

# Purpose-Driven Design in Computer Security: My SSL Labs Journey

Ivan Ristić

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

**Good security is possible,  
but at a substantial cost.**

**Not all can afford it.**

**New systems are not built in  
isolation: platforms, tools,  
documentation, know-how, all of  
that needs to change before we  
can move on...**

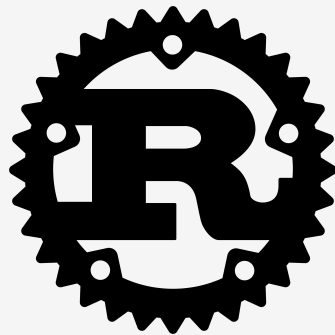




**Fixing the Internet is like fixing a plane while in the air.**

**Existing [insecure] platforms  
can't be saved. Learn, then  
move on. Focus on making new  
platforms secure by default.**

**Our goal should be to  
change the collective  
mindset so that security  
becomes the new norm.**



**It's working!**

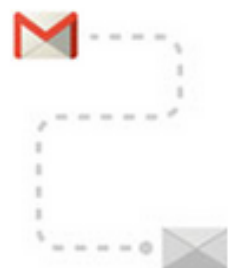
# Google Transparency Report

## How much email was encrypted in transit?



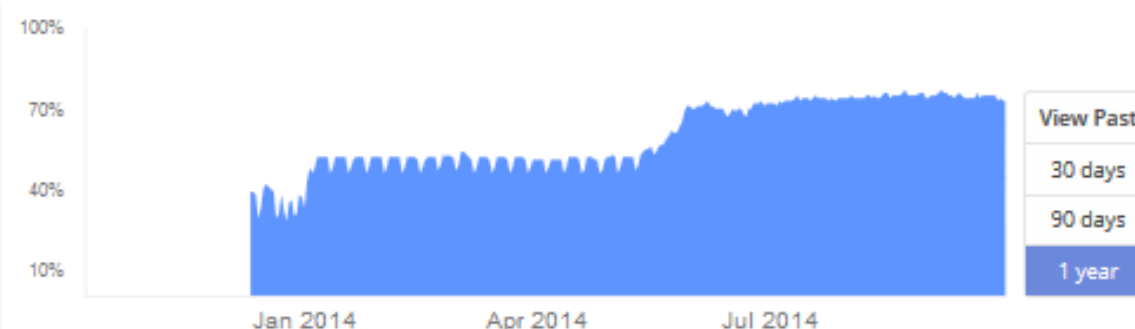
Generally speaking, use of encryption in transit increases over time, as more providers enable and maintain their support. Factors such as varying volumes of email may explain other fluctuations.

### Outbound

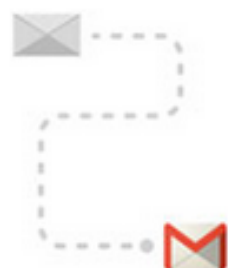


73%

Messages from Gmail to other providers.

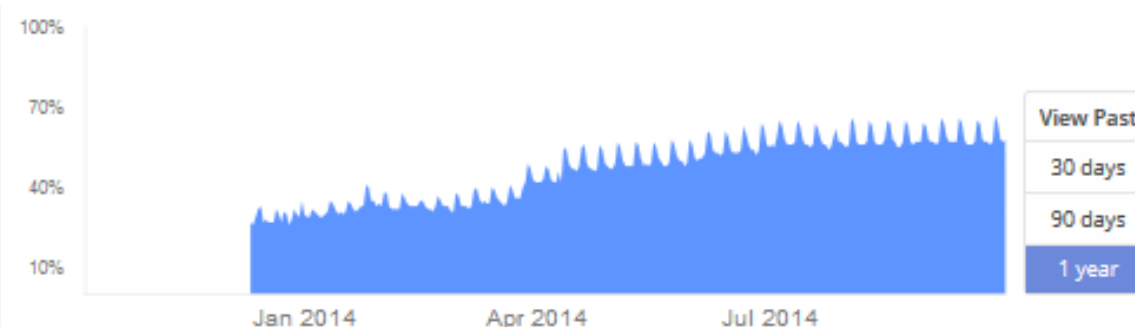


### Inbound



58%

Messages from other providers to Gmail.



### Outbound

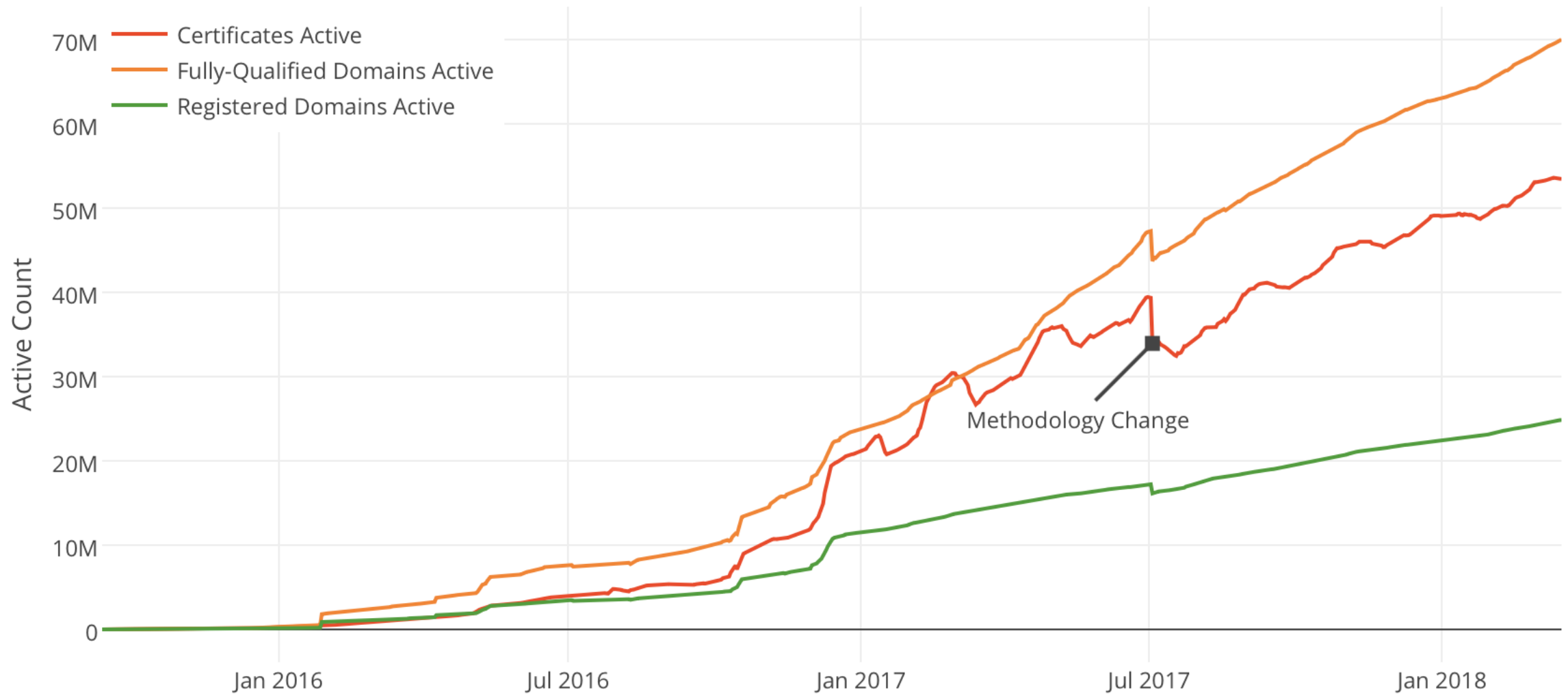
Jan 2014: 30%  
Sep 2018: 90%

### Inbound

Jan 2014: 25%  
Sep 2018: 89%

# Let's Encrypt Growth

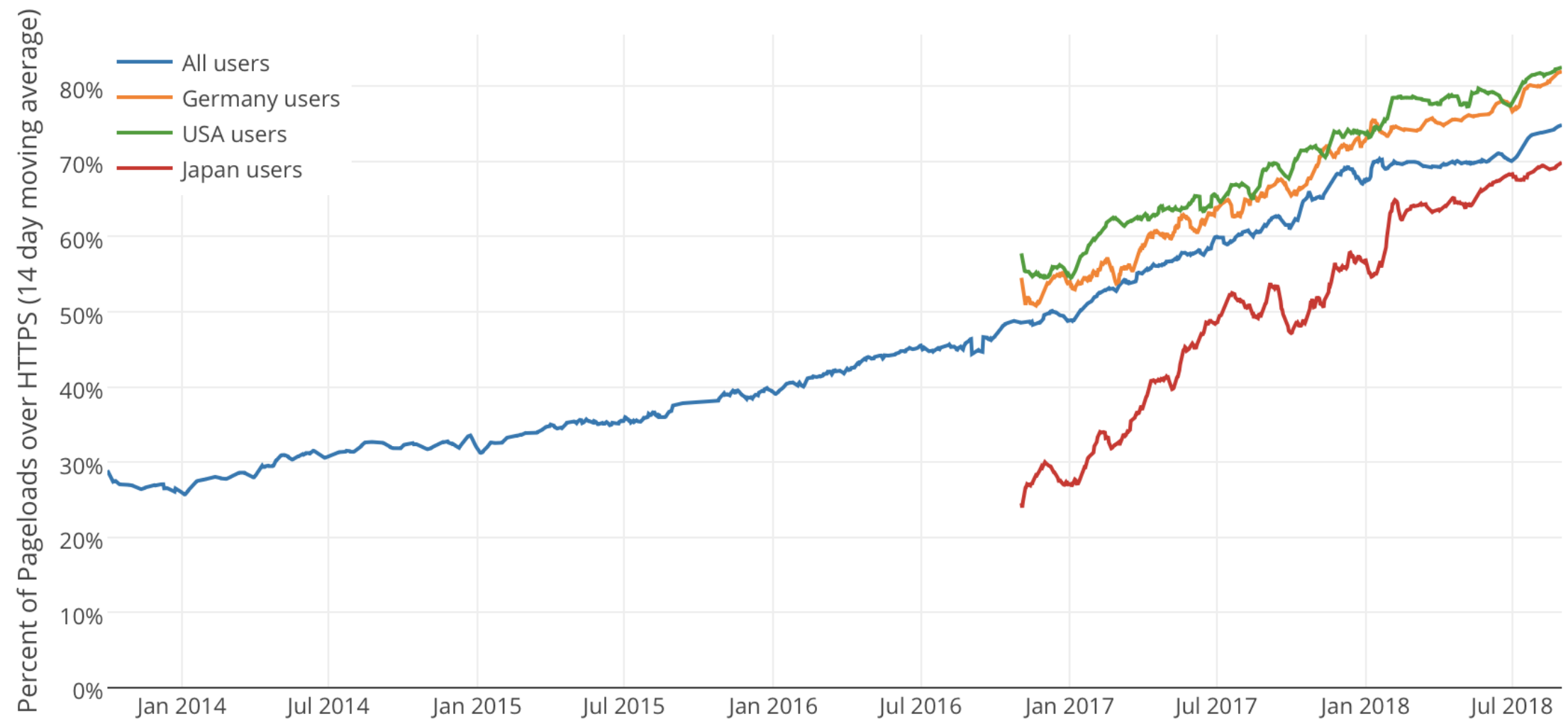
## Let's Encrypt Growth



# HTTPS pages over 80%

## Percentage of Web Pages Loaded by Firefox Using HTTPS

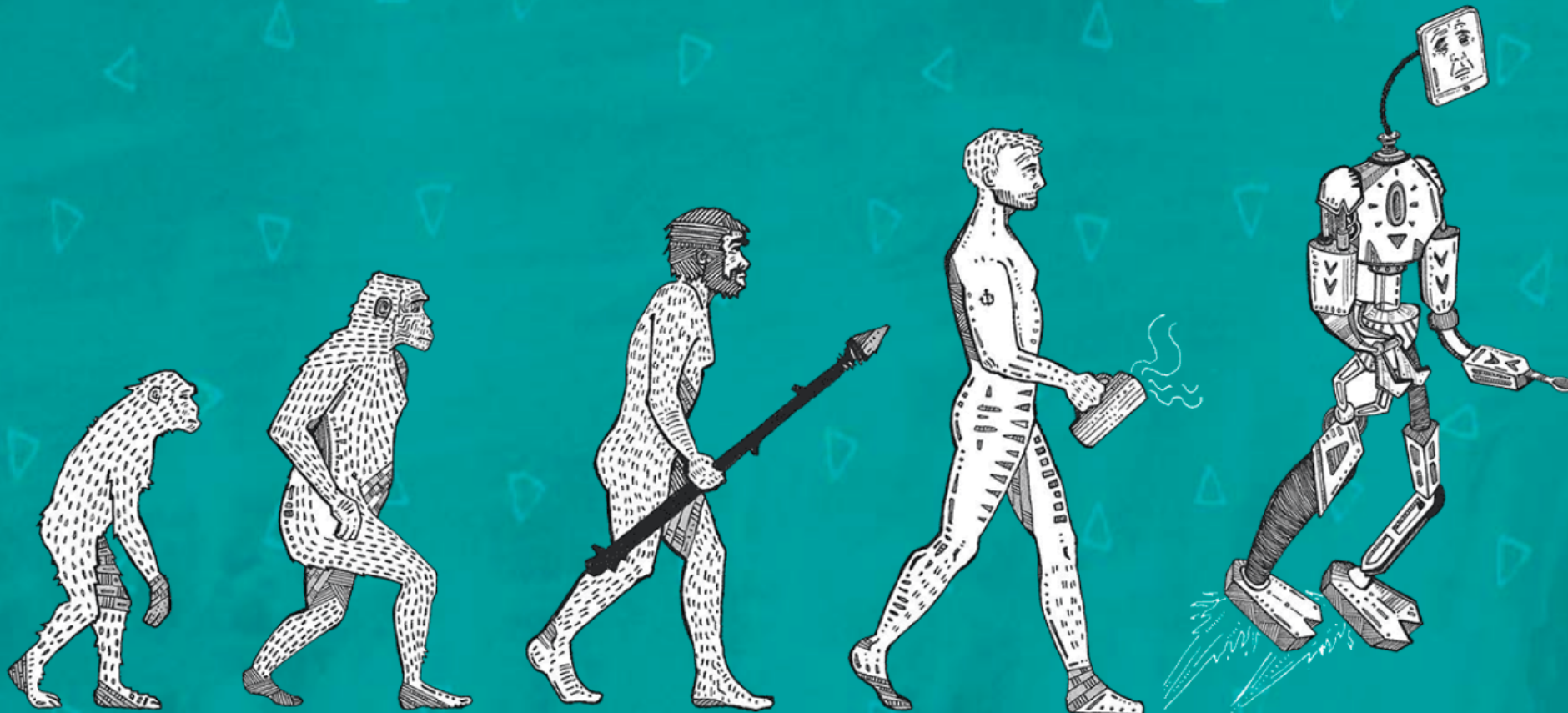
(14-day moving average, source: [Firefox Telemetry](#))





**Catch:** Most of these work  
only if the ecosystem is  
ready for the change.

# LEVEL UP HUMAN



Possible → Documented →  
Achievable → Convenient  
→ Widespread



# SSL Labs



[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

## HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.



### Test your server »

Test your site's certificate and configuration



### Test your browser »

Test your browser's SSL implementation



### SSL Pulse »

See how other web sites are doing



### Documentation »

Learn how to deploy SSL/TLS correctly

### Books



[\*\*Bulletproof SSL and TLS\*\*](#) is a complete guide to deploying secure servers and web applications. This book, which provides comprehensive coverage of the ever-changing field of SSL/TLS and Web PKI, is intended for IT security professionals, system

administrators, and developers, with the main focus on getting things done. [MORE »](#)

### News

#### [\*\*The Digital Transformation Age Is Dawning: Do You Know Where Your Certificates Are?\*\*](#)

June 6, 2018

#### [\*\*SSL Labs Grading Update: Forward Secrecy, Authenticated Encryption and ROBOT\*\*](#)

February 3, 2018

#### [\*\*Google and Mozilla are Deprecating Existing Symantec Certificates\*\*](#)

September 26, 2017

### About SSL Labs

SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved.

SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL.

-- Ivan Ristić, Qualys

# **“Try it now”**

Remove the barrier to entry by  
making tools easily available.

# SSL Labs Test



[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > SSL Server Test

## SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

Submit

☐ Do not show the results on the boards

### Recently Seen

[app.tablein.com](#)  
[uatpo4.cbre.com](#)  
[po.cbre.com](#)  
[plotter-folien.com](#)  
[apps.villeesch.lu](#)  
[mdm.apis-it.hr](#)  
[ebank.taipeifubon.com.tw](#)  
[myicheme.icheme.org](#)  
[www.bamsoftware.com](#)  
[l1rocks.r.worldssl.net](#)

Err

### Recent Best

[events.steinbeisschule-reutl ...](#) A+  
[oso.dhl.fi](#) A+  
[studenttenant.com](#) A+  
[www.sogndal.kommune.no](#) A  
[www.ecotank-easypay.eu](#) A  
[pic.ctrip.com](#) A  
[mitra.indogrosir.co.id](#) A  
[babyliss.fr](#) A  
[optenerges.convis.lu](#) B  
[box.p365services.com](#) B

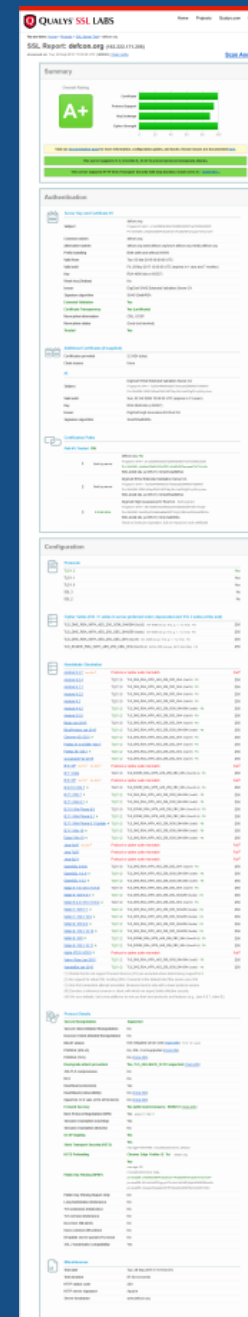
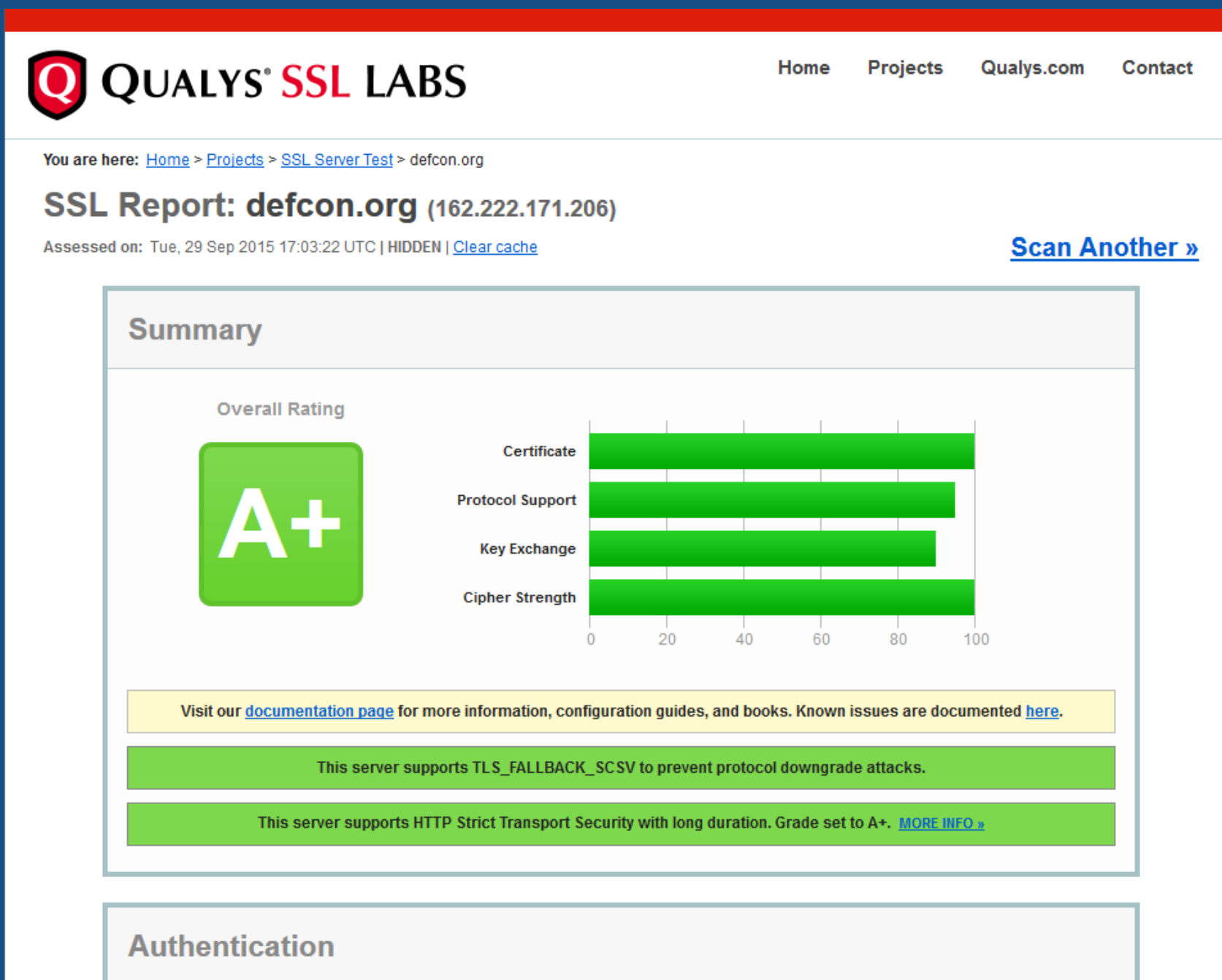
### Recent Worst

[demo-auto.dispatch.nl](#) F  
[portal.cenzo.nl](#) F  
[www.infodesk.nl](#) T  
[benefit.osohshiki.com](#) F  
[plasmatreteat.com.tr](#) T  
[sigma.speedcast.com](#) F  
[www.armstrong.nu](#) T  
[raad.zutphen.nl](#) T  
[enisbtpre.amadeusitalia.it](#) F  
[r4wt.infobolsa.es](#) F

# **Make it easy to understand**

Give users technical information they need,  
but structure it so that they know exactly  
where they stand.

# SSL Labs Report









# **Make the goals clear**


No confusion about what the  
next step should be.

# SSL Server Rating Guide



[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

 [ssllabs / research](#)

[Unwatch](#) 200 [Unstar](#) 1,209 [Fork](#) 123

[Code](#) [Pull requests](#) 0 [Projects](#) 0 [Wiki](#) [Insights](#) [Settings](#)

## SSL Server Rating Guide

[Edit](#) [New Page](#)

Yash K S edited this page 26 days ago · 34 revisions

### Version 2009o (8 May 2017)

The Secure Sockets Layer (SSL) protocol is a standard for encrypted network communication. We feel that there is surprisingly little attention paid to how SSL is configured, given its widespread usage. SSL is relatively easy to use, but it does have its traps. This guide aims to establish a straightforward assessment methodology, allowing administrators to assess SSL server configuration confidently without the need to become SSL experts.

### Methodology Overview

Our approach consists of four steps:

1. We first look at a certificate to verify that it is valid and trusted.
2. We inspect server configuration in three categories:
3. Protocol support
4. Key exchange support
5. Cipher support
6. We combine the category scores into an overall score (expressed as a number between 0

▼ Pages 23

[Home](#)

[Assessment Tools](#)

[Attack Tools](#)

[BEAST](#)

[Configuration tools](#)

[CRIME](#)

[Extended Validation Certificates](#)

[FIPS Requirements](#)

[Forward Secrecy](#)

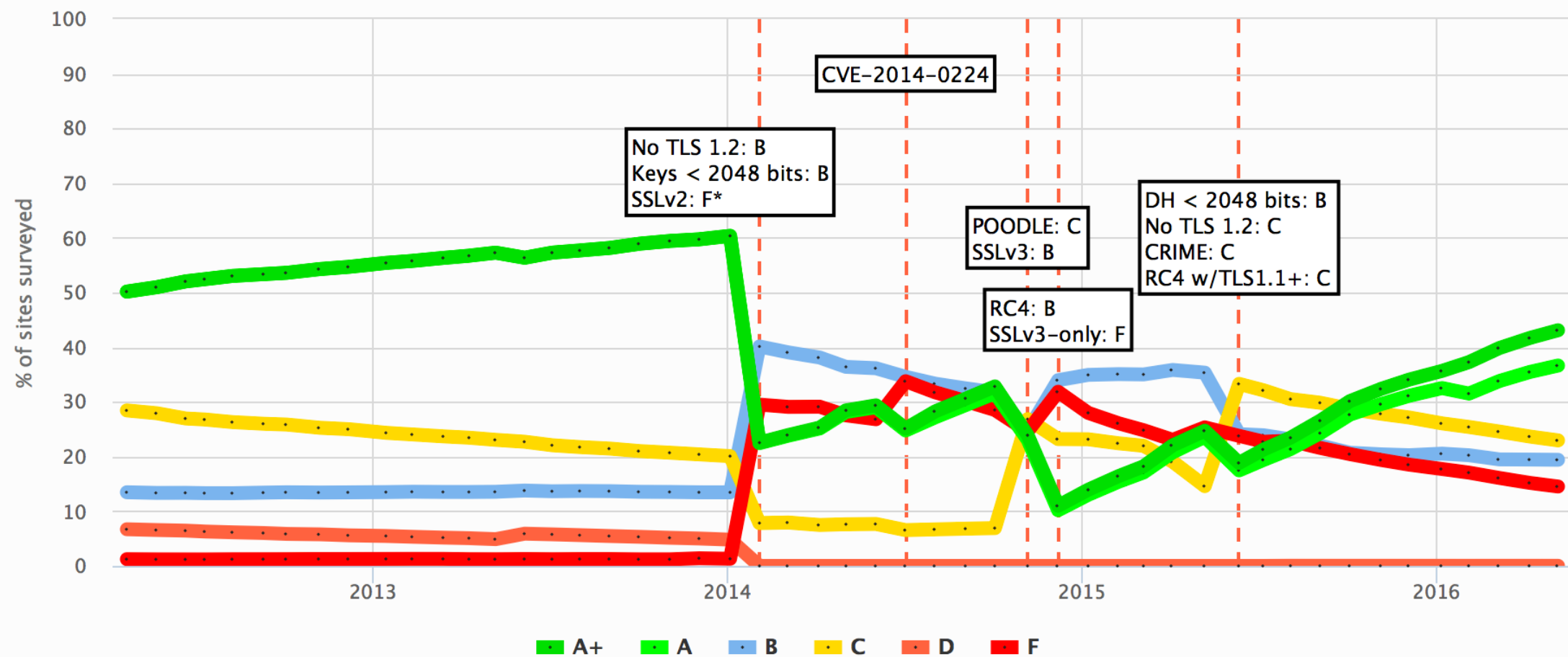
[Interoperability Test Servers](#)

# **Get the incentives right, keep moving**

Develop useful grading criteria that  
makes the next step just out of reach.

# SSL Pulse

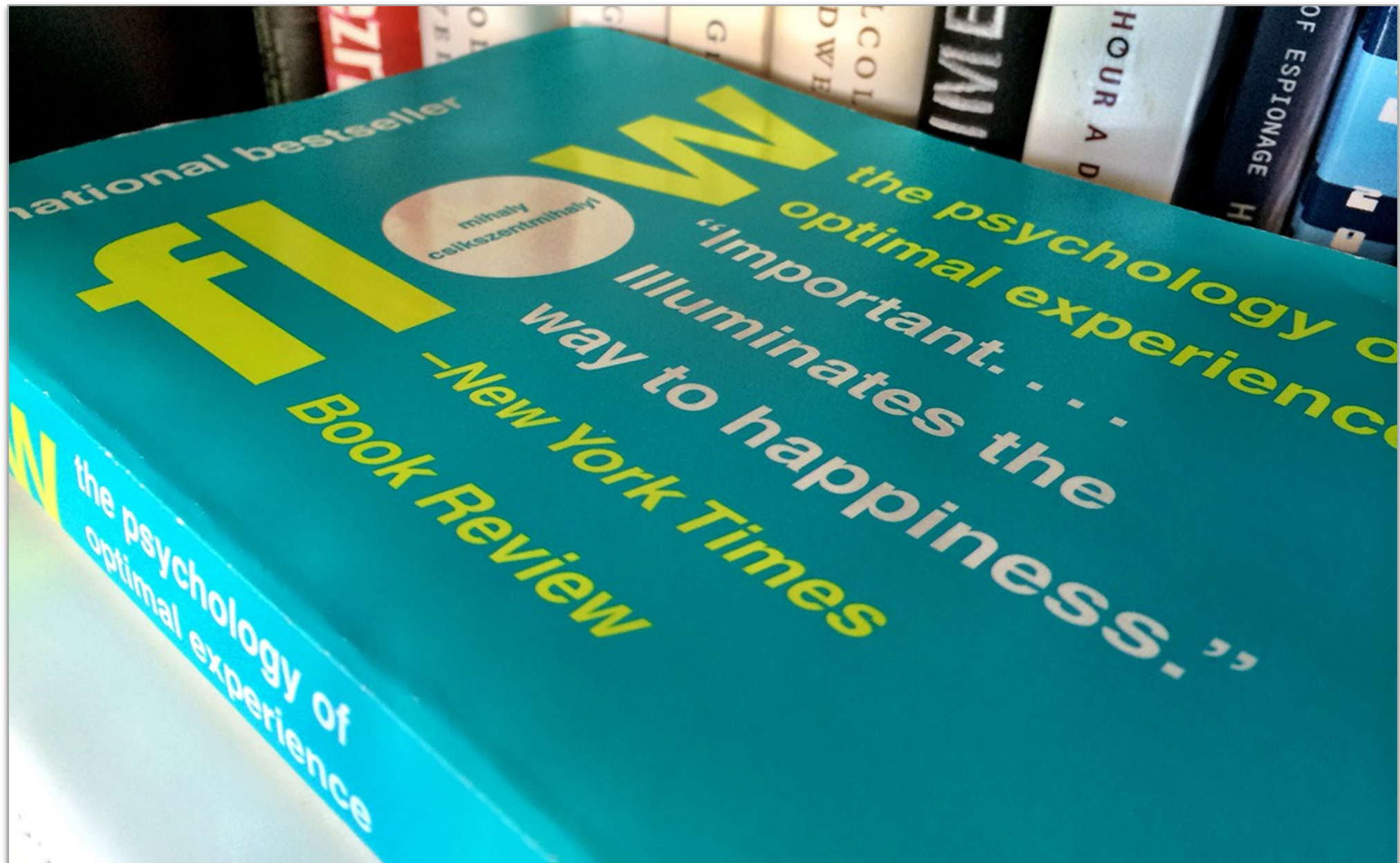
## SSL Labs Grade



# **Awareness is a vital ingredient**

Awareness starts conversations.  
Conversations lead to urgency. Urgency  
creates budget. Things get done.

# Flow: The Psychology of optimal experience





## Elevation of Privilege: Drawing Developers into Threat Modeling

Adam Shostack  
*adam.shostack@microsoft.com*

### Abstract

This paper presents Elevation of Privilege, a game designed to draw people who are not security practitioners into the craft of threat modeling. The game uses a variety of techniques to do so in an enticing, supportive and non-threatening way. The subject of security tools for software engineering has not generally been studied carefully. This paper shares the objectives and design of the game, as well as tradeoffs made and lessons learned while building it. It concludes with discussion of other areas where games may help information security professionals reach important goals.

### 1 Background

Software rarely becomes secure by luck. Software security usually requires focused engineering activities. Taking action to threat model a system under development is unusual, and usually happens only if there's a security enthusiast on the team, or if an organization has adopted some set of security practices. Both situations are rare, with lamentable consequences for the security of software, systems and critical infrastructures. When threat modeling happens, it is usually done by experts who have

that underlies this the practitioners. spect from threat r sus software devel lap, and as obvic falls squarely into

### 1.1 Tradeoffs

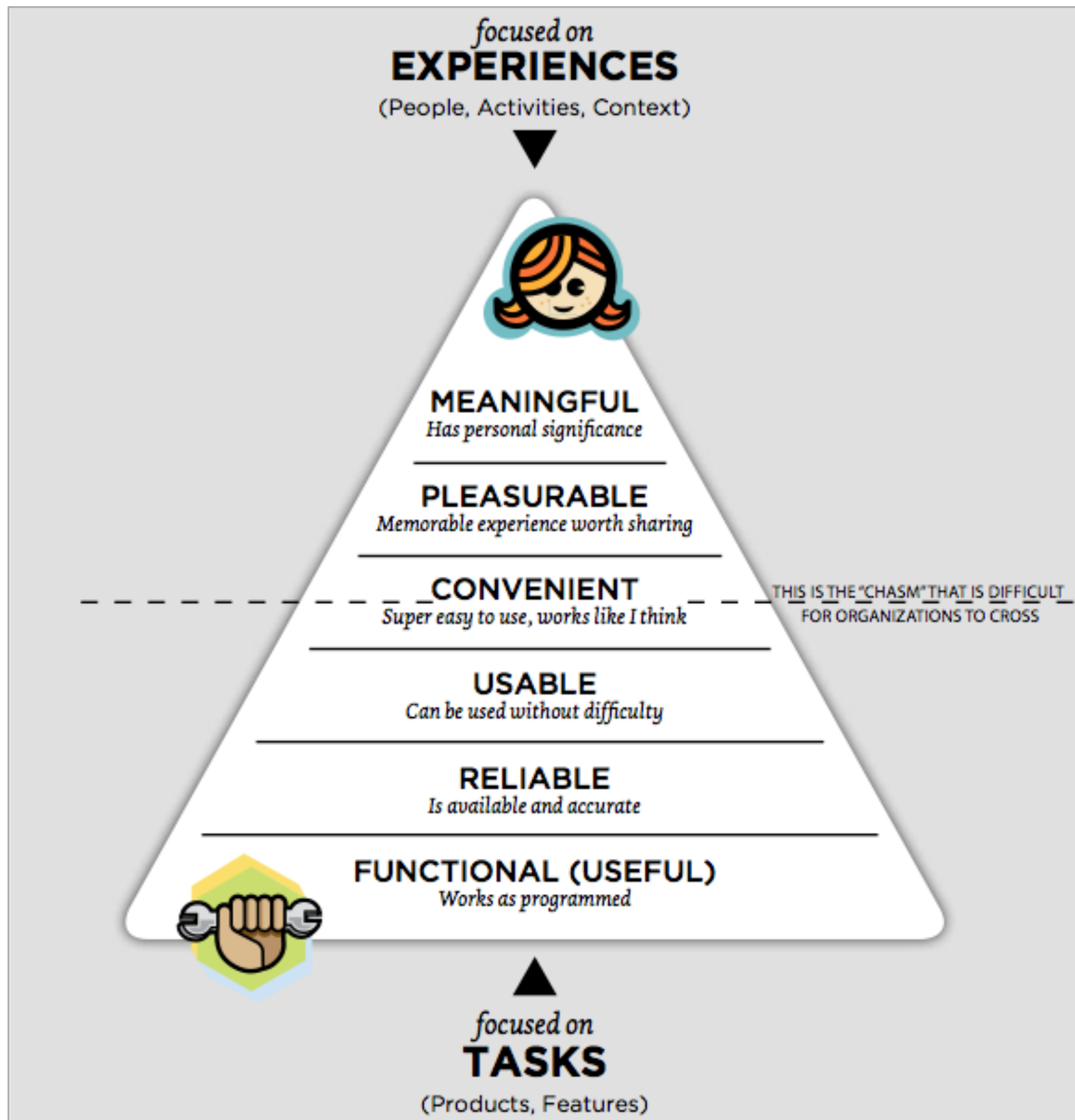
Threat modeling obvious advantages knowledge and t ing that experts c assume that expe activities. Howe downsides, and d obvious advantag what the code re involved in sugge are always presen being made, and c project. Training that the skills are "whiteboard" leve are rare and expensive. If it were possible to have de-

## 1.6 Psychology and Sociology

The Elevation of Privilege work draws on a number of areas of psychology and sociology which are worth discussing. A full discussion is beyond the scope of this paper, and references have been selected for accessibility to a security audience. The commonalities here are cognitive biases, as well as the different relationships that experts and beginners have with tasks, and with each other as they execute those tasks.

The first set of related work is Csíkszentmihályi's concept of flow [7]. Flow is a state of undistracted concentration on a task at hand, and is associated with effective performance by experts in many fields. Csíkszentmihályi describes "the person is fully immersed in what he or she is doing, characterized by a feeling of energized focus, full involvement, and success." Many structured approaches to threat modeling actively inhibit flow in both beginners and experts, and few allow it to emerge. The apparent lack of flow in threat modeling by developers was one of the motivators for this work. Other elements of flow include:

1. The activity is intrinsically rewarding
2. People become absorbed in the activity\*
3. A loss of the feeling of self-consciousness\*
4. Distorted sense of time
5. A sense of personal control over the situation or activity\*
6. Clear goals\*
7. Concentrating and focusing
8. Direct and immediate feedback\*



“Seductive Interaction Design”, by Stephen P. Anderson



*focused on*  
**EXPERIENCES**  
(People, Activities, Context)



**MEANINGFUL**  
*Has personal significance*

**PLEASURABLE**  
*Memorable experience worth sharing*

**CONVENIENT**  
*Super easy to use, works like I think*

THIS IS THE "CHASM" THAT IS DIFFICULT  
FOR ORGANIZATIONS TO CROSS

**USABLE**  
*Can be used without difficulty*

**RELIABLE**  
*Is available and accurate*



**FUNCTIONAL (USEFUL)**  
*Works as programmed*



*focused on*  
**TASKS**  
(Products, Features)

*focused on*  
**EXPERIENCES**  
(People, Activities, Context)



**MEANINGFUL**  
*Has personal significance*

**PLEASURABLE**  
*Memorable experience worth sharing*

**CONVENIENT**  
*Super easy to use, works like I think*

**USABLE**  
*Can be used without difficulty*

**RELIABLE**  
*Is available and accurate*

**FUNCTIONAL (USEFUL)**  
*Works as programmed*



*focused on*  
**TASKS**  
(Products, Features)



IS THE "CROSS" THAT IS DIFFICULT  
FOR ORGANIZATIONS TO CROSS

*focused on*  
**EXPERIENCES**  
(People, Activities, Context)



**MEANINGFUL**

*Has personal significance*

**PLEASURABLE**

*Memorable experience worth sharing*

**CONVENIENT**

*Super easy to use, works like I think*

**USABLE**

*Can be used without difficulty*

**RELIABLE**

*Is available and accurate*

**FUNCTIONAL (USEFUL)**

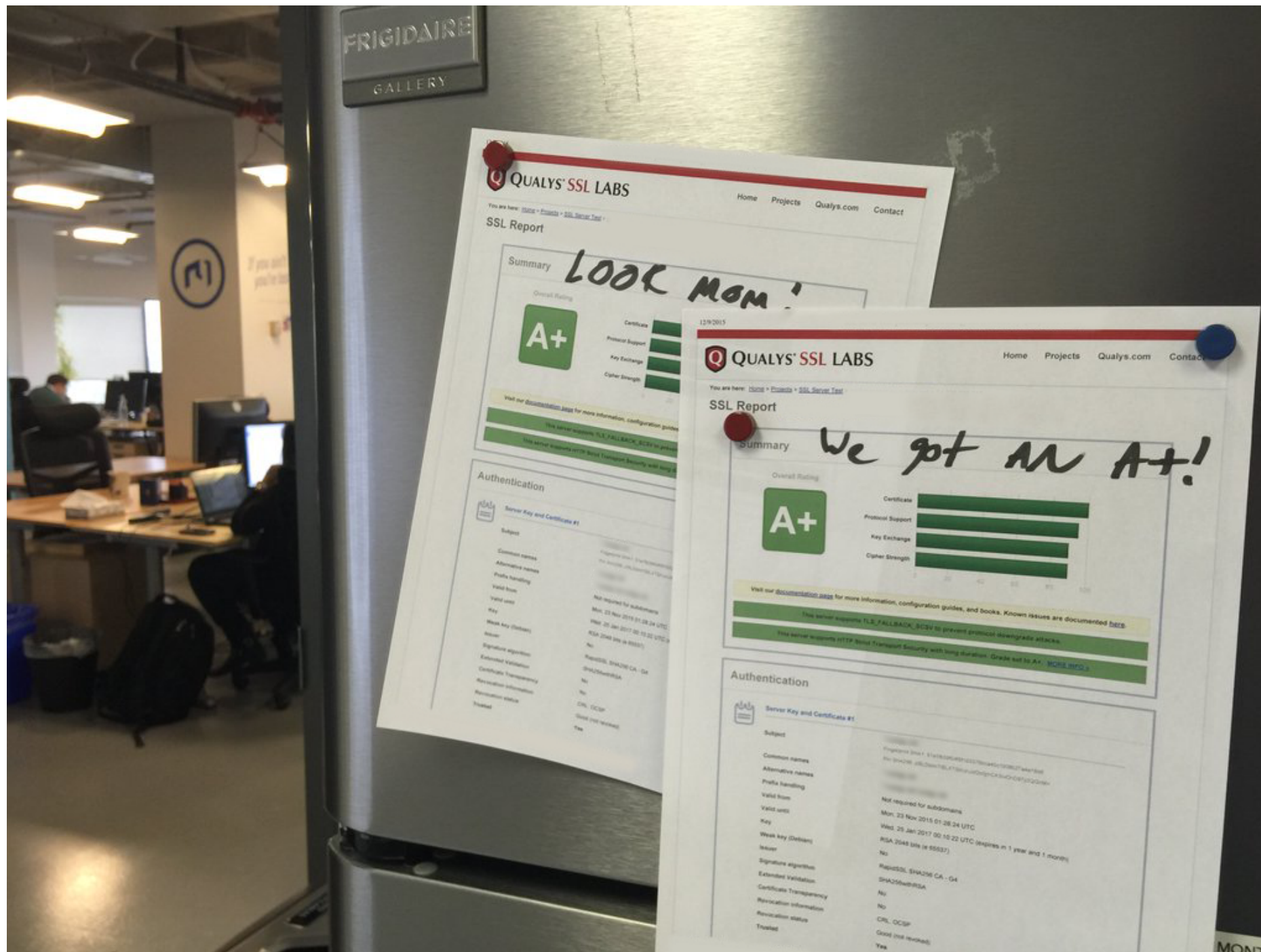
*Works as programmed*



*focused on*  
**TASKS**  
(Products, Features)



IS THE "CHASM" THAT IS DIFFICULT  
FOR ORGANIZATIONS TO CROSS



# **Make security interesting and fun**

Usable security that  
people actually want to use.



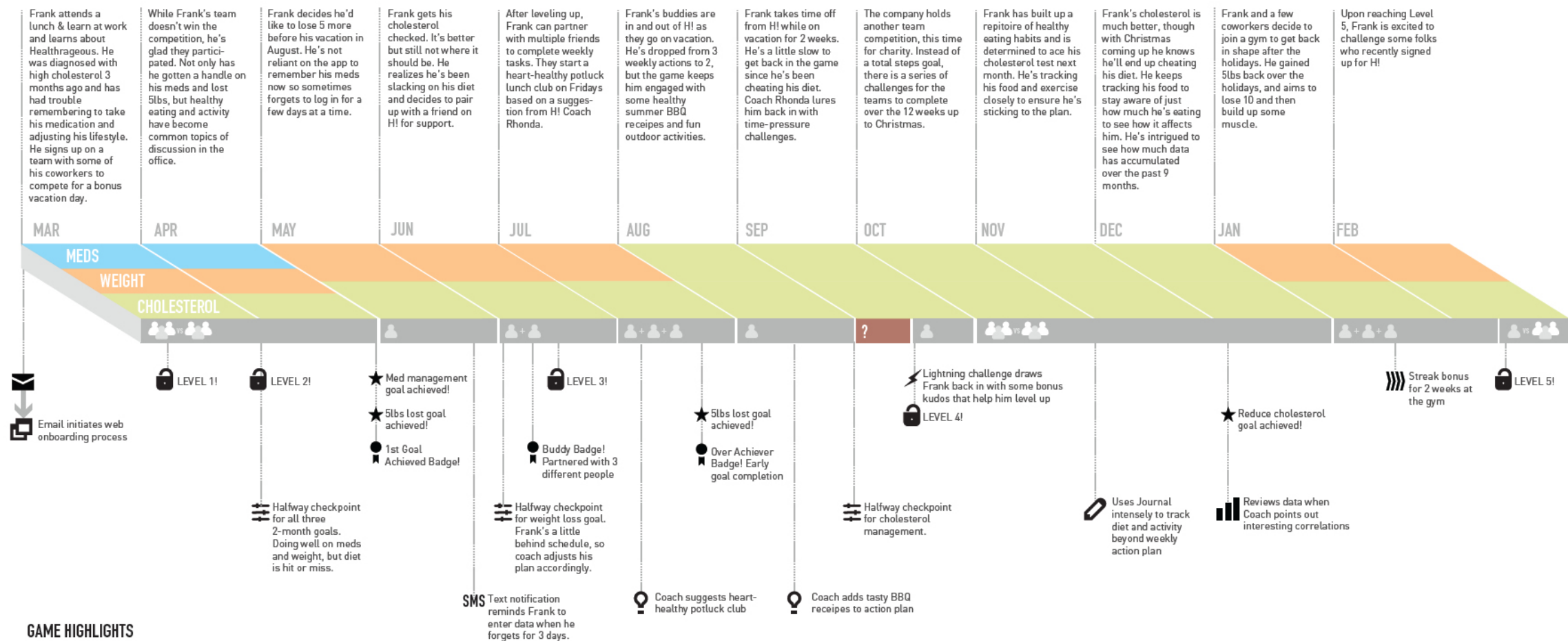
# Purpose-Driven Design

## PLAYER JOURNEY

mad\*power

**FRANK** 43, Call Center Manager, Family Man  
Recently diagnosed with high cholesterol

GADGETS: Pedometer, Wireless Scale in Office, Smartphone  
GOALS: 100% Med Adherence, Lose Weight, Reduce Cholesterol



## GAME HIGHLIGHTS

SCHEDULED NOTIFICATIONS

DAILY Mobile medication reminders & logging

FRIDAY End-of-week checkpoint

SUNDAY Summary of past week

MONTHLY Goal progress & maintenance report

## SAMPLE ACTION PLANS & KUDO SCORES

### WEEK 1 [MAR]

- ✓ Take medication when reminded by HI mobile app
- ✗ Walk 2500 steps per day [for team competition]
- ✓ Buy olive oil to use instead of butter

2 1 per action

### WEEK 8 [APR]

- ✓ Take medication without being reminded by HI mobile app
- ✓ Walk 4500 steps per day [for team competition]
- ✓ Play frisbee with the kids

18 1 per action + x2 completion bonus + x2 competition kudos for 3rd place

### WEEK 18 [JUL]

- ✗ Cook 3 healthy meals this week
- ✓ Go for a 5-mile bike ride
- ✓ Healthy potluck lunch [with Jim, Sally, Mark]

19 1 per action + 8 co-op bonus + 10 goal completion bonus

### WEEK 22 [AUG]

- ✓ Healthy BBQ with family
- ✗ Swim for 5 hours

5 1 per action - 1 sponsor penalty + 5 goal checkpoint evaluation

### WEEK 27 [SEP]

- ✓ Make a healthy fruit dessert [do it tonight for bonus kudos!]
- ✓ Walk 5000 steps per day

14 1 per action + 5 lightning bonus + x2 completion bonus

### WEEK 36 [NOV]

- ✓ Track meals in journal
- ✓ Eat 15 servings of veggies [for team competition]

4 1 per action + 2x completion bonus

### WEEK 47 [FEB]

- ✓ Go to the gym 4x
- ✓ Pack a new lunch food for you and the kids
- ✓ Walk more than a Level 1 group [versus Erik, Yang, Cory]

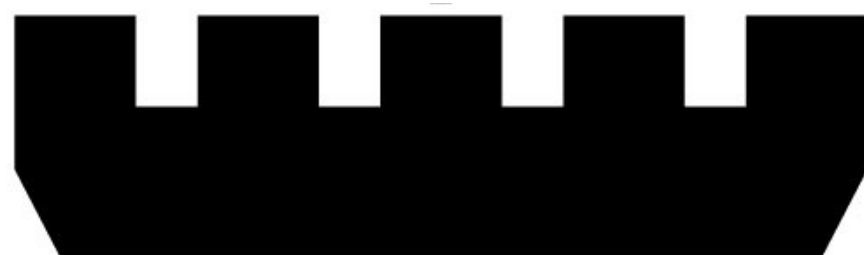
26 1 per action + 8 streak bonus + 4 challenge win + x2 completion bonus



EVERYONE SHOULD  
HAVE GOOD INTERNET  
SECURITY

**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  
CA<sub>s</sub> 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.**

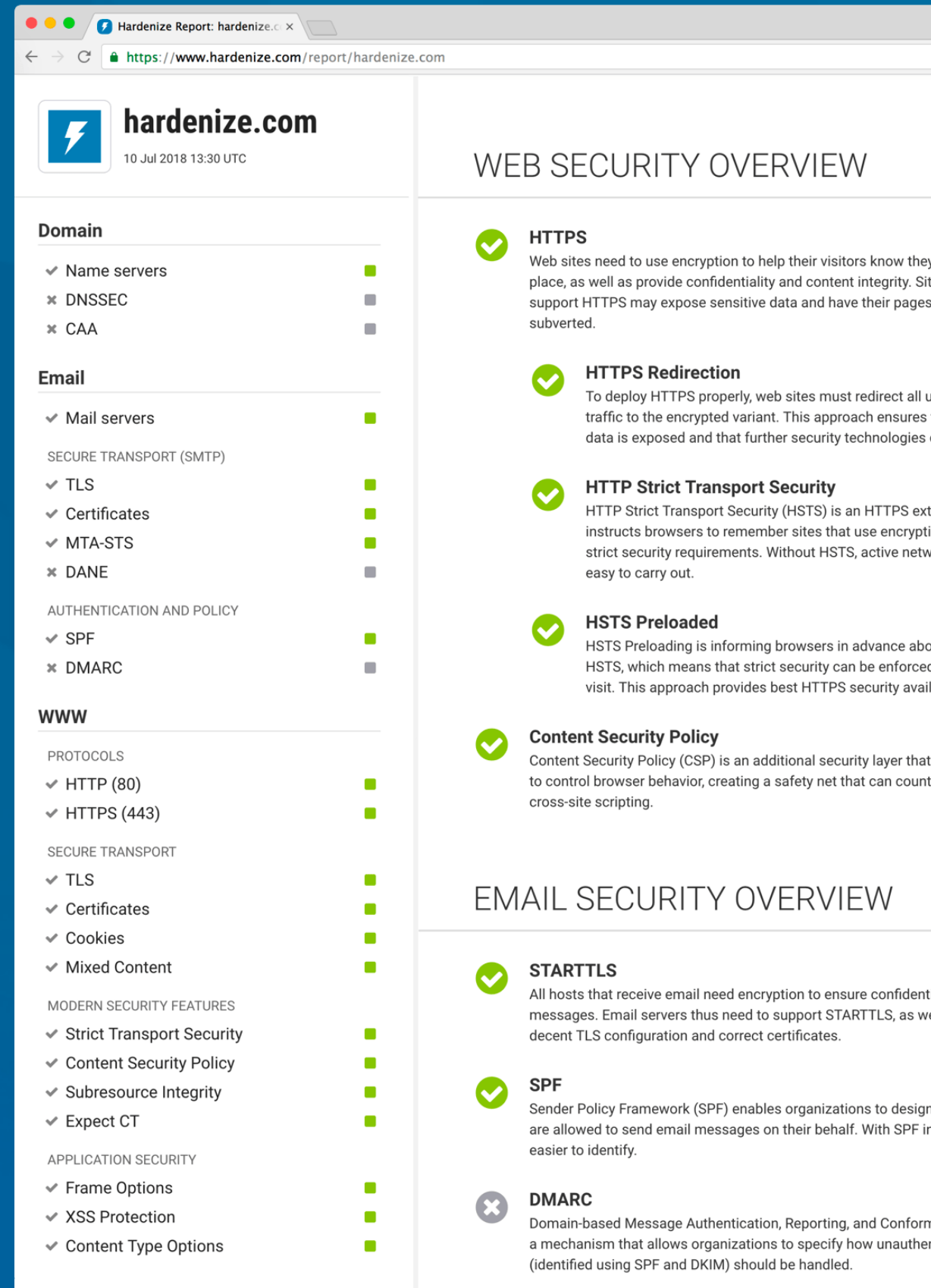
# Meet the new standard for web site network and security configuration monitoring

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](https://www.hardenize.com)

**RUN**



The screenshot shows a web browser displaying the Hardenize Report for the domain **hardenize.com**, dated 10 Jul 2018 13:30 UTC. The report is divided into two main sections: **WEB SECURITY OVERVIEW** and **EMAIL SECURITY OVERVIEW**.

**WEB SECURITY OVERVIEW** includes the following items:

- HTTPS** (Green checkmark): Web sites need to use encryption to help their visitors know they are in a secure place, as well as provide confidentiality and content integrity. Sites that do not support HTTPS may expose sensitive data and have their pages subverted.
- HTTPS Redirection** (Green checkmark): To deploy HTTPS properly, web sites must redirect all unencrypted traffic to the encrypted variant. This approach ensures that sensitive data is not exposed and that further security technologies can be applied.
- HTTP Strict Transport Security** (Green checkmark): HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers to remember sites that use encryption and to enforce strict security requirements. Without HSTS, active network attacks are easy to carry out.
- HSTS Preloaded** (Green checkmark): HSTS Preloading is informing browsers in advance about sites that support HSTS, which means that strict security can be enforced even on first visit. This approach provides best HTTPS security available.
- Content Security Policy** (Green checkmark): Content Security Policy (CSP) is an additional security layer that helps to control browser behavior, creating a safety net that can counteract the effects of cross-site scripting.

**EMAIL SECURITY OVERVIEW** includes the following items:

- STARTTLS** (Green checkmark): All hosts that receive email need encryption to ensure confidentiality of messages. Email servers thus need to support STARTTLS, as well as a decent TLS configuration and correct certificates.
- SPF** (Green checkmark): Sender Policy Framework (SPF) enables organizations to designate which mail servers are allowed to send email messages on their behalf. With SPF in place, it is easier to identify legitimate mail.
- DMARC** (Red X): Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism that allows organizations to specify how unauthorized email (identified using SPF and DKIM) should be handled.

The left sidebar of the report shows a detailed configuration checklist for the domain:

- Domain**
  - ✓ Name servers
  - ✗ DNSSEC
  - ✗ CAA
- Email**
  - ✓ Mail servers
  - SECURE TRANSPORT (SMTP)
    - ✓ TLS
    - ✓ Certificates
    - ✓ MTA-STX
    - ✗ 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



Simple on  
the surface

Easy to  
understand and  
communicate

Wide coverage  
of security and  
configurations  
standards



**feistyduck.com**







19 Oct 2017 18:25 UTC  

 Tweet


## 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) 



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 



# 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

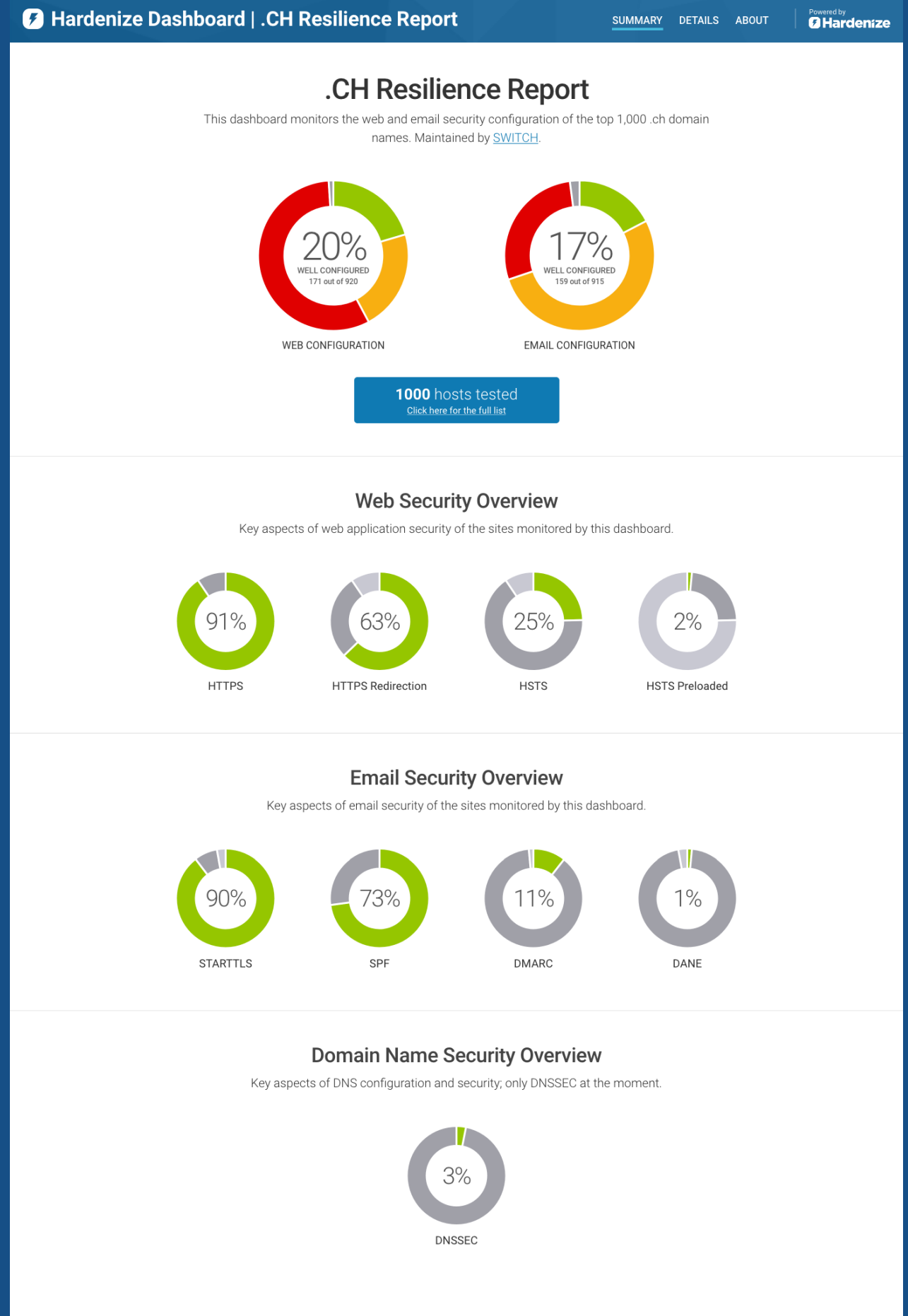
- |   |   |  |
|---|---|--|
| ✓ | Policy is valid                                     | OK. Your HSTS policy uses correct syntax.  |
| ✓ | Long policy age                                     | Your HSTS policy has a long max-age value, which offers better protection.   |
| ⚡ | No subdomains                                       | 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 <a href="https://hstspreload.org">hstspreload.org</a> .  |
| ⚠ | 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,  |





Public  
dashboards

In partnership  
with official  
organisations



# Web site badges



Everyone starts with the default badge



If you have robust HTTPS you get this one instead

Simplified to  
focus on most  
important  
aspects first.



## 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



**Make security**  
**interesting,**  
**easy, and fun.**