Improving security of complex ecosystems

Ivan Ristić

Hardenize

Everyone deserves good internet security.

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

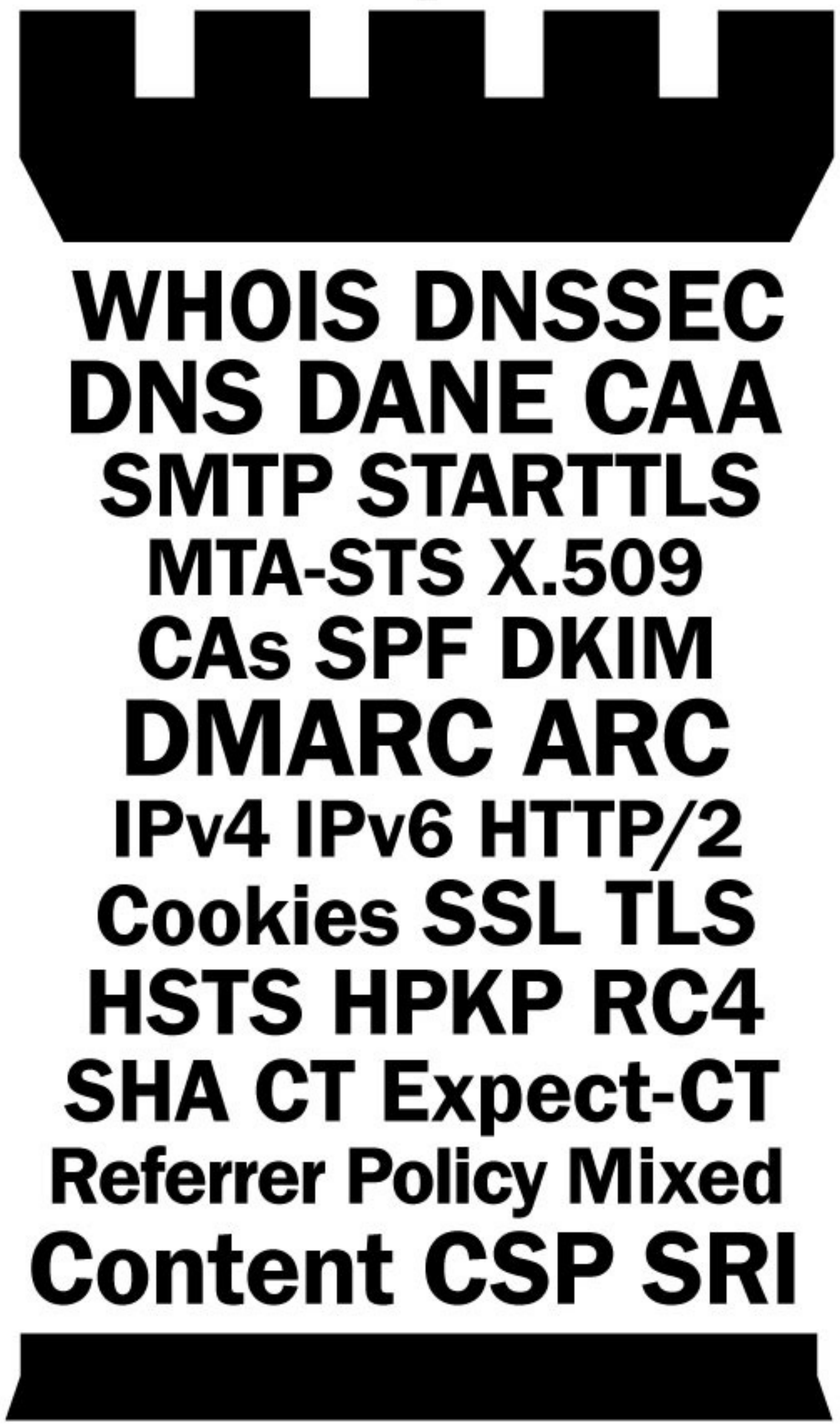
The future [of security] is already here, but it’s not evenly distributed.

William Gibson, adapted.

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, 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.

Level 0. There is no security.

No standards, know-how, or
awareness. Experts can’t agree.

Level 1. Security is very difficult and expensive.

Only for the wealthiest, most exposed, and most determined.

Level 2. Security is possible, but at substantial cost.

Within the reach of many, but must fight bad tools, libraries, docs, and practices.

Level 3. Security is a widely-accepted best practice.

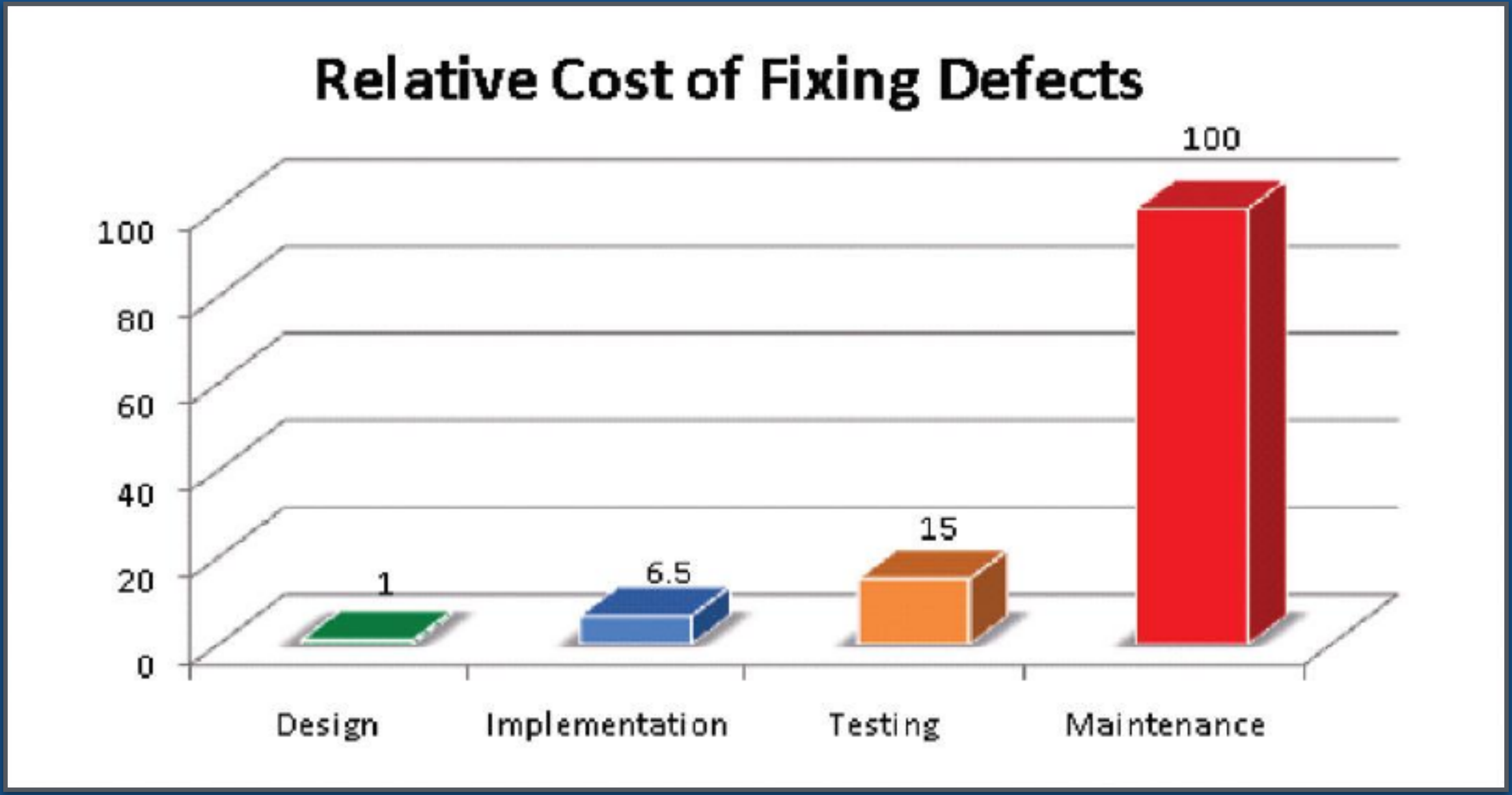
Documentation and know-how widely available, most can get it right.

Level 4. Security is required, by industry or law.

Security is now in the mainstream, and required to belong in the community.

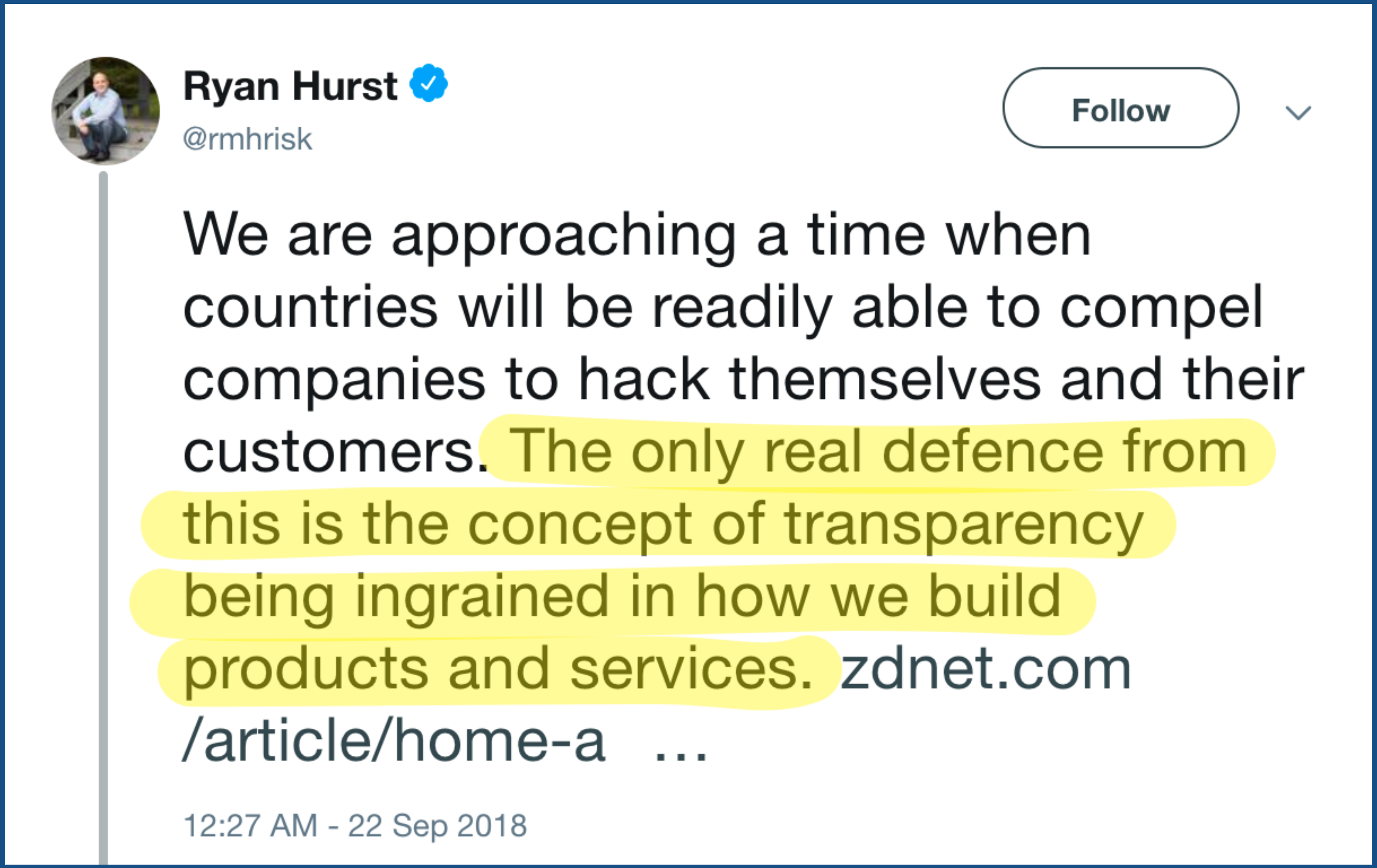
Level 5. Security is built-in for everyone.

End-game:
Built-in Security



From: “Integrating Software Assurance into the Software Development Life Cycle” (2010)

End-game:
Built-in Transparency

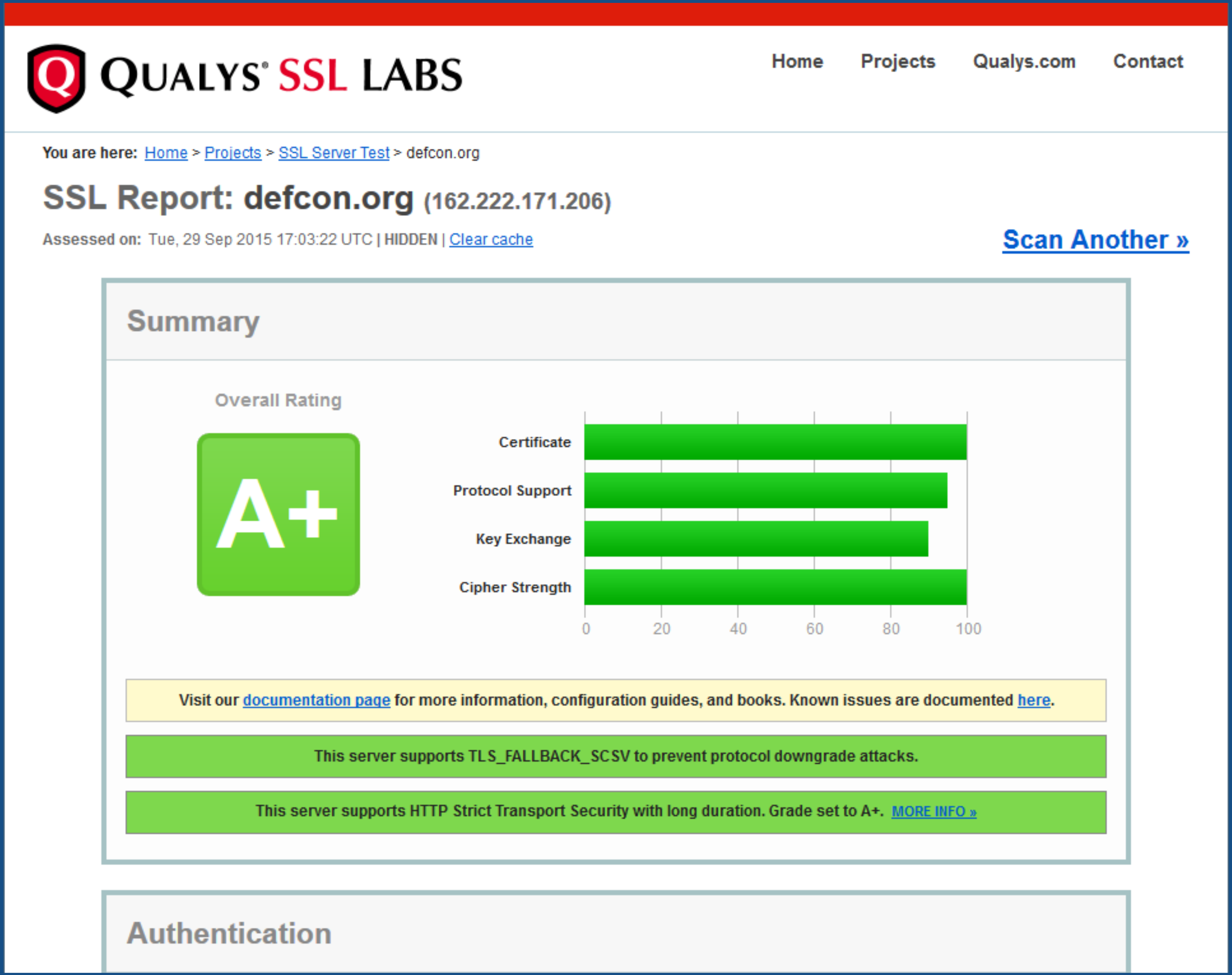


Ryan Hurst
@rmhrisk

We are approaching a time when countries will be readily able to compel companies to hack themselves and their customers. The only real defence from this is the concept of transparency being ingrained in how we build products and services. zdnet.com /article/home-a …

12:27 AM - 22 Sep 2018

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

Summary

Overall Rating

A+

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

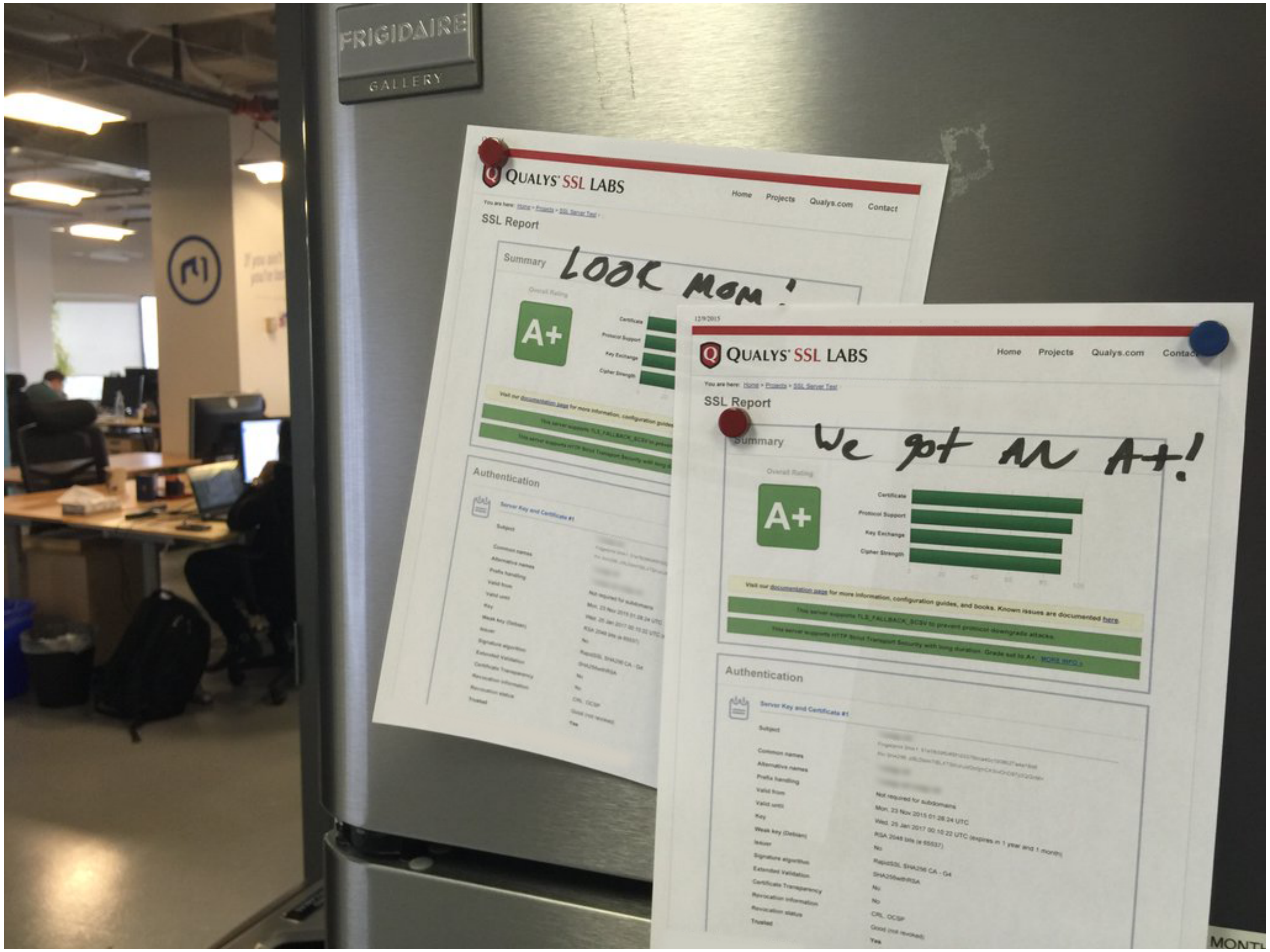
This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

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

Authentication

Make security interesting

Usable security that
people actually want to use.



Look mom!

QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test >

SSL Report

Summary

Overall Rating

A+

12/9/2015

QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test

SSL Report

Summary We got an A+!

Overall Rating

A+

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 »

Authentication

Server Key and Certificate #1

Subject	[redacted]
Common names	[redacted]
Alternative names	[redacted]
Prefix handling	Not required for subdomains
Valid from	Mon, 23 Nov 2015 01:28:24 UTC
Valid until	Wed, 25 Jan 2017 00:10:22 UTC (expires in 1 year and 1 month)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	RapidSSL SHA256 CA - G4
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Make security interesting, easy, and fun.

“Try it now”

Remove the barrier to entry by making tools easily available.

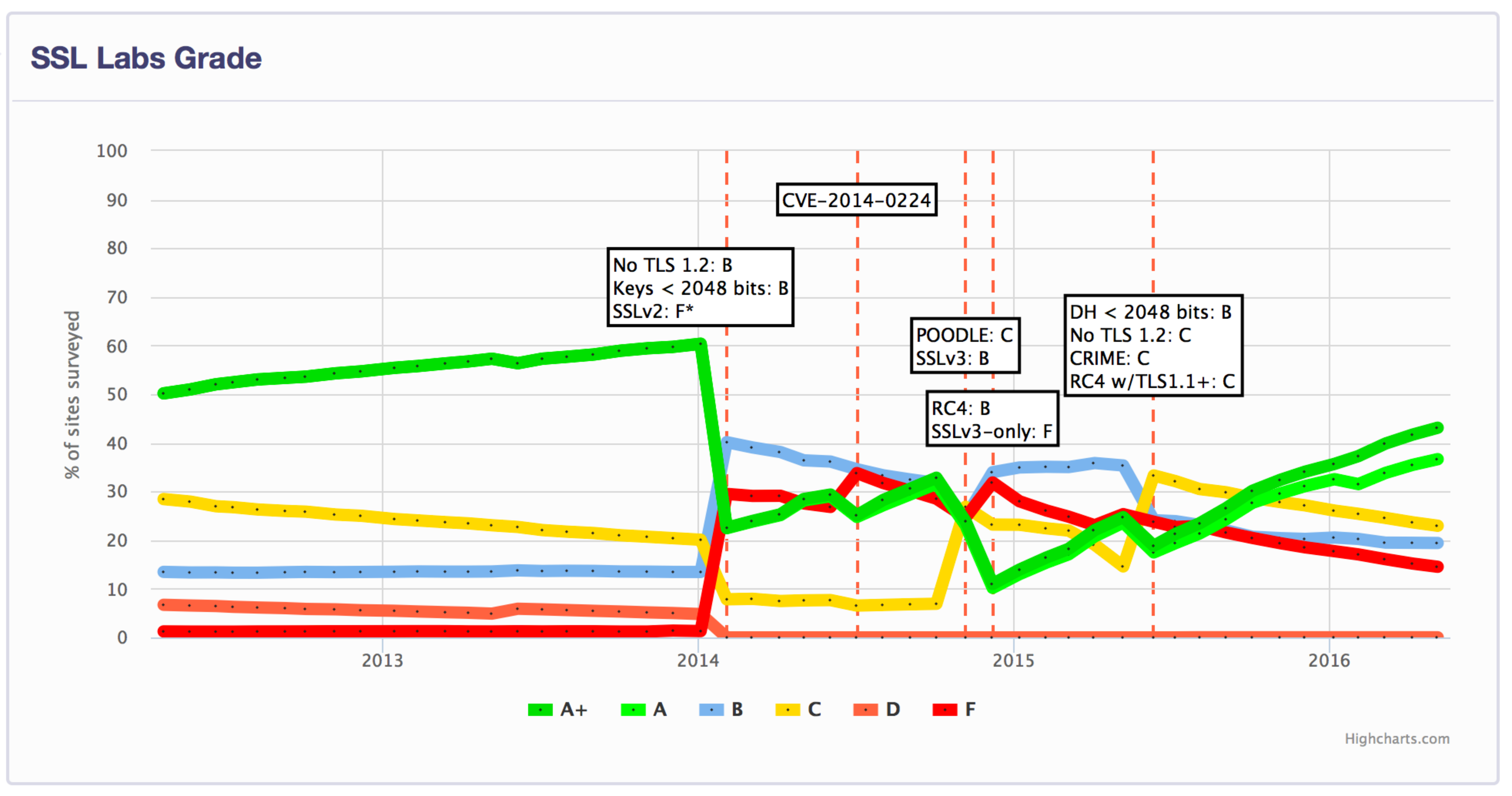
Make it clear

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 just out of reach.

SSL Pulse



SSL Labs Grade

Hardenize

Hardenize

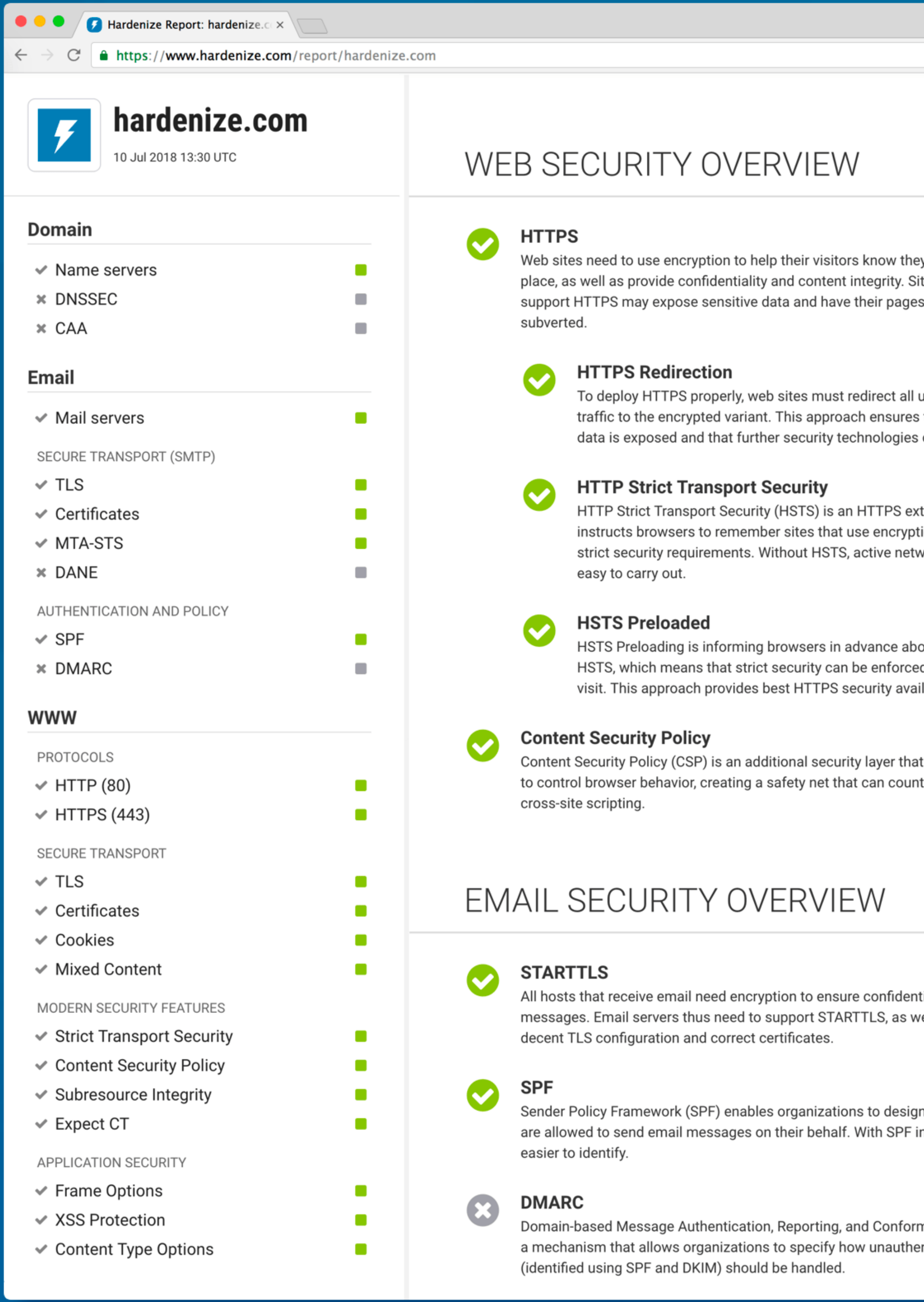
HOME PRODUCT DASHBOARDS BLOG ABOUT | ⚙ ADMIN

Meet the new standard for web site network and security configuration monitoring

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



Hardenize Report: hardenize.c ×

https://www.hardenize.com/report/hardenize.com

hardenize.com

10 Jul 2018 13:30 UTC

Domain

- ✓ Name servers 🟩
- ✕ DNSSEC ■
- ✕ CAA ■

Email

- ✓ Mail servers 🟩

SECURE TRANSPORT (SMTP)

- ✓ TLS 🟩
- ✓ Certificates 🟩
- ✓ MTA-STS 🟩
- ✕ DANE ■

AUTHENTICATION AND POLICY

- ✓ SPF 🟩
- ✕ DMARC ■

WWW

PROTOCOLS

- ✓ HTTP (80) 🟩
- ✓ HTTPS (443) 🟩

SECURE TRANSPORT

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

MODERN SECURITY FEATURES

- ✓ Strict Transport Security 🟩
- ✓ Content Security Policy 🟩
- ✓ Subresource Integrity 🟩
- ✓ Expect CT 🟩

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 place, as well as provide confidentiality and content integrity. Sit support HTTPS may expose sensitive data and have their pages subverted.

✓ **HTTPS Redirection**
To deploy HTTPS properly, web sites must redirect all u traffic to the encrypted variant. This approach ensures data is exposed and that further security technologies

✓ **HTTP Strict Transport Security**
HTTP Strict Transport Security (HSTS) is an HTTPS ext instructs browsers to remember sites that use encrypti strict security requirements. Without HSTS, active netw easy to carry out.

✓ **HSTS Preloaded**
HSTS Preloading is informing browsers in advance abo HSTS, which means that strict security can be enforced visit. This approach provides best HTTPS security avail

✓ **Content Security Policy**
Content Security Policy (CSP) is an additional security layer that to control browser behavior, creating a safety net that can count cross-site scripting.

EMAIL SECURITY OVERVIEW

✓ **STARTTLS**
All hosts that receive email need encryption to ensure confident messages. Email servers thus need to support STARTTLS, as we decent TLS configuration and correct certificates.

✓ **SPF**
Sender Policy Framework (SPF) enables organizations to design are allowed to send email messages on their behalf. With SPF in easier to identify.

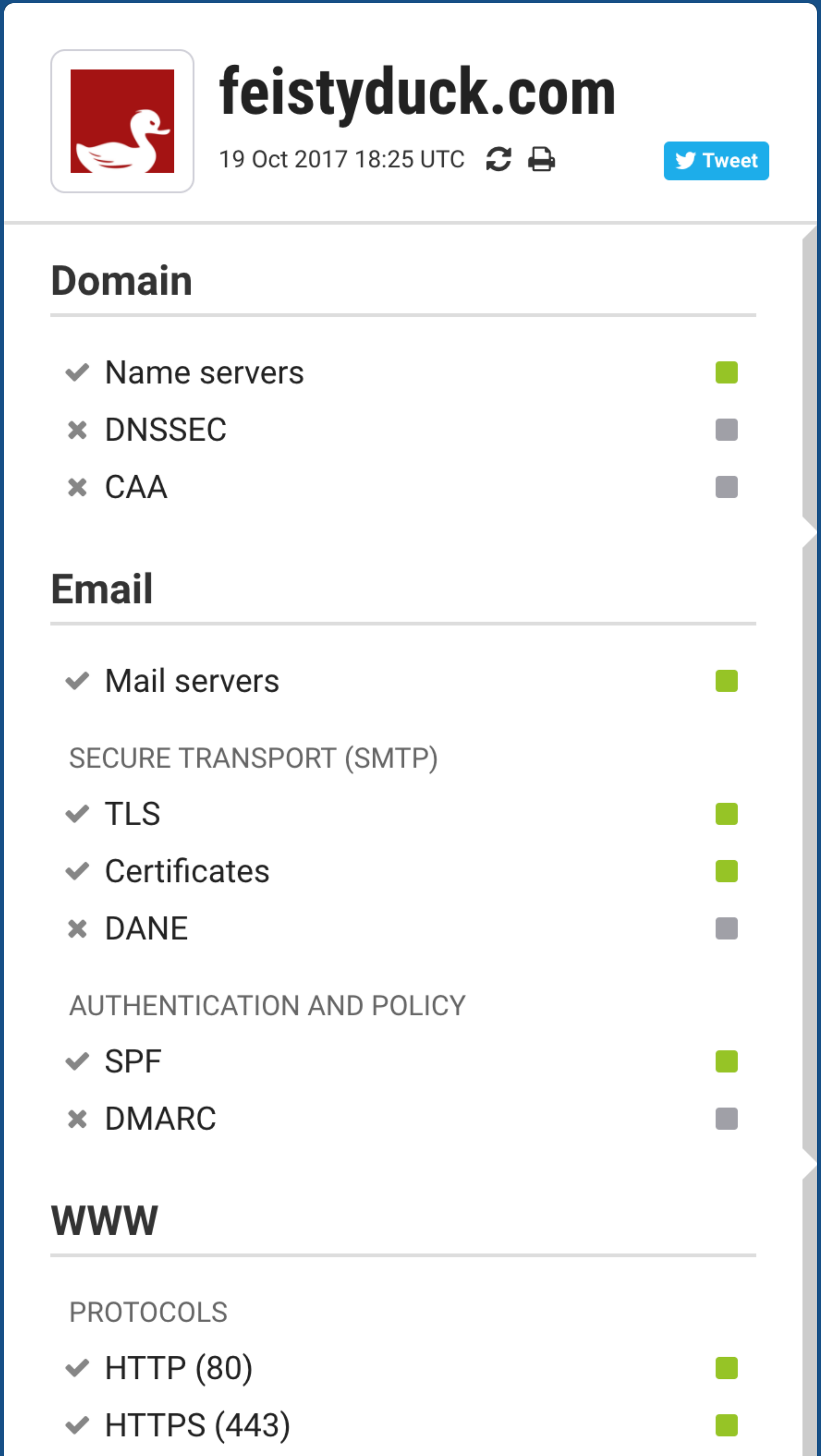
✕ **DMARC**
Domain-based Message Authentication, Reporting, and Conform a mechanism that allows organizations to specify how unauthen (identified using SPF and DKIM) should be handled.

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

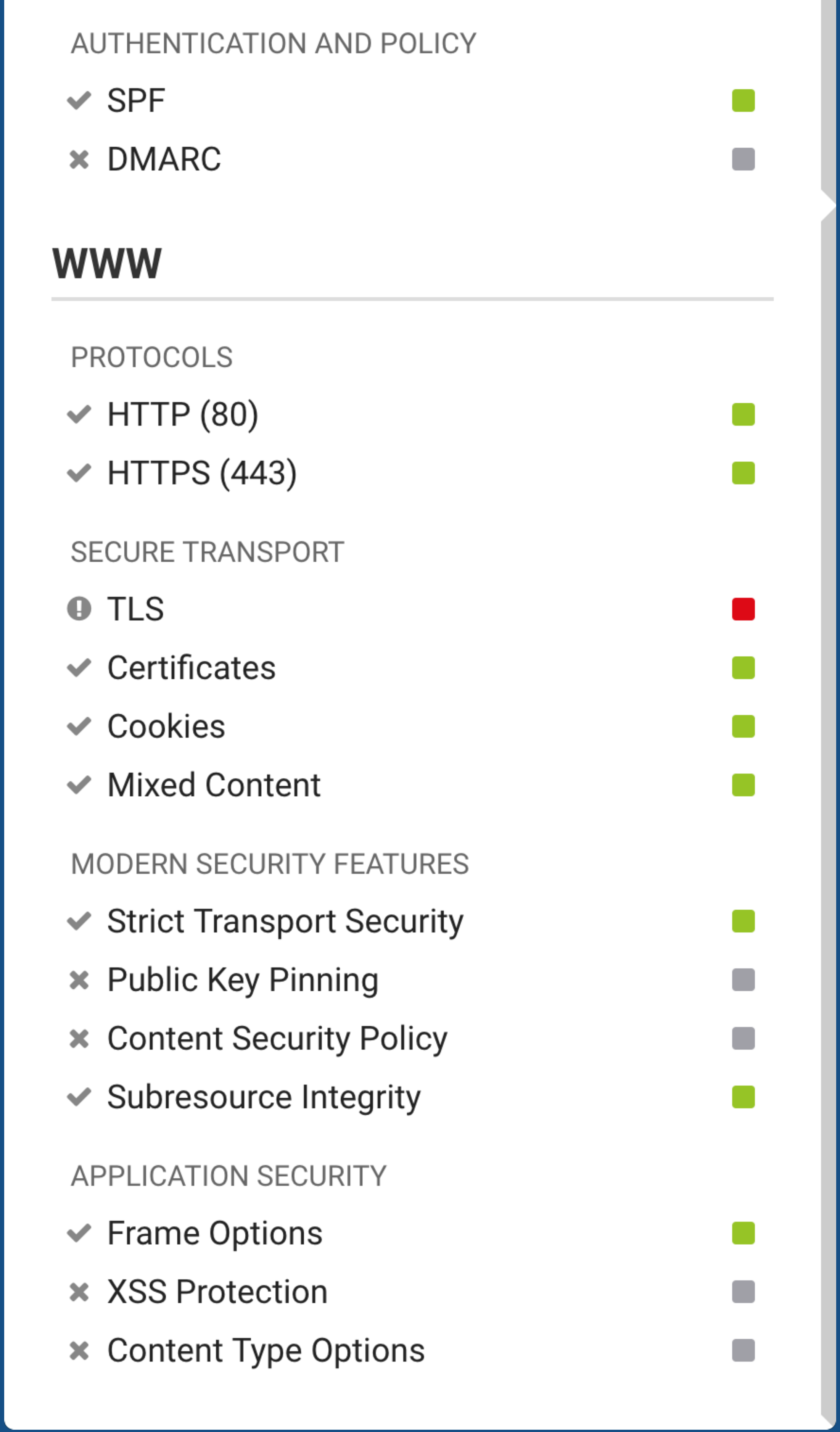
- ✓ HTTP (80) 🟩
- ✓ HTTPS (443) 🟩

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 🟩

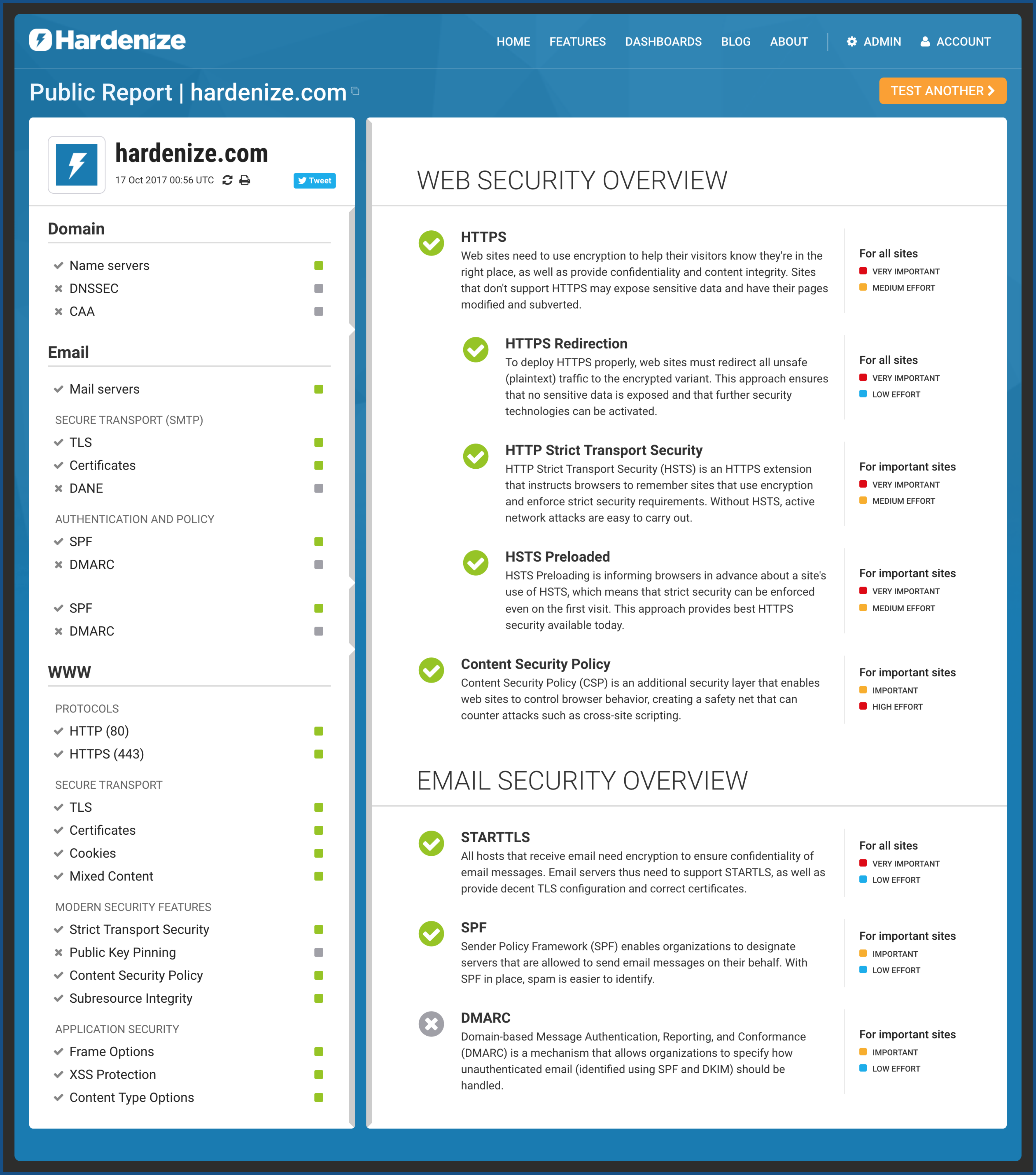
MODERN SECURITY FEATURES

✓ 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**

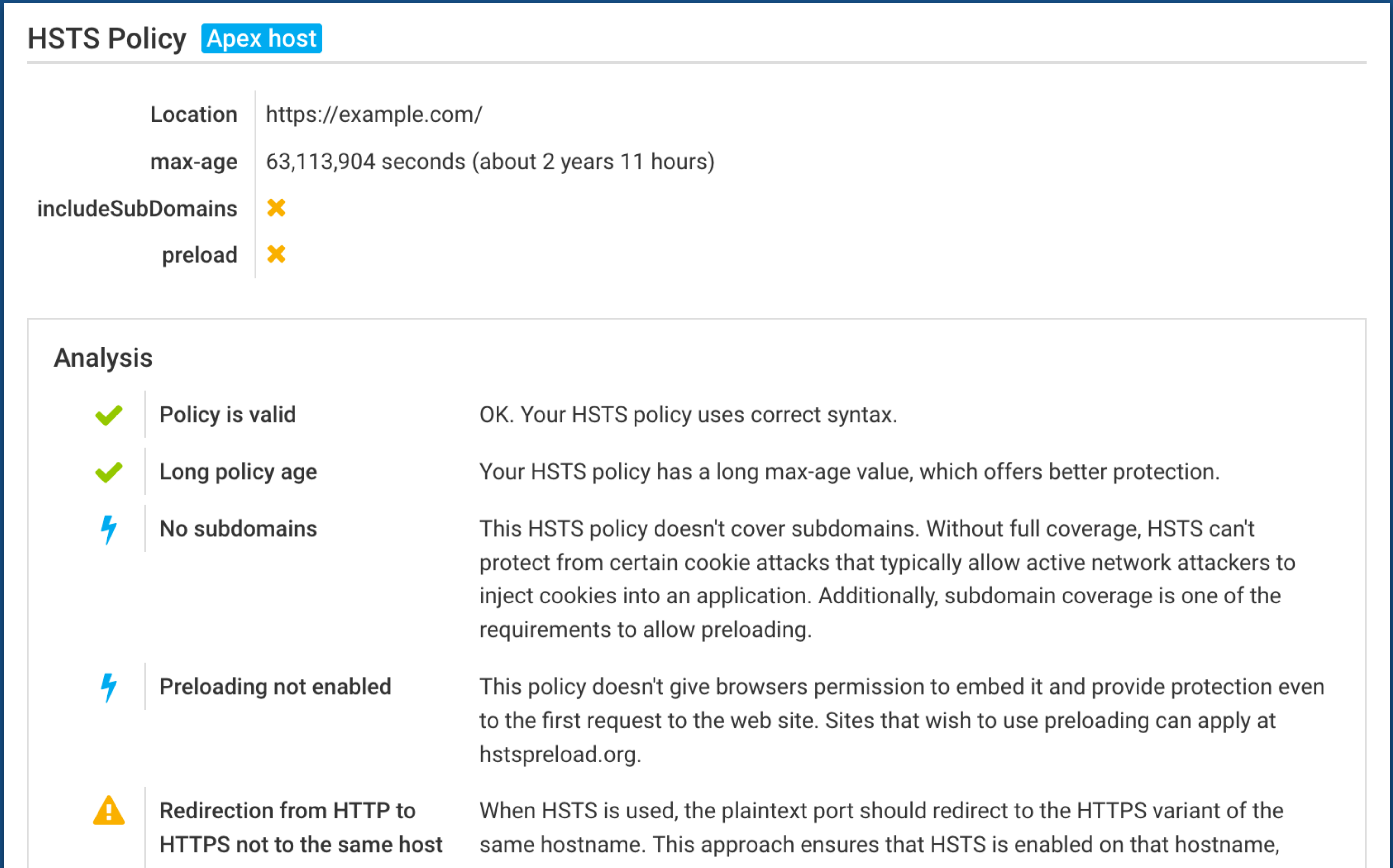
Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism that allows organizations to specify how unauthenticated email (identified using SPF and DKIM) should be handled.

For important sites
🟧 IMPORTANT
🟦 LOW EFFORT

Full data
available
as needed

Ease of Use

Reports show only what they need to, and provide practical advice.



HSTS Policy Apex host

Location	https://example.com/
max-age	63,113,904 seconds (about 2 years 11 hours)
includeSubDomains	✗
preload	✗

Analysis

✓	Policy is valid	OK. Your HSTS policy uses correct syntax.
✓	Long policy age	Your HSTS policy has a long max-age value, which offers better protection.
⚡	No subdomains	This HSTS policy doesn't cover subdomains. Without full coverage, HSTS can't protect from certain cookie attacks that typically allow active network attackers to inject cookies into an application. Additionally, subdomain coverage is one of the requirements to allow preloading.
⚡	Preloading not enabled	This policy doesn't give browsers permission to embed it and provide protection even to the first request to the web site. Sites that wish to use preloading can apply at hstspreload.org.
⚠	Redirection from HTTP to HTTPS not to the same host	When HSTS is used, the plaintext port should redirect to the HTTPS variant of the same hostname. This approach ensures that HSTS is enabled on that hostname,

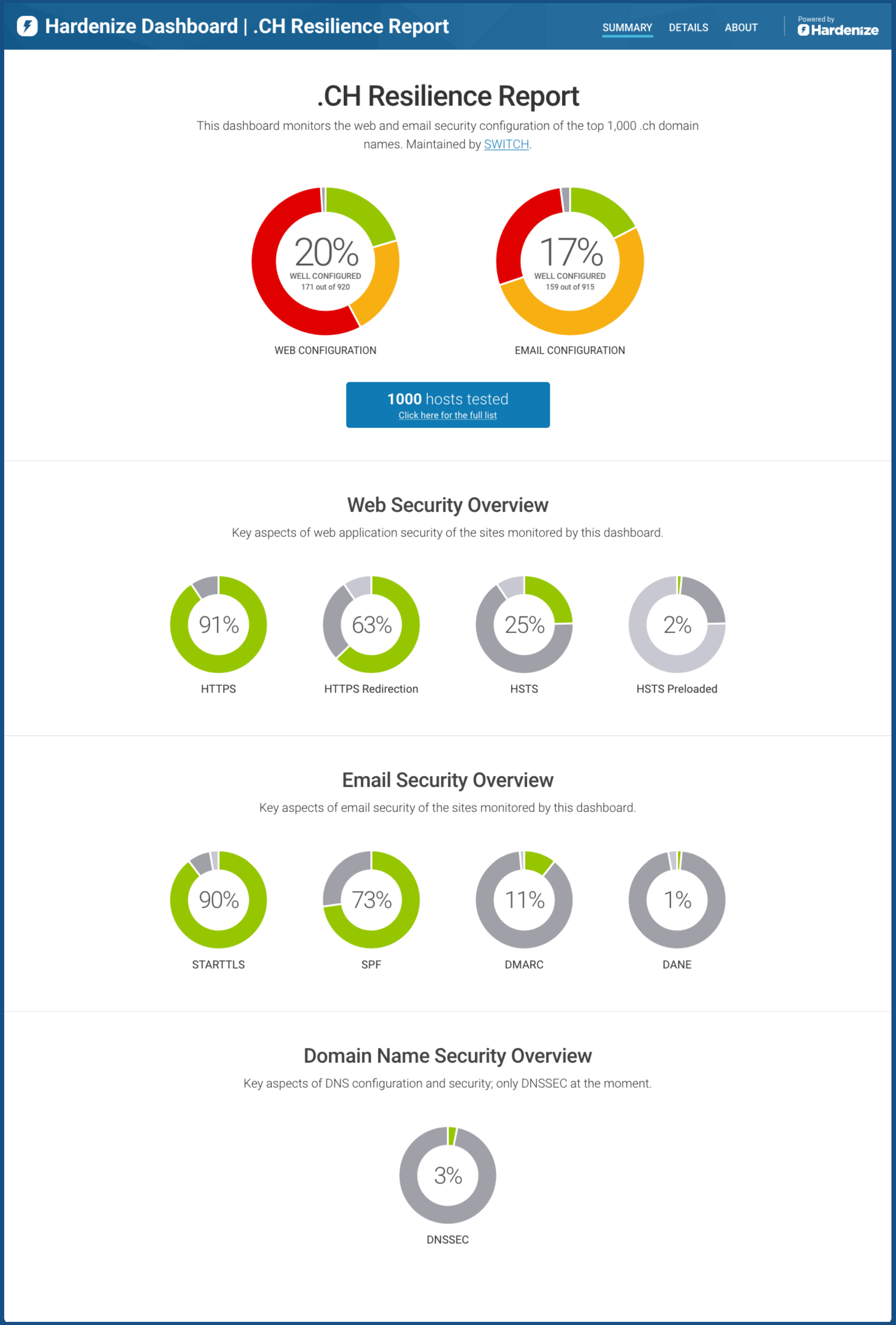
“Doesn’t look like a security product”

— One of our early users

Transparency is a vital ingredient

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

Hardenize



.CH Resilience Report

This dashboard monitors the web and email security configuration of the top 1,000 .ch domain names. Maintained by SWITCH.

20% WELL CONFIGURED 171 out of 920
WEB CONFIGURATION

17% WELL CONFIGURED 159 out of 915
EMAIL CONFIGURATION

1000 hosts tested
Click here for the full list

Web Security Overview

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

91%	63%	25%	2%
HTTPS	HTTPS Redirection	HSTS	HSTS Preloaded

Email Security Overview

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

90%	73%	11%	1%
STARTTLS	SPF	DMARC	DANE

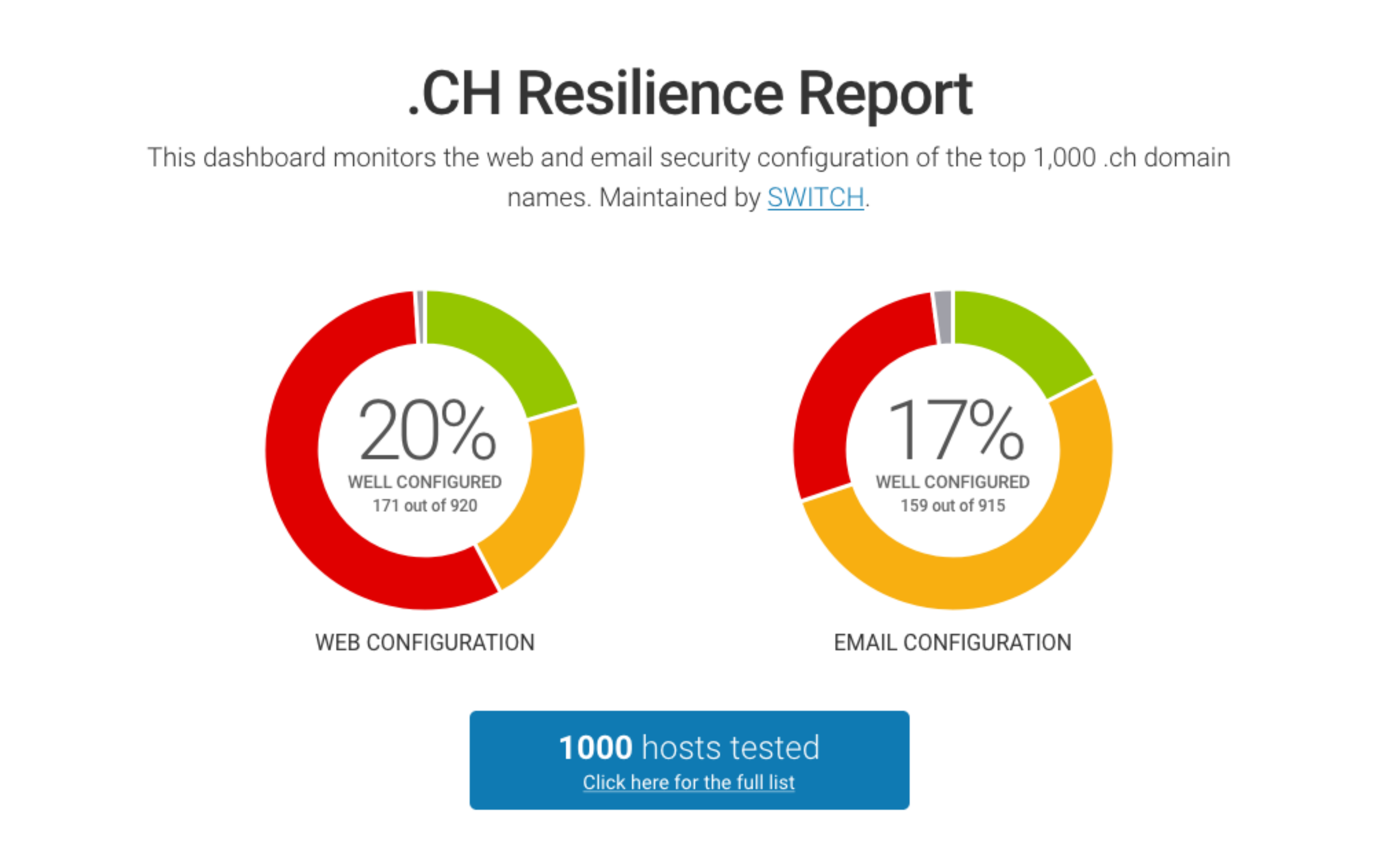
Domain Name Security Overview

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

3%
DNSSEC

Public dashboards

In partnership with official organisations

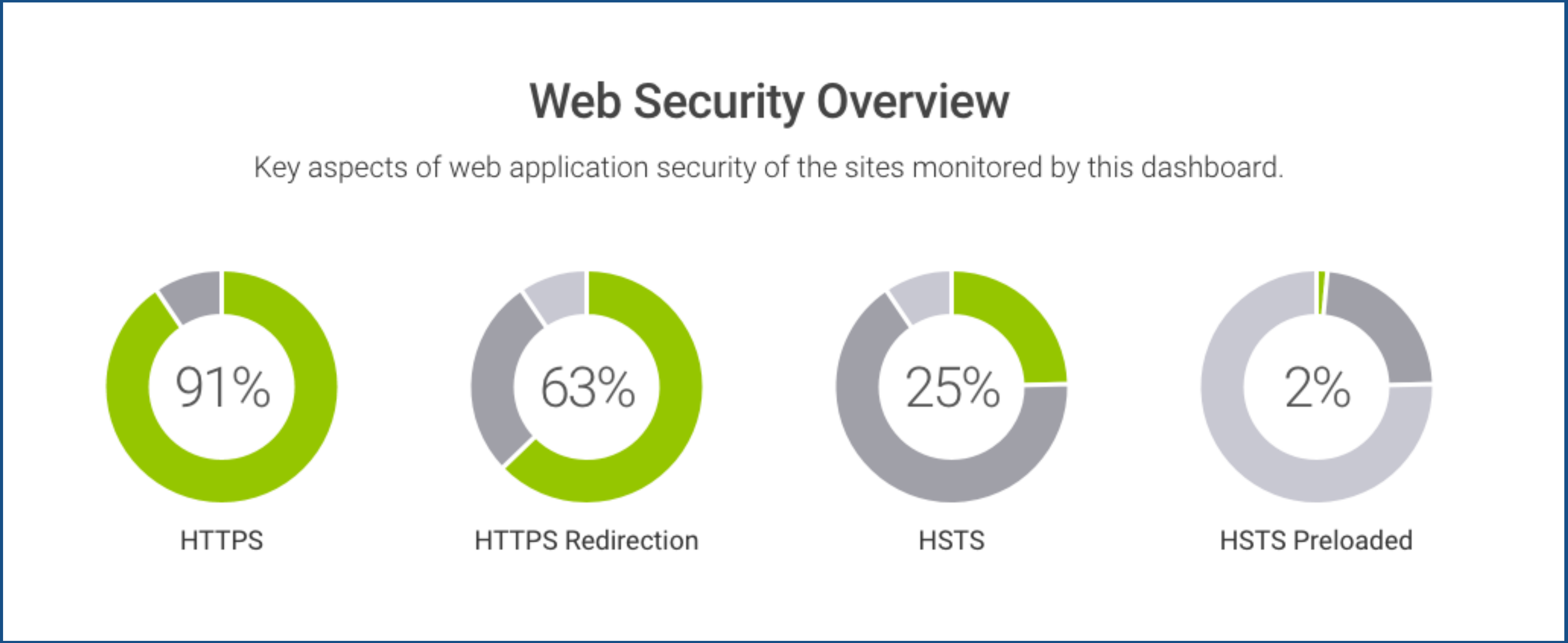


.CH Resilience Report

This dashboard monitors the web and email security configuration of the top 1,000 .ch domain names. Maintained by SWITCH.

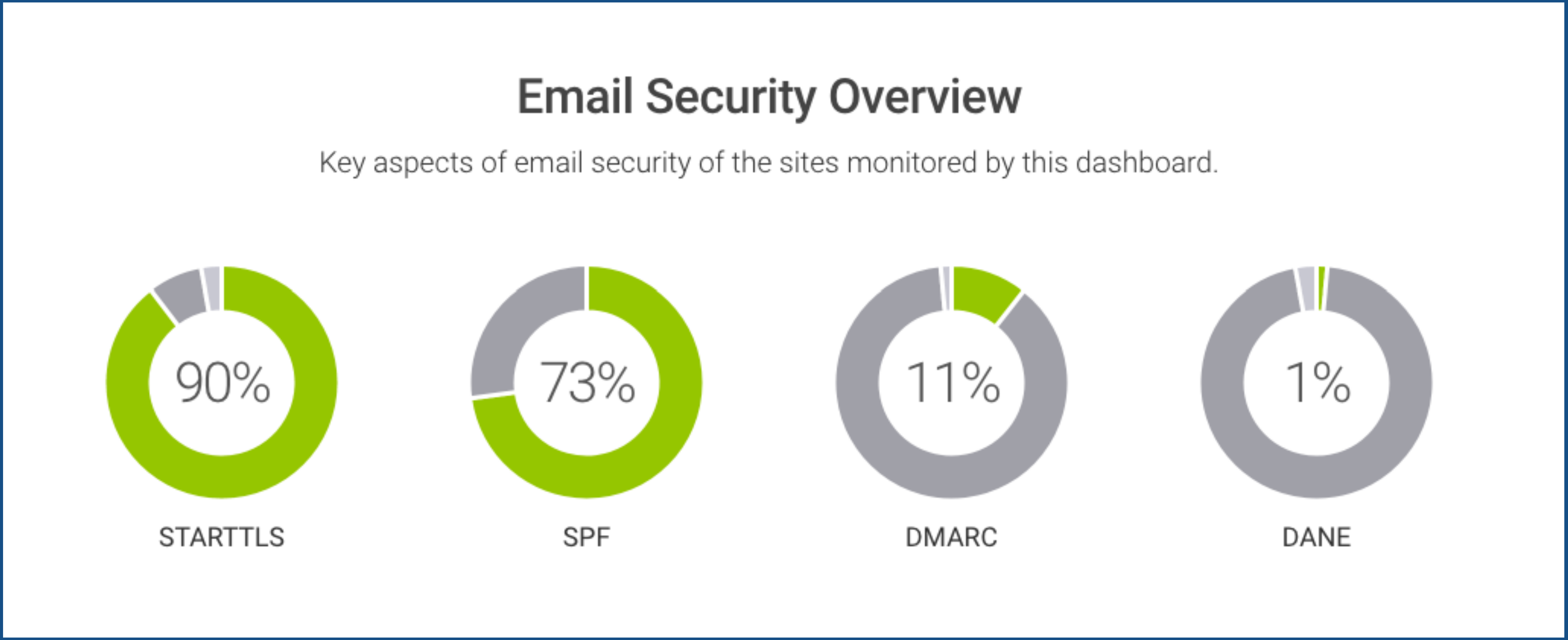
1000 hosts tested

Click here for the full list



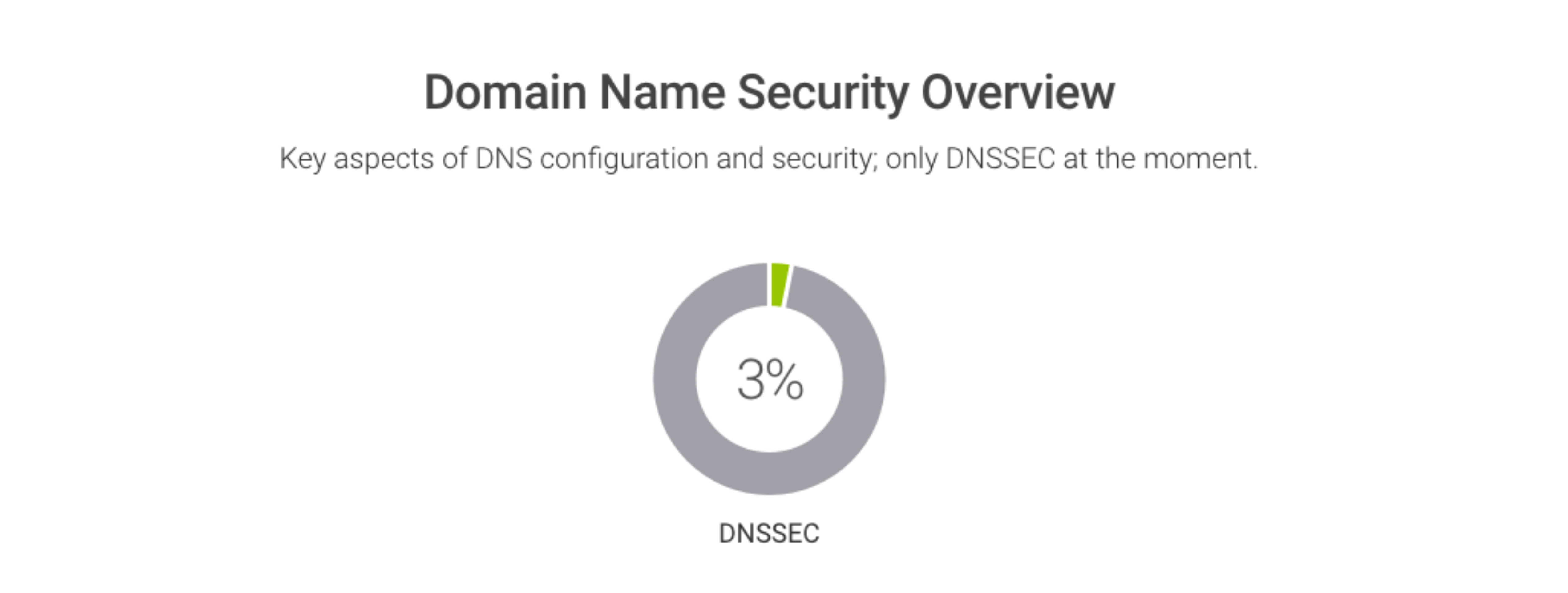
Web Security Overview

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



Email Security Overview

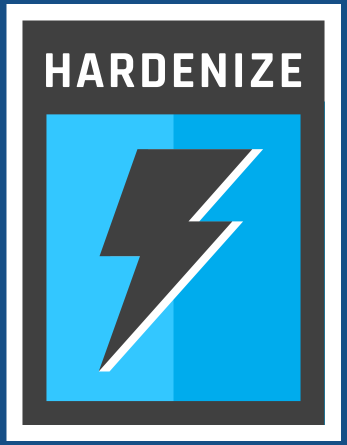
Key aspects of email security of the sites monitored by this dashboard.



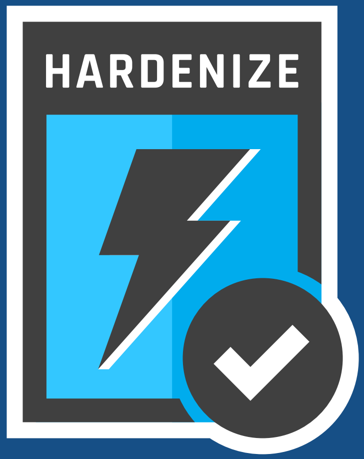
Domain Name Security Overview

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

Web site badges



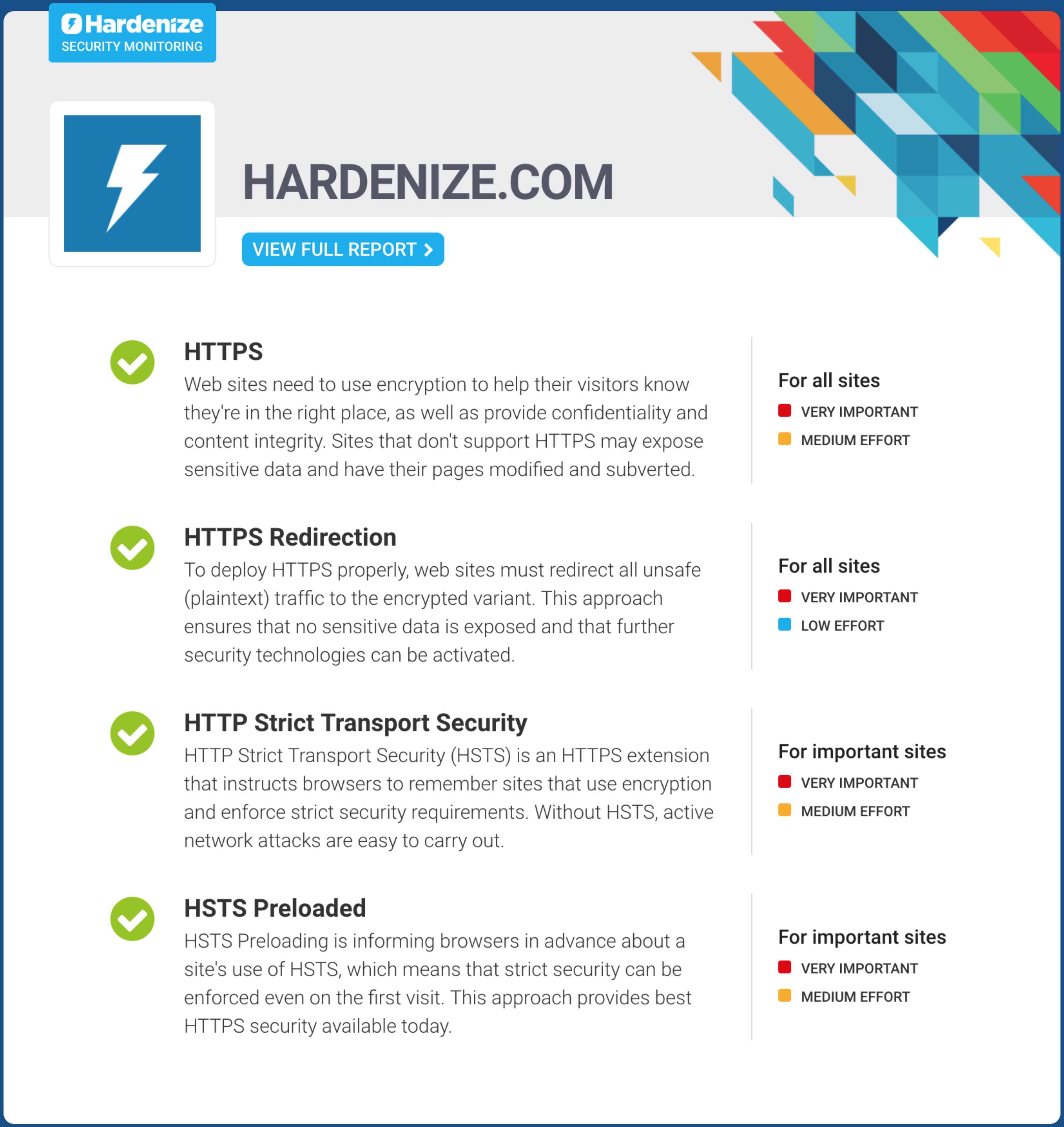
Everyone starts with the default badge



If you have robust HTTPS you get this one instead

Hardenize

Simplified to focus on most important aspects first.



Hardenize
SECURITY MONITORING

HARDENIZE.COM

VIEW FULL REPORT ›

✓ **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

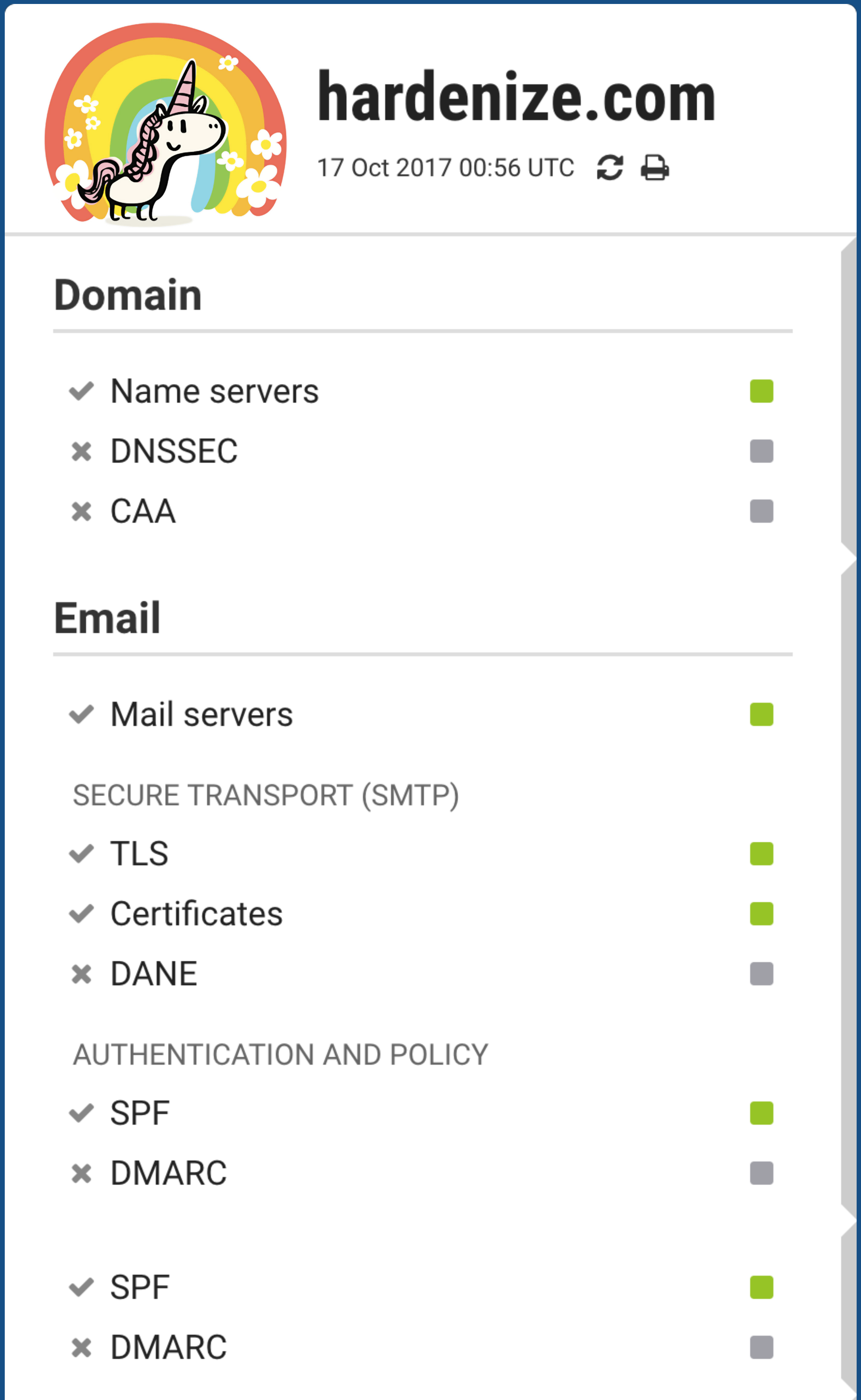
Free public assessments

Public dashboards

Security badge

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 ■