



Case Study: Fortune 500 Health Care Company

Introduction

This case study of a Fortune 500 health care company is based on an August 2015 survey of Venafi customers by TechValidate, a 3rd-party research service.



“We looked at using Microsoft CLM/FIM, but it didn’t seem to do everything Venafi products offer.”

Challenges

- Managed their keys and certificates using manual tracking and management (e.g., spreadsheet) before Venafi.
- Problems solved using Venafi:
 - Outage Prevention and Remediation
 - PKI Refresh

Use Case

- Venafi products currently being used:
 - TrustAuthority SSL
- Systems integrated with Venafi:
 - Public Certificate Authority
 - Private Certificate Authority
 - Databases

Results

- Improved their internal IT services SLA with Venafi.
- Found additional keys and certificates using Venafi that were previously unknown.
- Key and certificate visibility improved after finding additional keys and certificates using Venafi.
- Vulnerabilities to be addressed with Venafi:
 - Heartbleed
 - SHA-1 to SHA-2 migration
 - The use of secure key length
 - Key and certificate ownership identification
 - Key and certificate lifecycle policies

Company Profile

The company featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Company Size:
Fortune 500

Industry:
Health Care

About Venafi

Venafi is the cybersecurity market leader in protecting cryptographic keys and digital certificates which every business and government depends on to deliver safe encryption, authentication, and authorization.

Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

Learn More:

[Venafi](#)

Source: TechValidate survey of a Fortune 500 Health Care Company

✓ Validated Published: Sep. 27, 2016 TVID: 8BB-D7E-E16

Research by TechValidate