SOLUTION BRIEF

# Reduce the Impact of Migrating to SHA-2

Automatically identify and replace vulnerable SHA-1 certificates

## The Facts

**23,000+**
**Keys and Certificates**
Are in today's average enterprise[1]

**200+ Certificates**
Become unwieldy to track, according to Gartner[2]

**24% Still Use SHA-1**
Out of the world's top 143,0000 websites[3]

**1.5 Million**
**SHA-1 Certificates**
Set to expire beyond January 1, 2017[4]

**$15 Million**
Is the total possible impact per outage[5]

## SHA-1 Migration Challenges

SHA-1 deprecation deadlines are rapidly approaching. Migration to SHA-2 is in full swing. Organizations are moving quickly to avoid exploits using vulnerable SHA-1 certificates, browser security warnings, and outages caused by SHA-2 incompatibilities. Yet, manually migrating certificates is a slow and arduous task.

Many administrators are finding it difficult to manage and validate their SHA-1 migration progress. Often, they are blind to where they are in the transition or if it is complete. This challenge is compounded for internal SHA-1 certificates which are harder to discover, manage, secure, and migrate, because they are spread throughout the enterprise and owned by different organizational units.

As they migrate to SHA-2, administrators struggle to ensure that certificates remain available to secure communications and deploy trusted applications. To avoid outages when systems and applications will no longer trust code signed with SHA-1, developers must test and update all critical enterprise systems. It's not an easy task.

## Impacts on SHA-1 Migration

**Accelerated SHA-1 deprecation:** Google, Microsoft, Mozilla and others are bringing forward their SHA-1 deprecation schedules and issuing security warnings to reduce certificate risk exposure.

**New security standards:** NIST and CAs are replacing SHA-1 with SHA-2. Experts believe SHA-1 is now easy and affordable to exploit,[6] and now browsers will identify SHA-1 certificates as less trusted.

**New compliance rules:** Regulations (e.g., PCI DSS) and security frameworks (e.g., SANS 20 Critical Security Controls) have updated rules on maintaining digital certificates.

**Lack of visibility:** The average enterprise has over 23,000 keys and certificates, but 54% of security professionals admit to being unaware of where all of their keys and certificates are located, who owns them, or how they are used.[1]

To learn more visit www.venafi.com

## STREAMLINE YOUR SHA-1 MIGRATION

Venafi is the only company that can automatically discover all of your SHA-1 certificates and migrate them to SHA-2. You'll effectively remediate the risk of expiring trust for SHA-1 for any CA, reducing cost and risk to your organization. When you choose Venafi, you have access to our tools and expertize to help you migrate from SHA-1 to SHA-2 with speed, accuracy, and reliability—without requiring additional resources.

## ABOUT VENAFI

We are the market-leader in cybersecurity for keys and certificates. We protect them so bad guys can't use them in attacks. We are the Immune System for the Internet™, constantly assessing which keys and certificates are trusted, protecting those that should be trusted, and fixing or blocking those that are not.

[1] Ponemon Institute. *2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point*. 2015.

2 Ouellet, Eric and Wheatman, Vic. Gartner. *X.509 Certificate Management: Avoiding Downtime and Brand Damage.* November 4, 2011. Gartner Document G00226426.

[3] Constantin, Lucian. Computerworld. *Mozilla Mulls Early Cutoff for SHA-1 Digital Certificates.* October 21, 2015.

[4] Venafi. *How to Migrate to SHA-1 Now.* 2016.

[5] Ponemon Institute. *2015 Cost of Failed Trust Report: When Trust Online Breaks, Businesses Lose Customers.* 2015.

[6] Kovacs, Eduard. SecurityWeek. *New Collision Attack Lowers Cost of Breaking SHA1.* October 8, 2015.



Venafi automates, streamlines, and validates your SHA-1 migration. And with automated integration across hundreds of applications, devices, and CAs, you can deliver policy-enforced replacement or remediation of SHA-1 certificates in just minutes.

## Rapid and Complete Remediation

To ensure comprehensive SHA-1 migration, organizations need to be able to quickly identify all known and unknown certificates. They then need the visibility to quickly see which certificates are vulnerable and still need to be migrated to SHA-2. But conducting this process manually becomes cumbersome and prone to human error.

Using security policy templates to create an automated renewal schedule helps organizations proceed quickly and accurately. This level of automation saves time by identifying and replacing vulnerable SHA-1 certificates using established policies and workflows. Throughout the process, audit reports should include all migration details required to meet compliance and governance needs.

## Venafi Trust Protection Platform

With Venafi TrustAuthority™ and Venafi TrustForce™, the Venafi Trust Protection Platform™ enables you to detect all SHA-1 certificates, automate their revocation, issuance, and replacement, and generate reports that validate progress and completion.

### Venafi TrustAuthority

#### Ensures Complete Visibility

- Identifies all SHA-1certificates across networks, cloud instances, CAs, and trust stores
- Maps access to all servers, users, and applications
- Uses a baseline to identify misuse

#### Enforces Policies and Workflows

- Offers policy templates to create a SHA-2 renewal schedule
- Enforces configurable workflows capabilities for replacement, issuance, and renewal
- Provides a policy-enforced, web-based, self-service portal for certificate requests and renewals
- Tracks progress and completion of SHA-1 migration with real-time dashboards and detailed reporting

### Venafi TrustForce

#### Automates Management and Security

- Automates and validates the entire SHA-1 migration process
- Distributes and whitelists new CAs in trust stores
- Replaces certificates in seconds, integrating with dozens of internal and external CAs
- Validates certificates are installed