Hardenize

Hardenize Discovery and Monitoring Service

LAST UPDATE: JANUARY 2019

Hardenize provides a managed service that combines host and web site discovery, network and security configuration analysis, and certificate monitoring in one package.

Overview

Ten years ago, we didn't have enough security standards to secure our computer systems. Today, we do—but they require a substantial effort to deploy and use correctly. In practice, no one has enough time, expertise, and budget to keep up properly with the constant changes.

We made Hardenize to address these challenges of network visibility and situational awareness, as well as to help organizations of all sizes take advantage of all the security standards that are available. Think about us as a network monitor and flight recorder that keeps track of your infrastructure **to highlight problems and provide coherent friendly guidance about how your security posture could be improved**.

At a high level, our product provides benefits in four key areas: *host discovery*, *network and security configuration analysis*, *certificate inventory, and Certificate Transparency monitoring*.

Host Discovery

On the path to network visibility, often the first challenge is building an inventory of hosts and web sites that need to be monitored. Many organizations—especially the larger ones—struggle to keep track of their properties. We approach this problem with a combination of passive and active techniques.

At the core, we build and maintain a large database of public internet infrastructure. Starting from a list of your key domains, in only minutes we are able to build a complete list of your hosts who have left a footprint on the Internet.

We complement this approach by **importing information from your**

systems (e.g., DNS zone transfers, cloud provider integration, etc.) and with our own **active network scanning.** Our discovery works in the background to find new hosts and add them to your inventory.

Network and Security Configuration Analysis

Understanding all the relevant network and security standards is our core competency. We make it our job to know everything there is about these technologies so that we can pass the necessary knowledge to you. We have a long history of setting new standards and establishing best practices for secure service deployment, especially in the areas of TLS and PKI.

Our **assessments are automated and correlated**, which enables us to deliver meaningful reports and guidance at scale. **We check every network endpoint we discover, recursively.**

One of our key differentiators is that we test comprehensively. For example, when we test your web site, we don't check just the main web server, but extend the test to cover the relevant third-party resources on which you rely.

Continuous Monitoring

Our monitoring is automated and runs continuously, but we don't stop there. **Behind the scenes, we build and continuously update a data model of your infrastructure.** In the future, this will enable us to keep a history of your configuration and answer questions about what changed and when.

Supported Network and Security Standards

Our purpose is to understand all network and security protocols. In our first release our main focus is on having complete coverage of the TLS and PKI fields.

- **TLS:** Detection of all protocol versions, suites, named curves, and key exchange parameters. Simulations of TLS connections by popular clients to anticipate configuration problems. Also, checking for correctly configured forward secrecy and authenticated encryption.
- **PKI:** Discovery of RSA and ECDSA certificates, incorrectly configured certificate chains, trust for major root stores, OCSP stapling, and revocation checking.
- **HSTS:** Comprehensive analysis of *HTTP Strict Transport Security* (HSTS) across hostname variants and parent hostnames and including preloading.
- **CT:** Validation of each network endpoint separately for compliance with *Certificate Transparency* (CT) requirements. Validation of Expect-CT configuration.
- **CAA:** We discover and validate *Certification Authority Authorization* (CAA) configuration.
- **Application security:** We have extensive support for a variety of application security standards—

Content Security Policy (CSP), mixed content detection, *Subresource Integrity* (SRI), and various other security headers. We also inspect cookie security, including new RFCs such as *Same-Site Cookies* and *Cookie Name Prefixes*.

- **Email security:** We check SPF, DMARC, MTA-STS and TLSRPT. We will check ARC as and when it becomes a viable standard. We will also check DKIM in the future.
- **Core network protocols:** Our network infrastructure supports both IPv4 and IPv6. We inspect DNS (including public zone transfer availability) and inspect and validate DNSSEC and DANE when they are present.

Certificate Discovery and Monitoring

A significant part of Hardenize's feature set is focused on certificate discovery and monitoring. In this section, we highlight some of our most useful features.

Certificate Inventory

Public key infrastructure (PKI) is a complex and diverse field. The improvements made to the ecosystem in recent years have further increased the possible sources of problems. As a result, **it's never been more difficult to deploy certificates correctly**.

Using the combination of our database of public certificates and our network assessments, **we build a central database of your certificates**. You can analyze the certificates using our user interfaces or you can export them for local analysis. The certificates can be managed centrally or assigned to different teams. Our certificate inventory works across certification authorities (CAs).

Additionally, **we monitor issuance of new certificates via Certificate Transparency** and provide smart automation to highlight only situations where your attention is required.

Installed Locations

We track not only the certificates, but also the **network locations where they are installed**. This approach lets us to detect a wider set of potential problems and reliably track renewal.

Third-Party Monitoring

We track your certificates, but also **all third-party certificates on which you rely**. In the simplest case, this could mean the certificates on your outsourced email servers. In the more interesting case, we track all certificates that are required for your web site to function correctly, recursively. As a result, **we're able to detect problems that arise outside your own infrastructure, but ultimately affect your properties**.

Renewal Planning and Notifications

The key purpose of our monitoring is to help you renew your certificates in a timely fashion. Using **a combination**

of renewal reports highlighting individual network locations, charts, and notification emails, we create a workflow that helps you streamline all your renewal activities.

We provide a handy certificate calendar integration with other calendaring systems, such as G Suite or Outlook. We also understand managed certificates (when someone else is responsible for the renewal) and don't bother you unless something goes wrong.

Symantec Certificates

In 2017, Google and Mozilla decided to cut short the lifetime of all existing Symantec certificates. Certificates issued before June 2016 expired in March 2018; certificates issued before December 2017 de-facto expired in September 2018. All Symantec brands are affected, which means that there is a large number of installed certificates that have stopped working sooner than expected.

A large number of affected certificates remain in operation. We can easily single them out with our reporting and treat them as expired.

Certificate Transparency Ecosystem Monitoring

Certificate Transparency (CT) is a system that enables logging of all public certificates. Chrome was first to require logging of public certificates, affecting all certificates issued from May 2018 onwards. From October 2018, Apple has similar requirements in place.

We provide **real-time monitoring of all logged certificates worldwide** and match them against your domain namespace to identify those that belong to you.

CT monitoring assists with host discovery, helps enforce policy, and detects unauthorized and fraudulent use. We are able to monitor for variations of your key names and trademark, assisting with detection of phishing web site.

Newly discovered hosts can be automatically added to your Hardenize account for further analysis and monitoring. In fact, this is a critical component of our discovery.

Crucially, **we automate handling of CT discoveries using what we know about your infrastructure.** This allows us to handle most situations without requiring any work on your part. When you hear from us, it will be because there is a genuine problem that needs addressing. For example, **if you deployed CAA, we will highlight certificates that don't match your policies.** Some organizations don't like CAA because it could lead to the blocking of legitimate certificates. We have our own issuance monitoring tools that can perform equivalent or stricter checks, but require no changes to your DNS configuration.