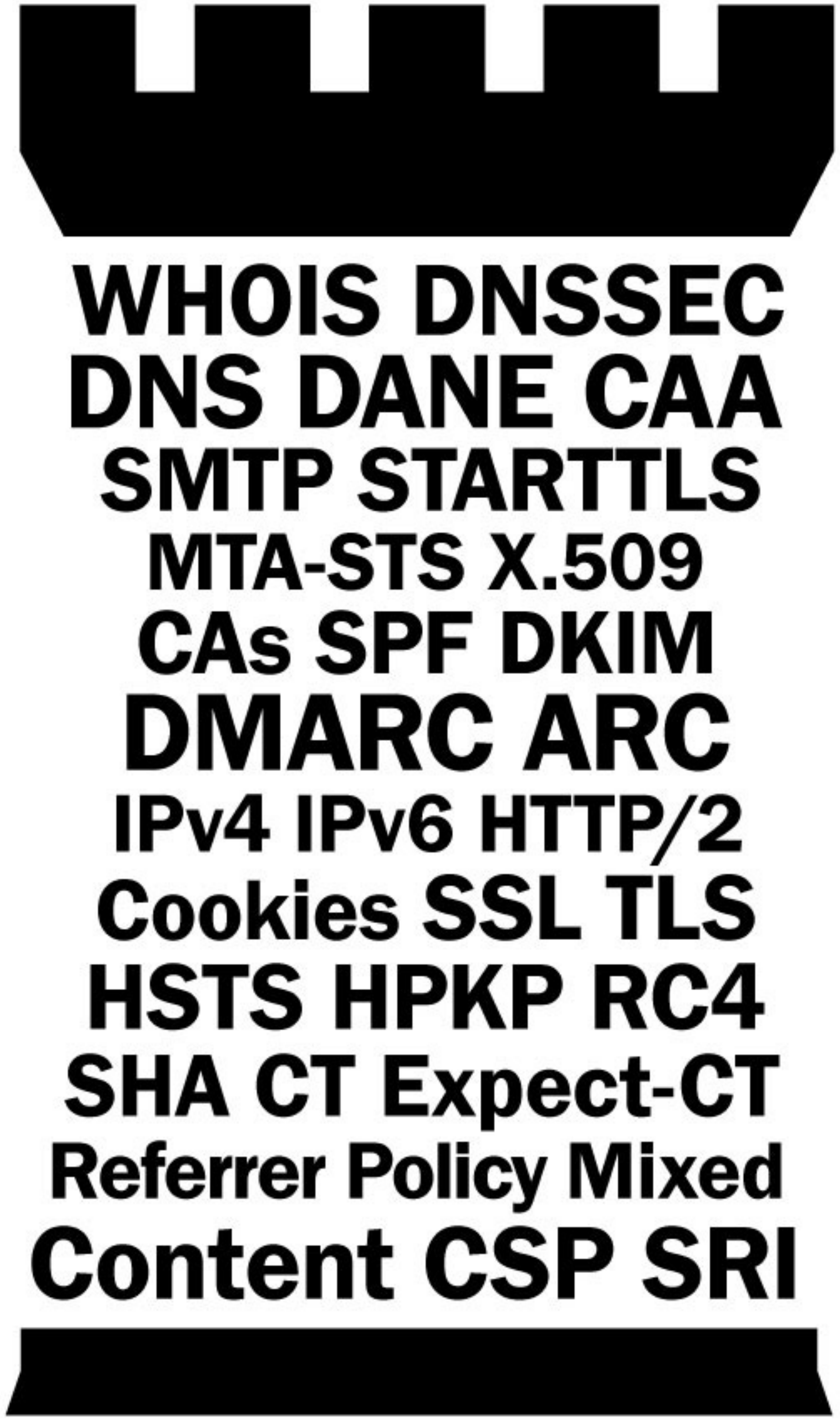
Everyone deserves good internet security

Hardenize

Less than 1% of top web sites use security features available today.

Internet is insecure by default. To be secure, we need to work hard.

WHOIS, DNS, DNSSEC, DANE, CAA, SMTP, STARTTLS, MTA-STS, X.509, CAs, SPF, DKIM, DMARC, ARC, IPv4, IPv6, HTTP/2, Cookies, SSL, TLS, HSTS, HPKP, RC4, SHA, CT, Expect-CT, Referrer Policy, Mixed content, CSP, SRI, privacy, and many more…



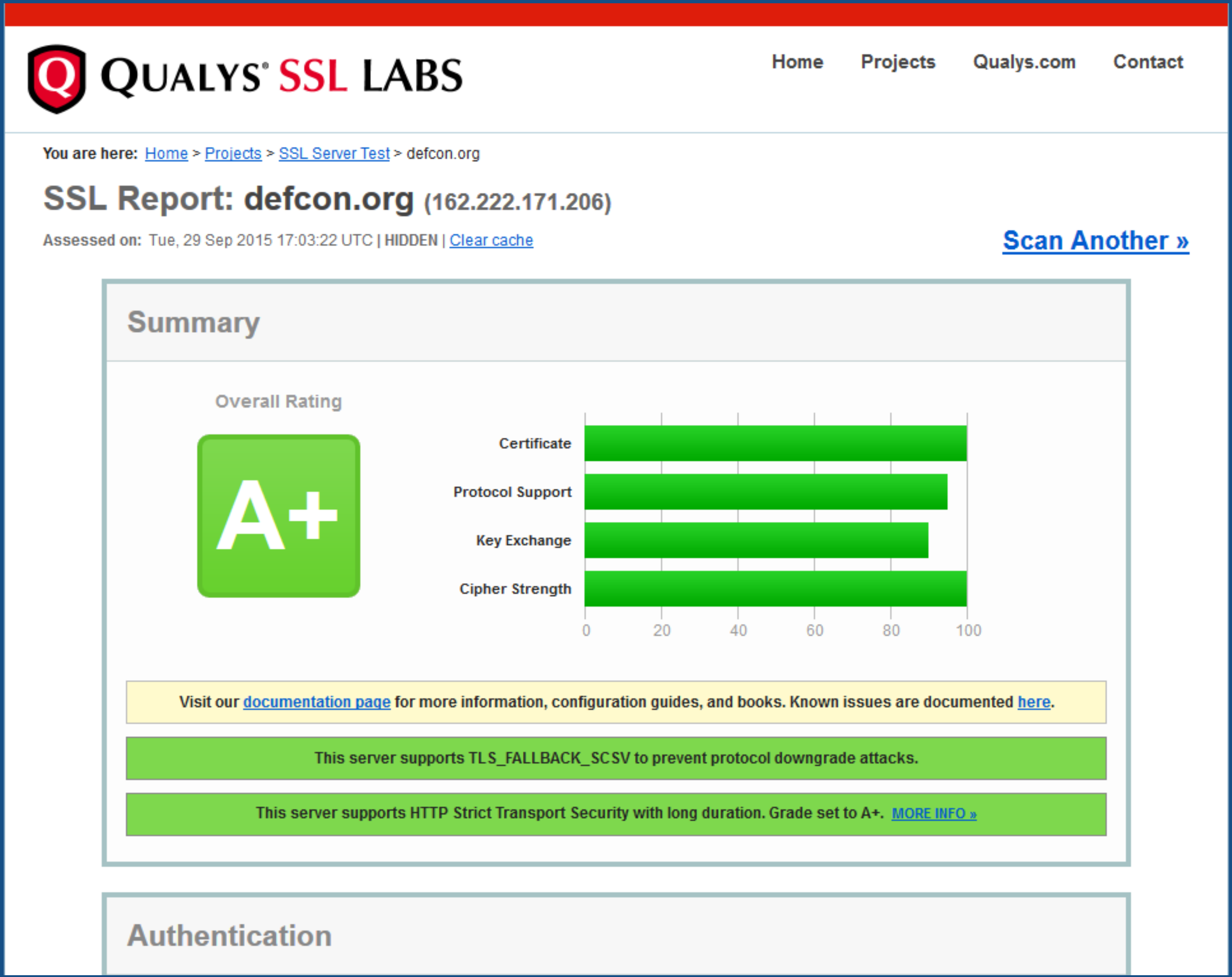
WHOIS DNSSEC
DNS DANE CAA
SMTP STARTTLS
MTA-STS X.509
CAs SPF DKIM
DMARC ARC
IPv4 IPv6 HTTP/2
Cookies SSL TLS
HSTS HPKP RC4
SHA CT Expect-CT
Referrer Policy Mixed
Content CSP SRI

No one has time, expertise, or budget to do all of this properly.

Hardenize

Know Audit Guide

SSL Labs (2009)



You are here: Home > Projects > SSL Server Test > defcon.org

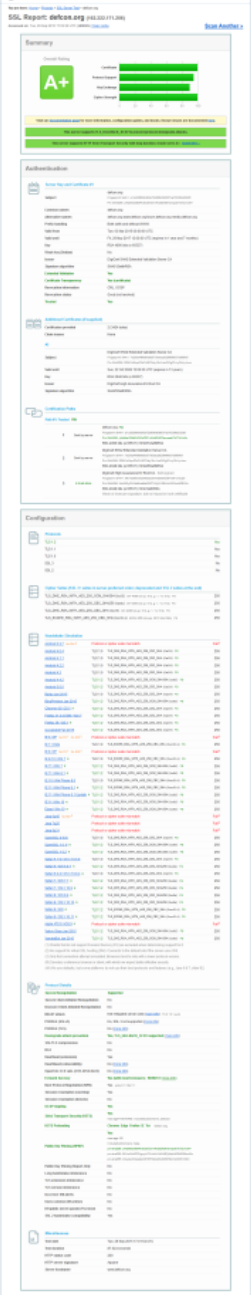
SSL Report: defcon.org (162.222.171.206)

Assessed on: Tue, 29 Sep 2015 17:03:22 UTC | HIDDEN | Clear cache

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

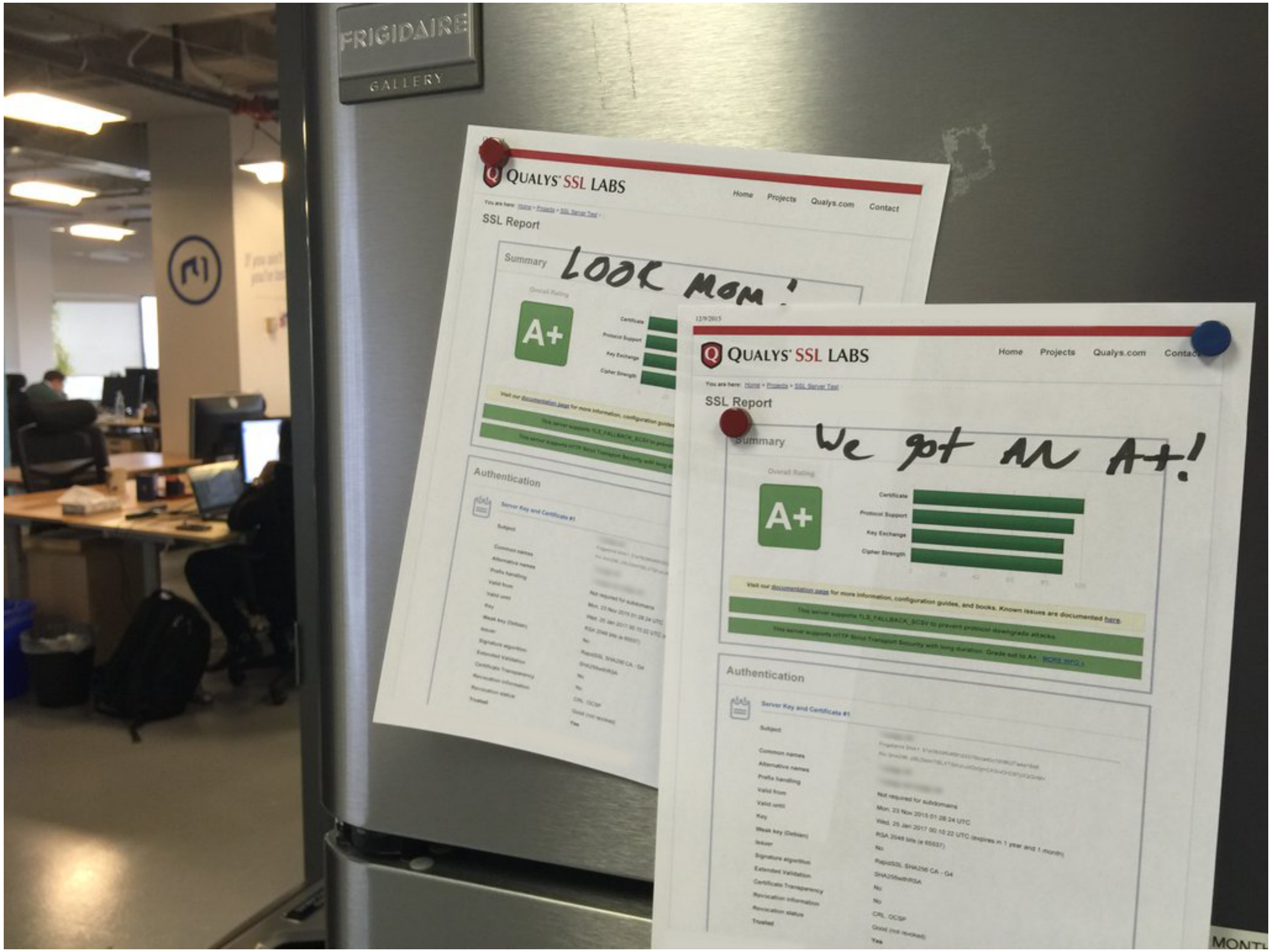
This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »



Make security interesting

Usable security that
people actually want to use.


FRIGIDAIRE
GALLERY
QUALYS SSL LABS
Home Projects Qualys.com Contact
SSL Report
Summary
Look mom!
A+
Authentication
QUALYS SSL LABS
Home Projects Qualys.com Contact
SSL Report
Summary
We got an A+!
A+
Authentication

Make security interesting, easy, and fun.

“Try it now”

Remove the barrier to entry by
making tools easily available.

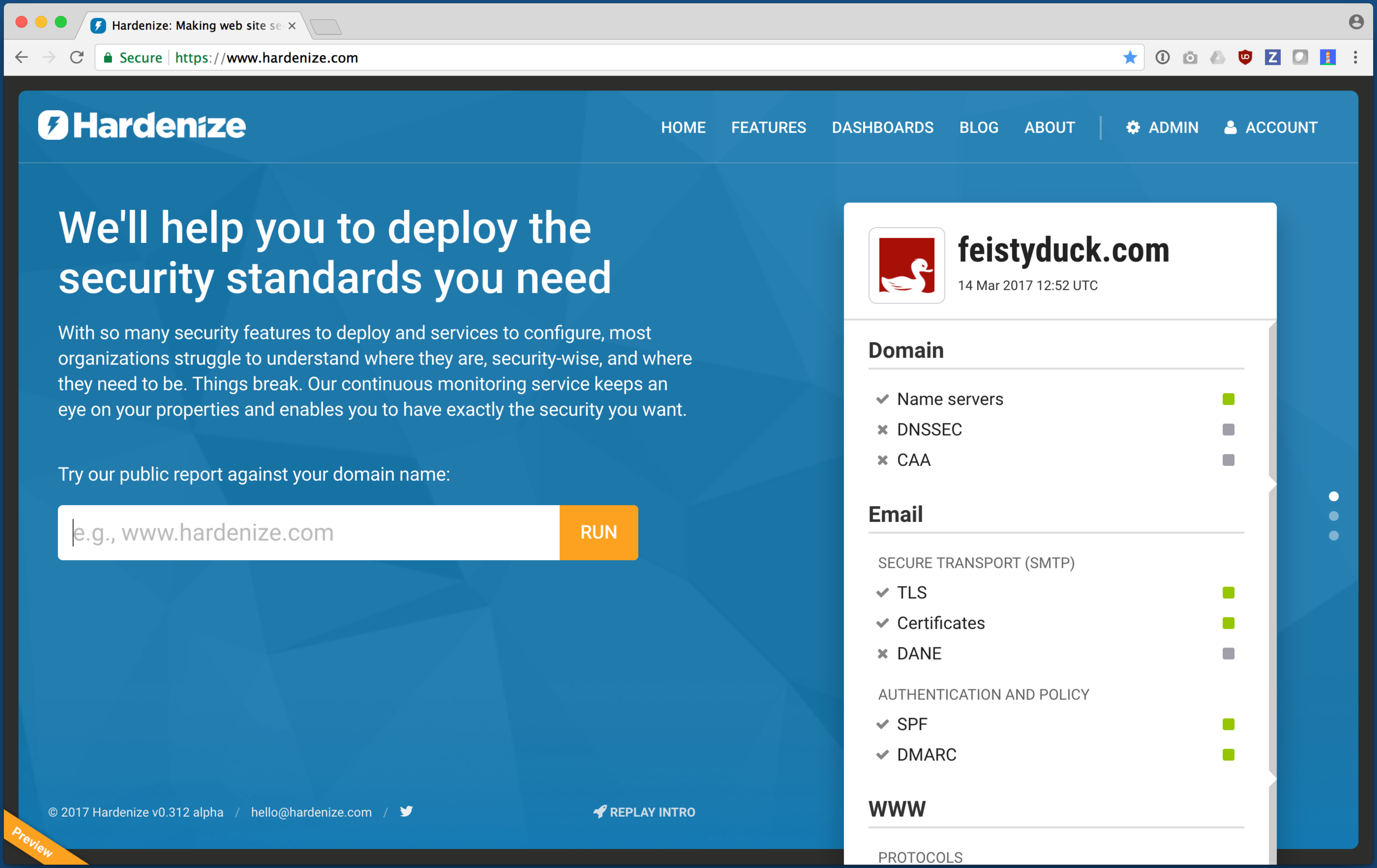
Make it clear

Hide most of technical information. What you do show, make clear and relevant.

It should be a game

Develop useful grading criteria that makes the next step <u>just</u> out of reach.

Hardenize


Hardenize: Making web site se
Secure https://www.hardenize.com
Hardenize
HOME
FEATURES
DASHBOARDS
BLOG
ABOUT
ADMIN
ACCOUNT

We'll help you to deploy the security standards you need

With so many security features to deploy and services to configure, most organizations struggle to understand where they are, security-wise, and where they need to be. Things break. Our continuous monitoring service keeps an eye on your properties and enables you to have exactly the security you want.

Try our public report against your domain name:

e.g., www.hardenize.com RUN

feistyduck.com

14 Mar 2017 12:52 UTC

Domain

- ✓ Name servers 🟩
- ✖ DNSSEC ⬜
- ✖ CAA ⬜

Email

SECURE TRANSPORT (SMTP)

- ✓ TLS 🟩
- ✓ Certificates 🟩
- ✖ DANE ⬜

AUTHENTICATION AND POLICY

- ✓ SPF 🟩
- ✓ DMARC 🟩

WWW

PROTOCOLS

© 2017 Hardenize v0.312 alpha / hello@hardenize.com /

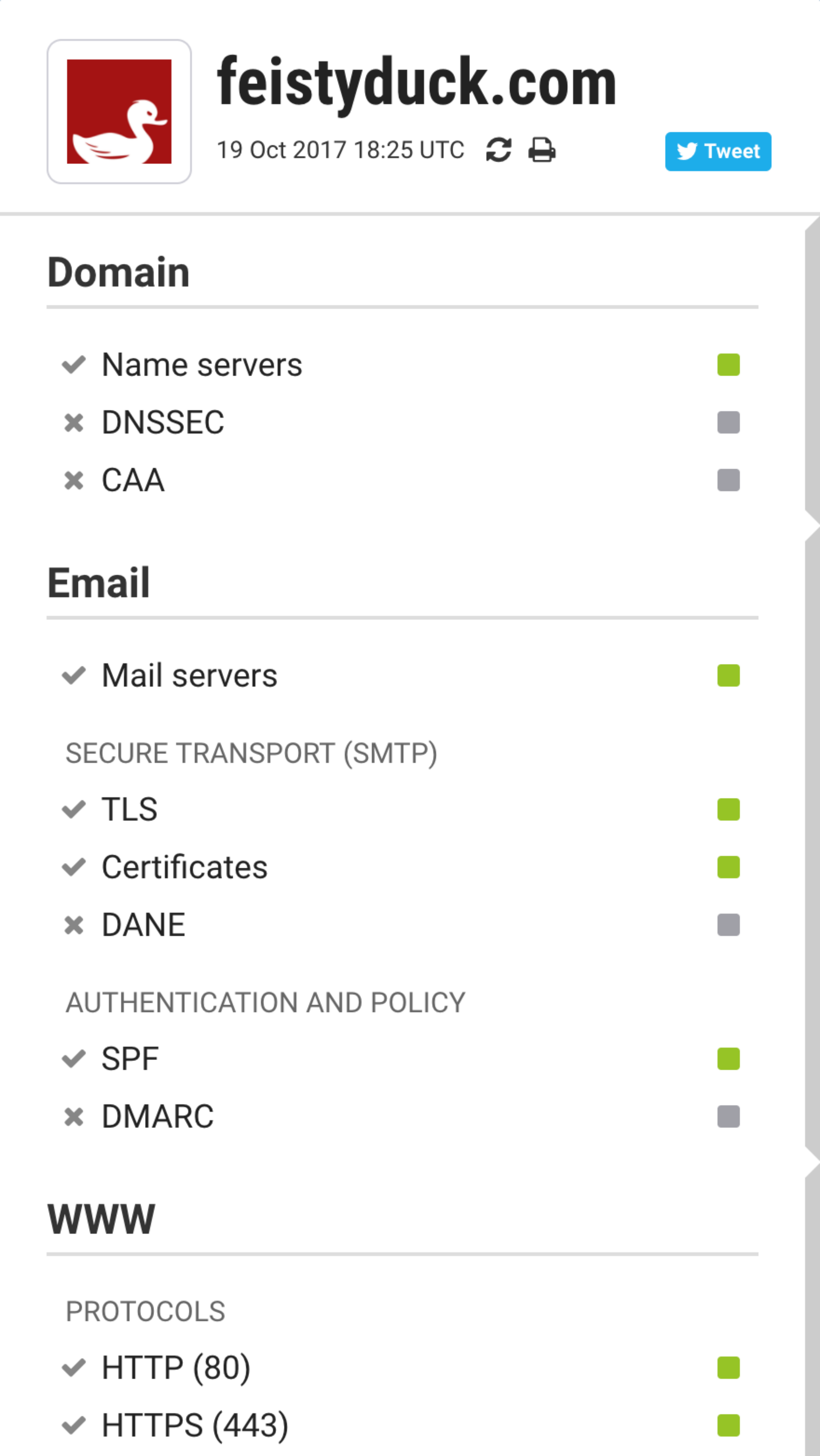
REPLAY INTRO

Hardenize

Simple on
the surface

Easy to
understand and
communicate

Wide coverage
of security and
configurations
standards



feistyduck.com

19 Oct 2017 18:25 UTC

Domain

- ✓ Name servers 🟩
- ✖ DNSSEC ⬜
- ✖ CAA ⬜

Email

- ✓ Mail servers 🟩

SECURE TRANSPORT (SMTP)

- ✓ TLS 🟩
- ✓ Certificates 🟩
- ✖ DANE ⬜

AUTHENTICATION AND POLICY

- ✓ SPF 🟩
- ✖ DMARC ⬜

WWW

PROTOCOLS

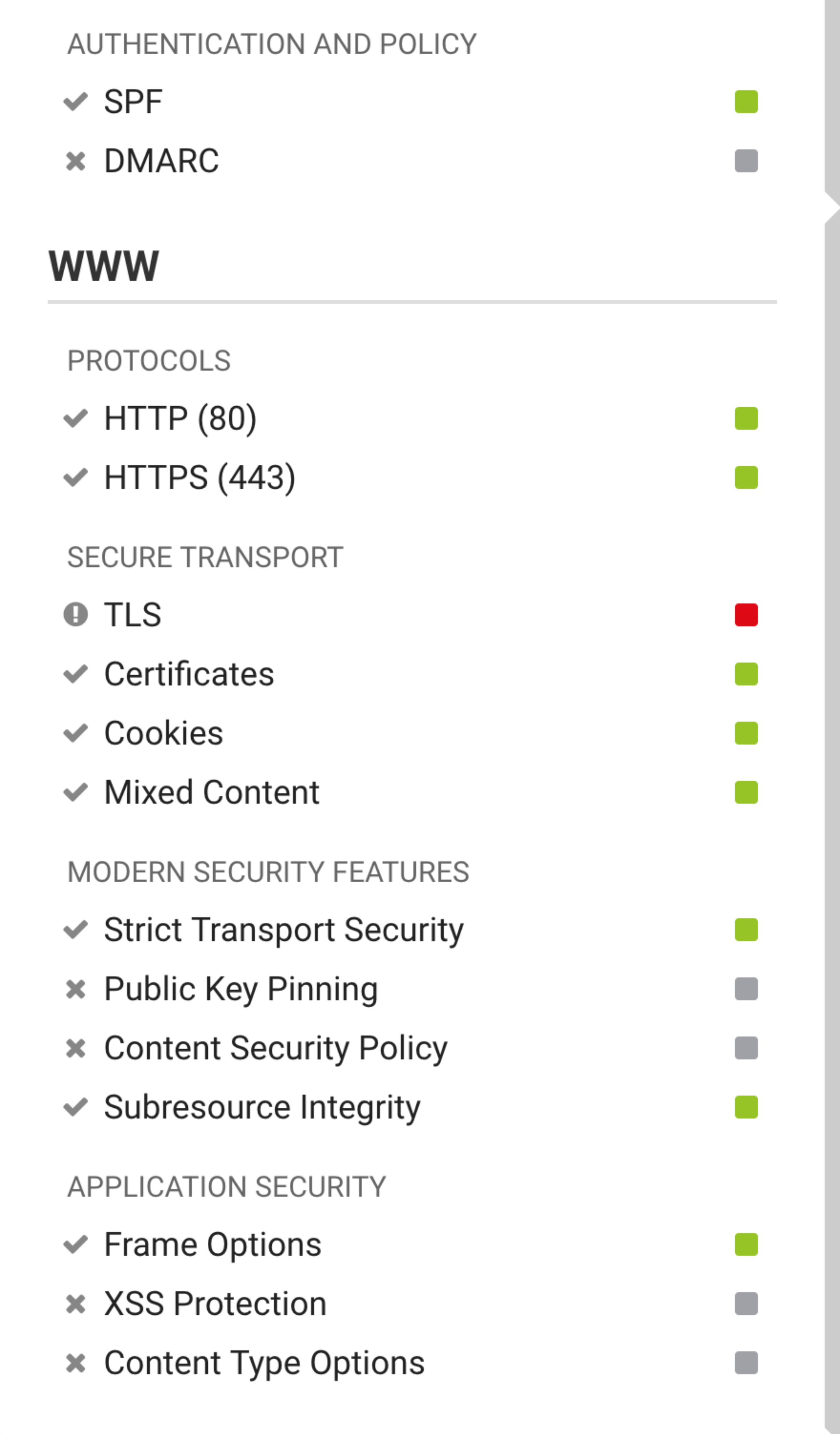
- ✓ HTTP (80) 🟩
- ✓ HTTPS (443) 🟩

Hardenize

Hundreds of complex tests under the hood

Correlation and meaningful findings

Full data available when needed



AUTHENTICATION AND POLICY

✓ SPF 🟩
✖ DMARC ◼

WWW

PROTOCOLS

✓ HTTP (80) 🟩
✓ HTTPS (443) 🟩

SECURE TRANSPORT

! TLS 🟥
✓ Certificates 🟩
✓ Cookies 🟩
✓ Mixed Content 🟩

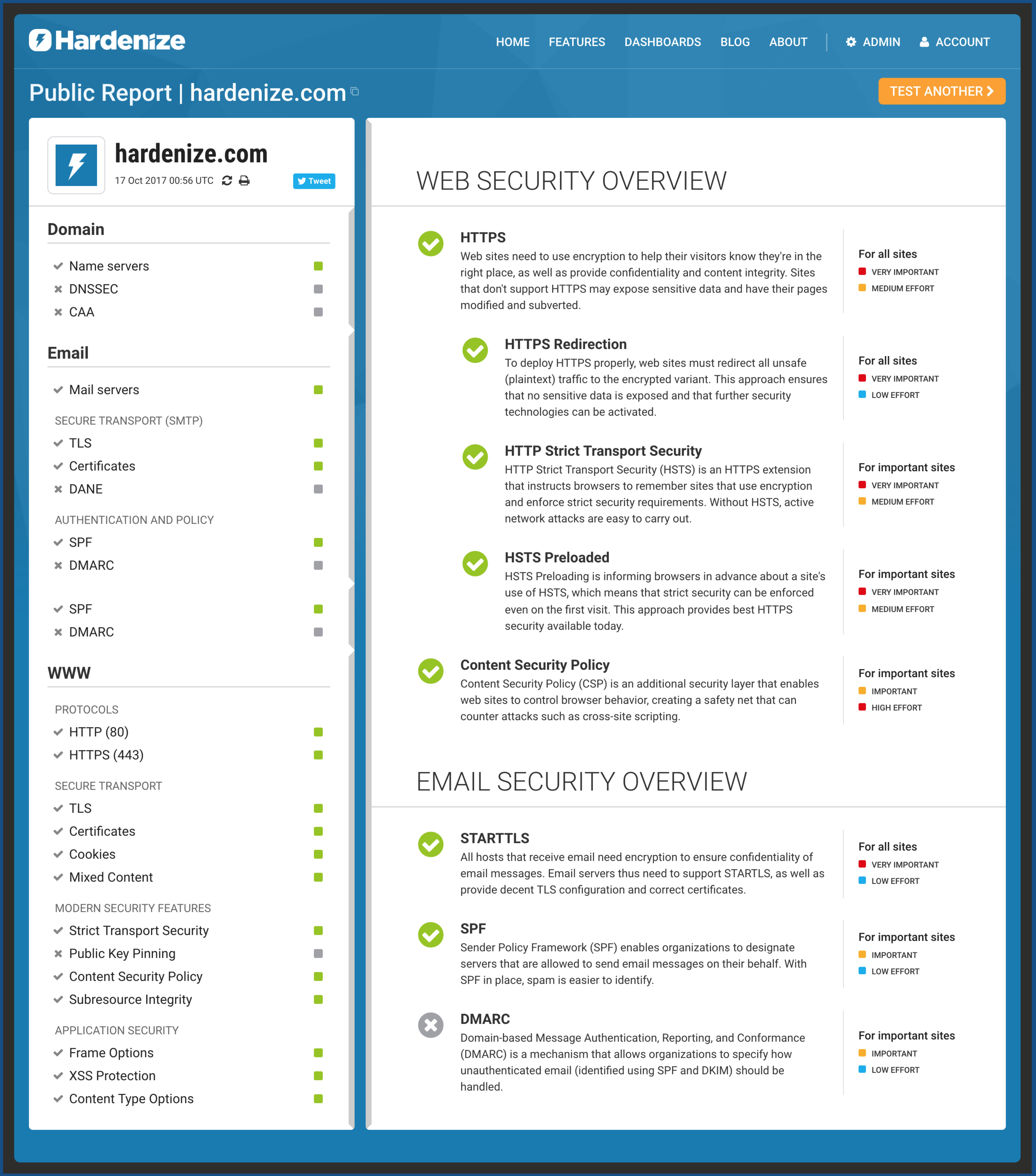
MODERN SECURITY FEATURES

✓ Strict Transport Security 🟩
✖ Public Key Pinning ◼
✖ Content Security Policy ◼
✓ Subresource Integrity 🟩

APPLICATION SECURITY

✓ Frame Options 🟩
✖ XSS Protection ◼
✖ Content Type Options ◼

Hardenize



Public Report | hardenize.com

hardenize.com
17 Oct 2017 00:56 UTC

Domain

- ✓ Name servers 🟩
- ✗ DNSSEC ◼
- ✗ CAA ◼

Email

- ✓ Mail servers 🟩

SECURE TRANSPORT (SMTP)

- ✓ TLS 🟩
- ✓ Certificates 🟩
- ✗ DANE ◼

AUTHENTICATION AND POLICY

- ✓ SPF 🟩
- ✗ DMARC ◼

- ✓ SPF 🟩
- ✗ DMARC ◼

WWW

PROTOCOLS

- ✓ HTTP (80) 🟩
- ✓ HTTPS (443) 🟩

SECURE TRANSPORT

- ✓ TLS 🟩
- ✓ Certificates 🟩
- ✓ Cookies 🟩
- ✓ Mixed Content 🟩

MODERN SECURITY FEATURES

- ✓ Strict Transport Security 🟩
- ✗ Public Key Pinning ◼
- ✓ Content Security Policy 🟩
- ✓ Subresource Integrity 🟩

APPLICATION SECURITY

- ✓ Frame Options 🟩
- ✓ XSS Protection 🟩
- ✓ Content Type Options 🟩

WEB SECURITY OVERVIEW

✓ **HTTPS**
Web sites need to use encryption to help their visitors know they're in the right place, as well as provide confidentiality and content integrity. Sites that don't support HTTPS may expose sensitive data and have their pages modified and subverted.
For all sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

✓ **HTTPS Redirection**
To deploy HTTPS properly, web sites must redirect all unsafe (plaintext) traffic to the encrypted variant. This approach ensures that no sensitive data is exposed and that further security technologies can be activated.
For all sites
🟥 VERY IMPORTANT
🟦 LOW EFFORT

✓ **HTTP Strict Transport Security**
HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers to remember sites that use encryption and enforce strict security requirements. Without HSTS, active network attacks are easy to carry out.
For important sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

✓ **HSTS Preloaded**
HSTS Preloading is informing browsers in advance about a site's use of HSTS, which means that strict security can be enforced even on the first visit. This approach provides best HTTPS security available today.
For important sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

✓ **Content Security Policy**
Content Security Policy (CSP) is an additional security layer that enables web sites to control browser behavior, creating a safety net that can counter attacks such as cross-site scripting.
For important sites
🟧 IMPORTANT
🟥 HIGH EFFORT

EMAIL SECURITY OVERVIEW

✓ **STARTTLS**
All hosts that receive email need encryption to ensure confidentiality of email messages. Email servers thus need to support STARTLS, as well as provide decent TLS configuration and correct certificates.
For all sites
🟥 VERY IMPORTANT
🟦 LOW EFFORT

✓ **SPF**
Sender Policy Framework (SPF) enables organizations to designate servers that are allowed to send email messages on their behalf. With SPF in place, spam is easier to identify.
For important sites
🟧 IMPORTANT
🟦 LOW EFFORT

✗ **DMARC**
Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism that allows organizations to specify how unauthenticated email (identified using SPF and DKIM) should be handled.
For important sites
🟧 IMPORTANT
🟦 LOW EFFORT

Full data
available
as needed

> “Doesn’t look like a security product”
>
> — One of our early users

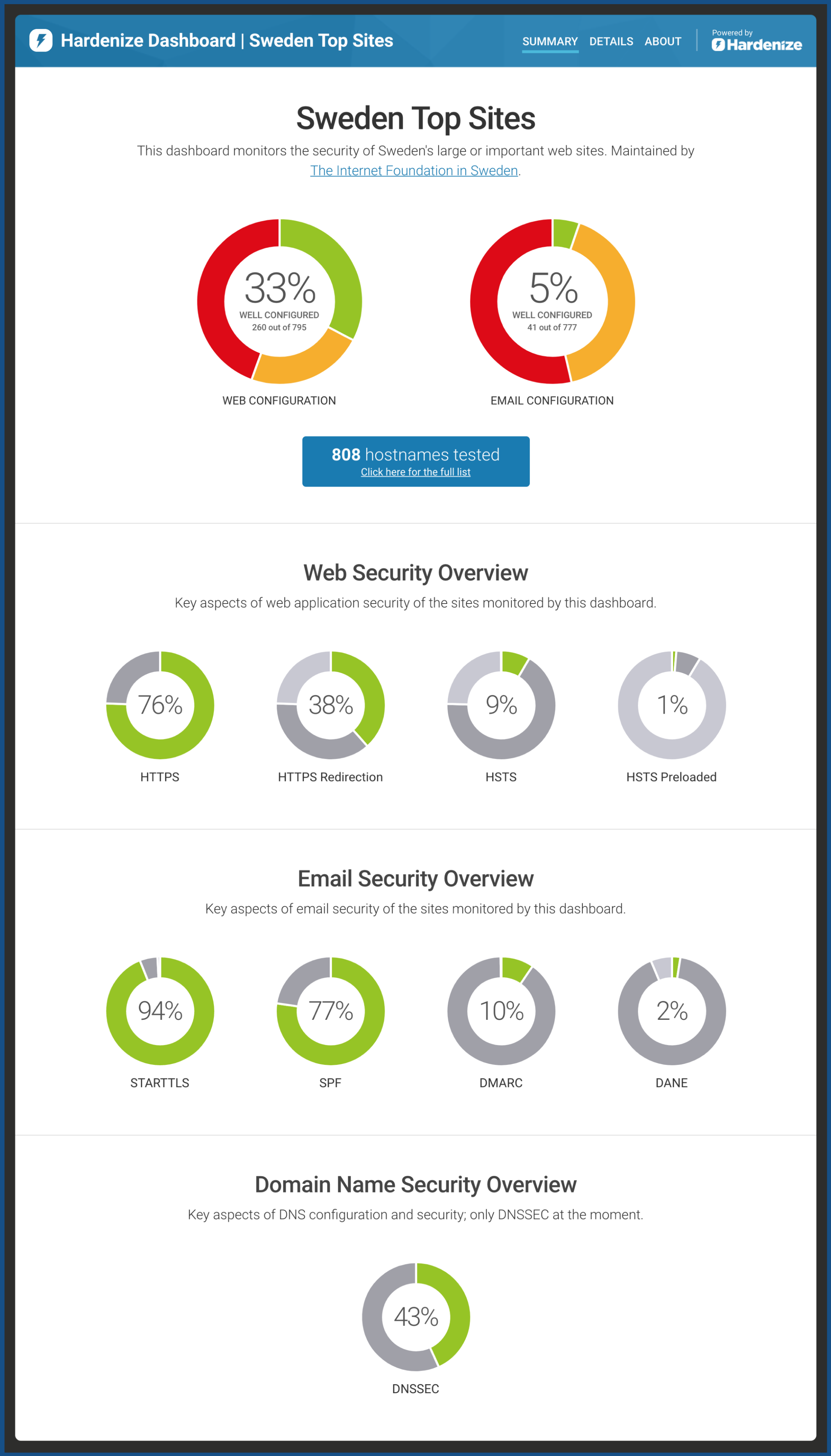
Transparency is a vital ingredient

Transparency creates urgency. Urgency creates budget. Things get done.

Hardenize

Public dashboards

Provided for free to official organisations



Sweden Top Sites

This dashboard monitors the security of Sweden's large or important web sites. Maintained by The Internet Foundation in Sweden.

808 hostnames tested
Click here for the full list

Web Security Overview

Key aspects of web application security of the sites monitored by this dashboard.

Email Security Overview

Key aspects of email security of the sites monitored by this dashboard.

Domain Name Security Overview

Key aspects of DNS configuration and security; only DNSSEC at the moment.

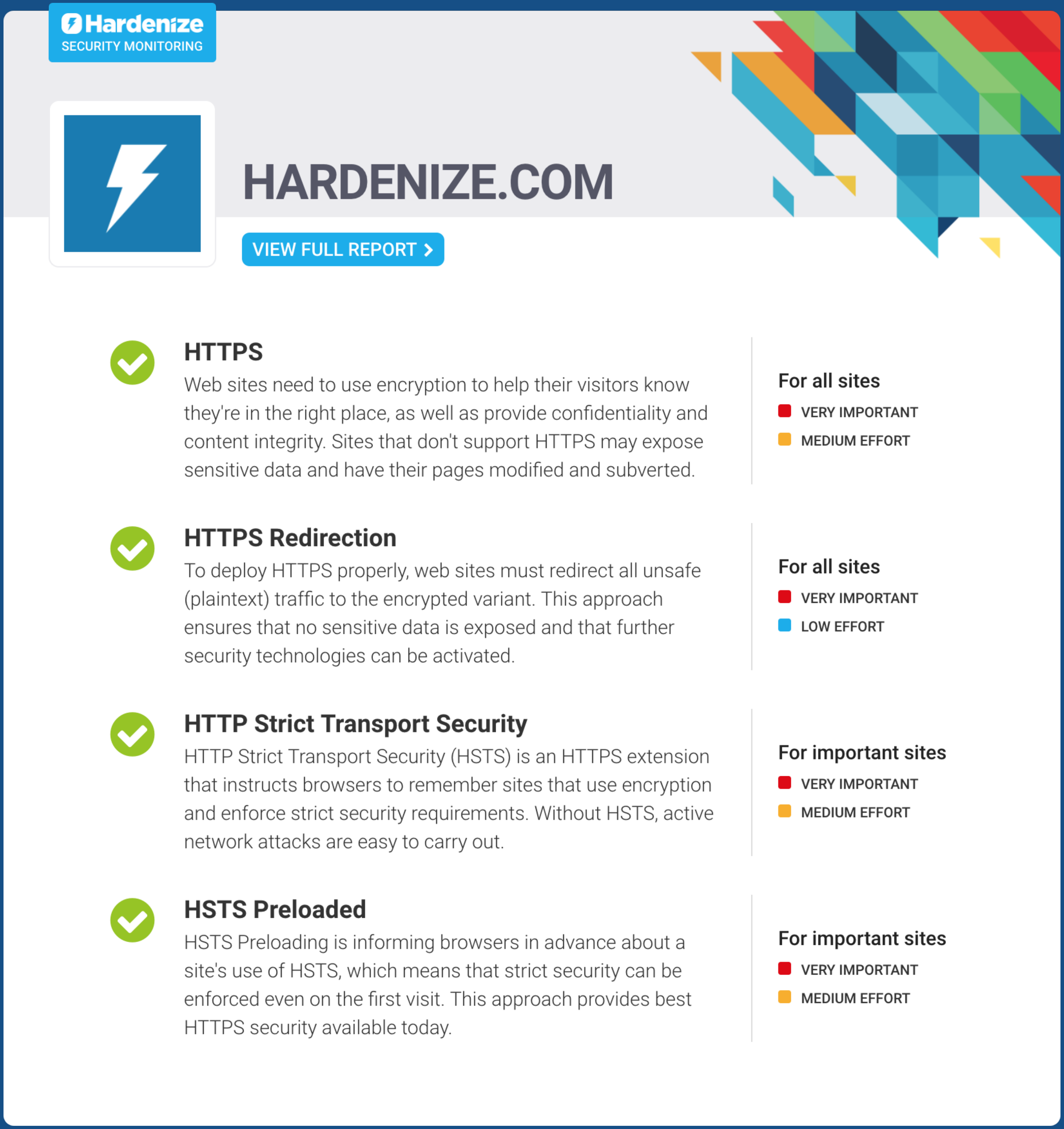
Web site badges

Everyone starts with the default badge

If you have robust HTTPS you get this one instead

Hardenize

Simplified to focus on most important aspects first.



HARDENIZE.COM

✓ **HTTPS**

Web sites need to use encryption to help their visitors know they're in the right place, as well as provide confidentiality and content integrity. Sites that don't support HTTPS may expose sensitive data and have their pages modified and subverted.

For all sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

✓ **HTTPS Redirection**

To deploy HTTPS properly, web sites must redirect all unsafe (plaintext) traffic to the encrypted variant. This approach ensures that no sensitive data is exposed and that further security technologies can be activated.

For all sites
🟥 VERY IMPORTANT
🟦 LOW EFFORT

✓ **HTTP Strict Transport Security**

HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers to remember sites that use encryption and enforce strict security requirements. Without HSTS, active network attacks are easy to carry out.

For important sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

✓ **HSTS Preloaded**

HSTS Preloading is informing browsers in advance about a site's use of HSTS, which means that strict security can be enforced even on the first visit. This approach provides best HTTPS security available today.

For important sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

Free public assessments

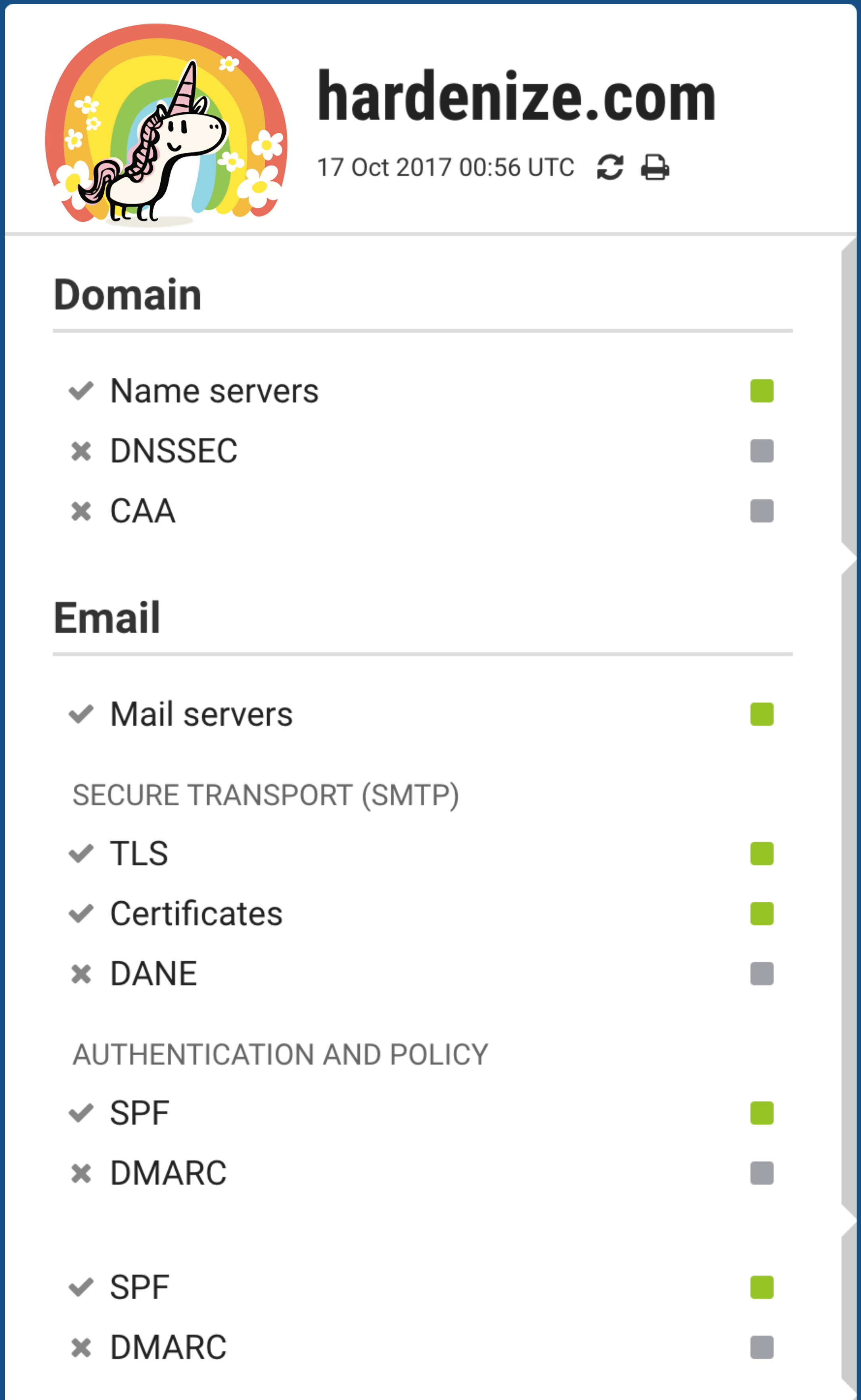
Public dashboards

Security badge

Continuous monitoring

Hardenize

EVERYONE DESERVES
GOOD INTERNET SECURITY



hardenize.com

17 Oct 2017 00:56 UTC

Domain

✓ Name servers 🟩
✗ DNSSEC ■
✗ CAA ■

Email

✓ Mail servers 🟩

SECURE TRANSPORT (SMTP)

✓ TLS 🟩
✓ Certificates 🟩
✗ DANE ■

AUTHENTICATION AND POLICY

✓ SPF 🟩
✗ DMARC ■

✓ SPF 🟩
✗ DMARC ■