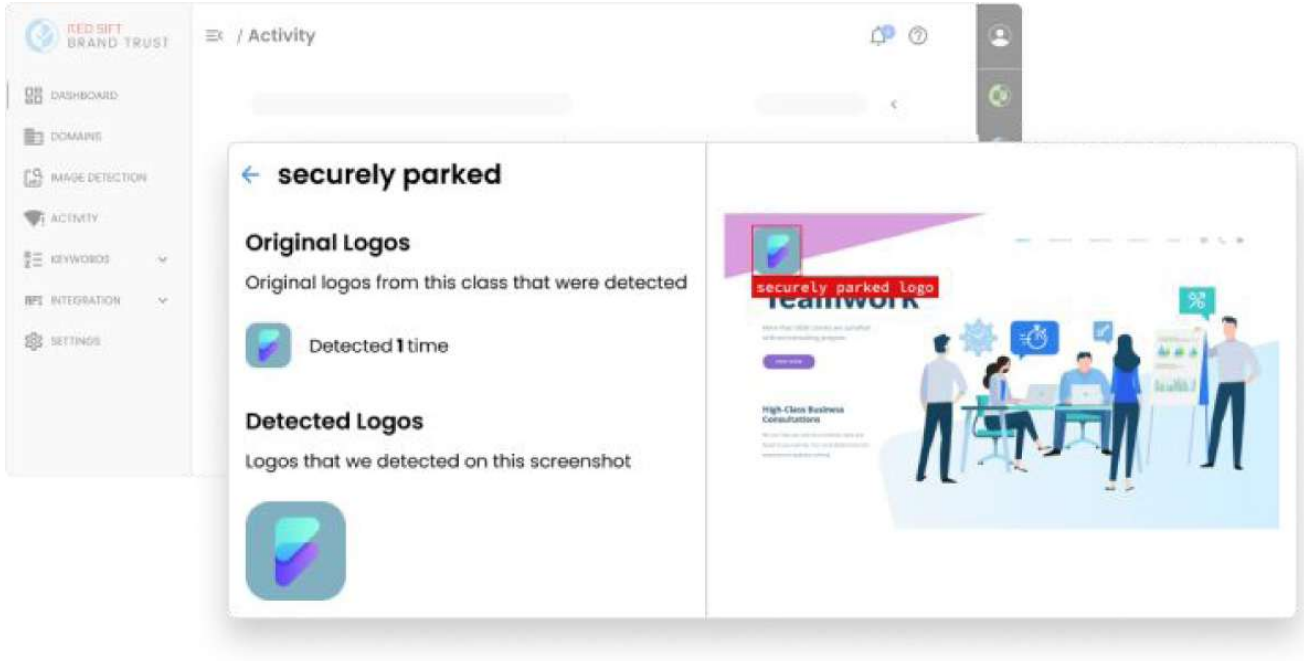


RED SIFT
BRAND TRUST

**Unmatched, AI-driven brand impersonation discovery and monitoring**

## Uncover brand abuse through AI-driven logo detection

Purpose-built logo-matching engine
identifies sites abusing your brand assets
– even if they are scaled, warped, or reflected on a motorcycle visor (seriously!).



RED SIFT
ASM

**Continuously discover, inventory and manage your business's critical assets.**

## Leverage unmanaged attack surface data

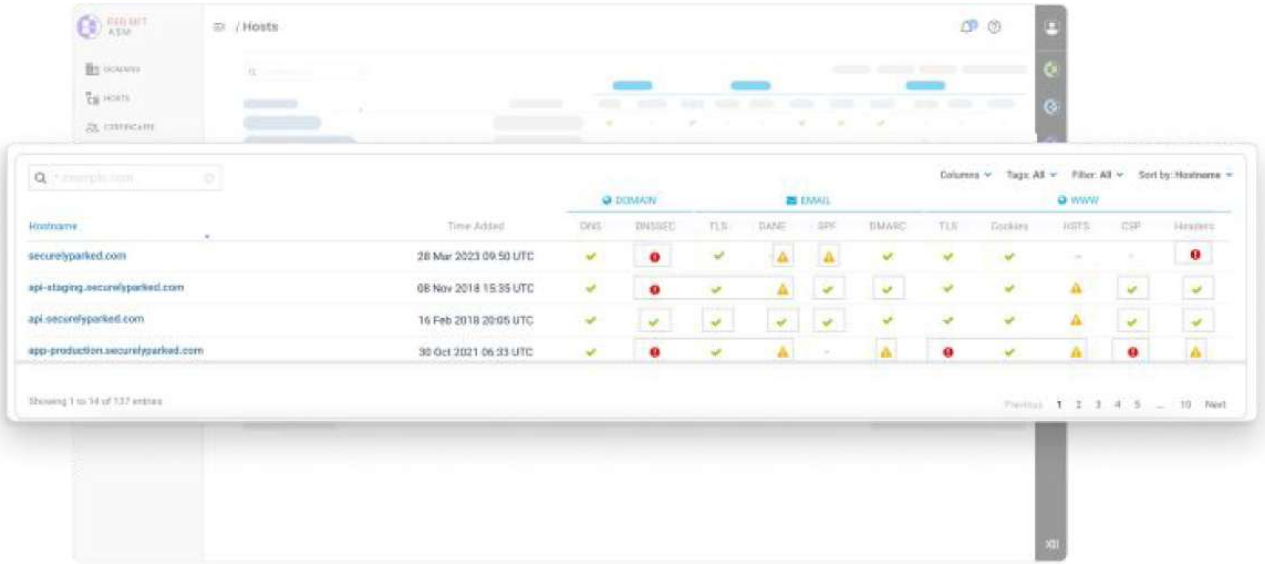
Identify mismanaged or unmanaged assets that other tools miss. Red Sift ASM continuously scans domains, hostnames, and IP addresses so your data is always fresh.

RED SIFT ASM

**Continuously discover, inventory and manage your business's critical assets.**

## Automated asset Inventory

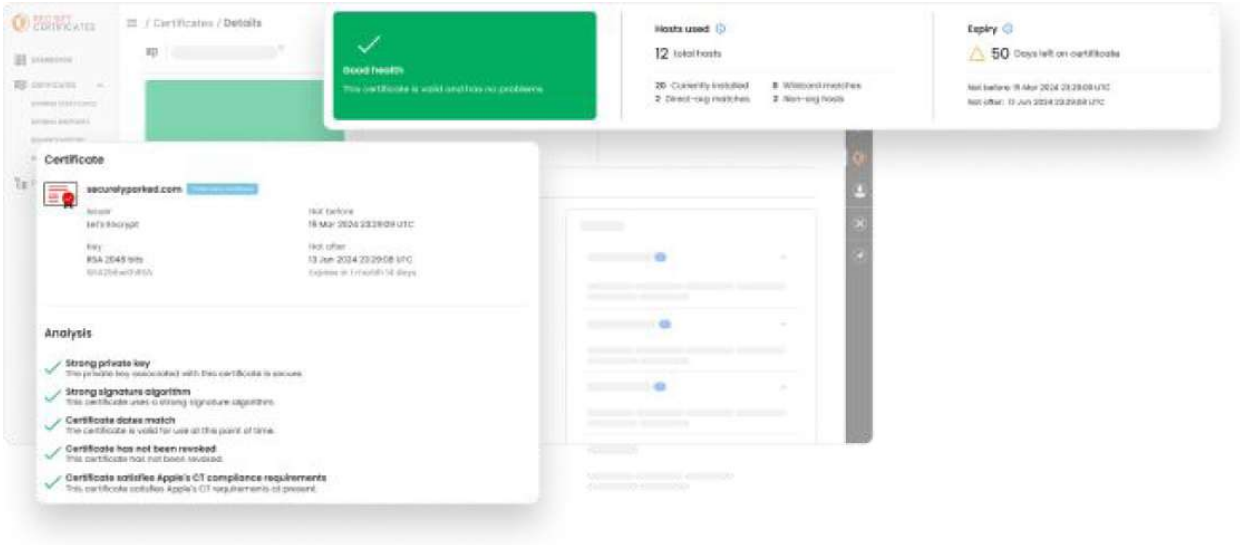
Build an inventory of your external-facing and cloud assets without spreadsheets or manual processes. Connect to cloud providers, certificate authorities, registrars, and managed DNS providers to import and monitor all of your assets.



RED SIFT
CERTIFICATES

## Information to take action

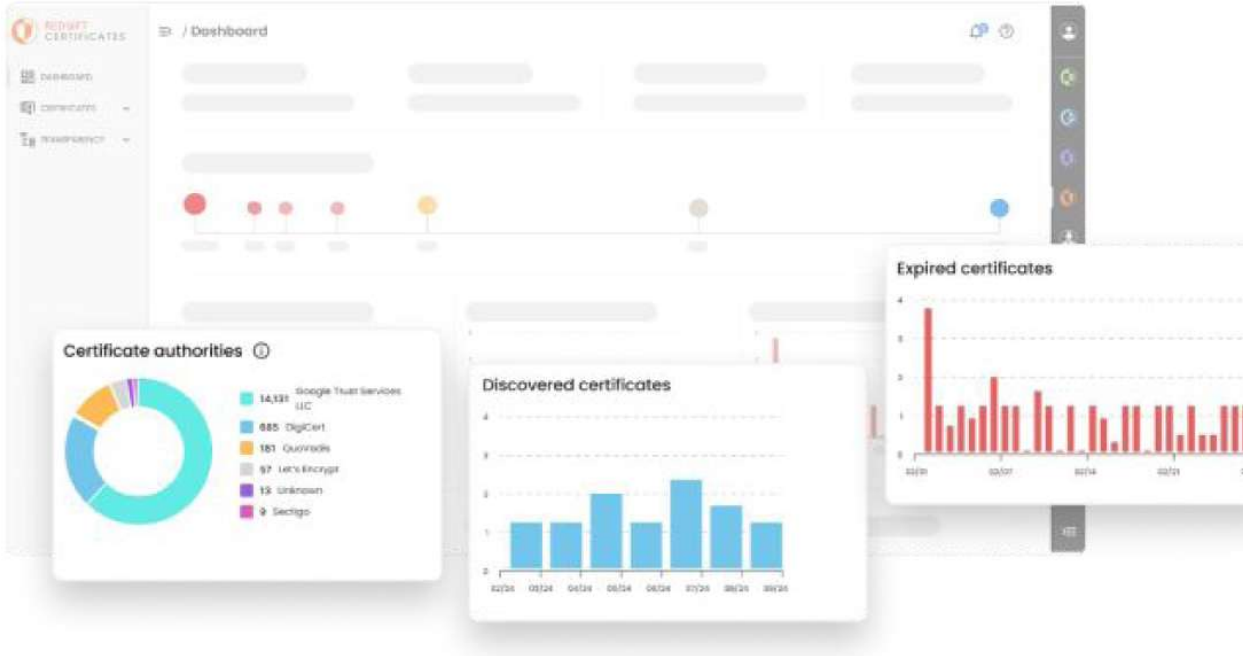
Real-time certificate installation location
data and content classification capabilities make it easy to prioritize remediation when problems are found.



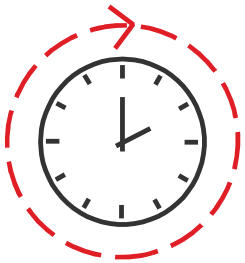
RED SIFT
CERTIFICATES

**The deepest, freshest certificate data**

Identify certificates other tools miss with
proprietary certificate monitoring technology. Red Sift Certificates ingests
and monitors every public certificate that is issued and looks for changes in real-time.



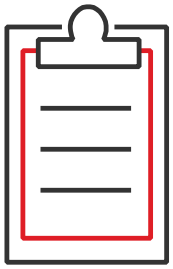
# Perché Red Sift? Sfide principali



## Visibilità

“Mentre le aziende Fortune 500 rilevano una grave vulnerabilità ogni 12 ore, gli aggressori impiegano meno di 45 minuti per fare lo stesso.”

*Source MIT Technology Review: A Game Changer in IT Security*



## Direttive

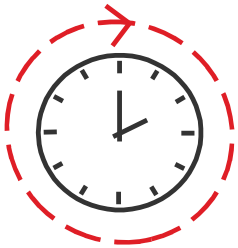
- ✓ Nis2
- ✓ PCI 4.0
- ✓ SEC cybersecurity rules
- ✓ DORA
- ✓ Security scorecards and ratings
- ✓ 2024 email authentication requirements
- ✓ And, many, many more


## Complessità

“Entro il 2026, le superfici di attacco non patchabili cresceranno da meno del 10%... a più della metà dell'esposizione totale dell'impresa”

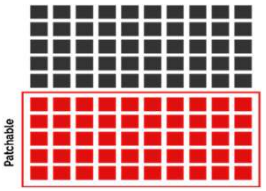
*Source* Gartner®

# Perché Red Sift? Sfide principali



**Visibilità**

**Direttive**




**Complessità**

RED SIFT OnDMARC

RED SIFT BRAND TRUST

RED SIFT ASM

RED SIFT CERTIFICATES

RED SIFT PULSE

RED SIFT RADAR

# Q&A

**Contatti:**

**marketing@bludis.it**

**Vieni a trovarci al nostro stand!**