Making the Switch from Venafi

Discover the 3 reasons why users make the switch, and 3 steps we take to get you there.

KEYFACTOR

EBOOK

Contents

KEYFACTOR

The Rise of Machine Identity Management

The explosion of machines, including connected IoT devices, mobile devices, virtual machines, cloud workloads, containers, software-defined applications, and even the code running on all of these, has created an enormous need for machine identity management.

Machine identities are much like human identities: They offer a way to distinguish one unique machine from another in credentials to secure authentication and communication.

Several types of machine identities exist:

- SSL/TLS Server Certificates, which establish trust on public-facing applications and websites.
- SSL/TLS Client Certificates, which authenticate users' identity, web services, or machines to one another.
- Code Signing Certificates, which verify the authenticity and integrity of scripts, executables, and software builds.
- SSH Keys, which provide users (typically system administrators) with secure privileged access to critical systems.
- Cryptographic (Symmetric) Keys, which protect data at rest on endpoints, databases, and cloud workloads.

KEYFACTOR

The growing variety of machine identities and their potential weaknesses make centralized machine identity management critical. As Gartner puts it in their 2020 Hype Cycle for Identity and Access Management: "This is a new profile that reflects an increased need to manage the cryptographic keys, X.509 certificates, and other credentials that are used to establish trust in the identities of machines, such as IoT devices, virtual machines, containers, and RPA bots."

However, if your organization is shifting to the cloud and remote workforce, your current legacy machine identity solution and outdated on-prem PKI aren't built for the task.

KEYFACTOR

It's time for a new approach.

Here are the 3 reasons why our customers switch from Venafi and the three steps it takes to migrate their data onto a modern machine identity platform.

3 Reasons to Switch from Venafi to Keyfactor

See how Venafi Compares to Keyfactor

Discover why enterprises like yours choose Keyfactor over Venafi for cloud-first PKI and machine identity management.

LEARN MORE

KEYFACTOR

#1 Go Cloud, Remove Operation Headaches

Adopt a complete cloud-first machine identity platform.

> *"The SaaS model has us running with 100% uptime and 0% infra-structure footprint at a cost far below what it would take to stand up and maintain internally"*

Gartner peerinsights

PKI Team Lead
Financial Services

One Cloud Platform

Combines certificate lifecycle automation and expert-run PKI into a single cloud platform. No hardware, no complex installation, no headaches.

Flexible Deployment

Cloud-first, not cloud-only. Our customers have the flexibility to deploy on-premise, as-a-service (CLMaaS), or combined with fully-managed PKI (PKIaaS).

Modular Architecture

Our modular, pluggable architecture makes it easier to deploy, upgrade, and scale in hybrid cloud and segmented network environments.

KEYFACTOR

#2 Automate More, Reduce Costs

Achieve faster time to value, without costly add-on fees.

> *I like that the interface to generate and manage certificates is easy to navigate and is almost 100% point and click. ”*

★★★★★ Administrator in Information Technology and Services
Enterprise (>1000 emp.)

Better Visibility

Visibility is priority #1 for our customers. Keyfactor provides complete visibility of certificates from your CAs, to your network, to your end devices. Our AnyCA™ technology delivers faster time to inventory with direct, real-time visibility of every certificate issued from your CAs within minutes.

End to End Automation

Automation isn't nice to have, it's a need to have. Keyfactor customers benefit from our zero-touch Orchestrators that enable certificate lifecycle automation without the need for additional licensing or complex installation.

Every Certificate - One License

Every certificate matters, and you shouldn't have to pick and choose what to manage based on price. We pride ourselves on a clear, predictable pricing model that doesn't nickel and dime you with per-certificate fees.

KEYFACTOR

#3 Scale Without Limits

Upgrade to expert support and better performance.

> *Comparing Keyfactor to Venafi, Keyfactor is more willing to work with us on getting the product to fit our needs, whereas Venafi would just tell us that's the way they do it and to deal with it."*
>
> Senior Security Systems Engineer
> Healthcare Information Technology Leader

Read why a leader in Healthcare Information Technology Replaced Venafi

VIEW CASE STUDY

Top-notch services & support

Keyfactor started as a managed services company. Whether you're on-prem or cloud-hosted, you get access to the same fast response times and elite team of knowledgeable PKI experts.

PKI experts, so you don't have to be

Keyfactor customers benefit from access to industry-leaders in PKI and cryptography. No environment is too complex - go ahead, put us to the test.

Extreme scalability & performance

Speed and scale are the name of the game. Our platform is tested and proven to handle mass revocation and replacement of 500 million+ certificates with a single instance of Keyfactor.

3 Steps to Migrate from Venafi

Connect with one of our Migration Experts

Migrating to Keyfactor will position your organization for more effective and secure machine identity management in the future.

Global 1000 organizations have easily migrated from the Venafi Trust Protection Platform to Keyfactor's PKI as-a-Service and certificate lifecycle automation.

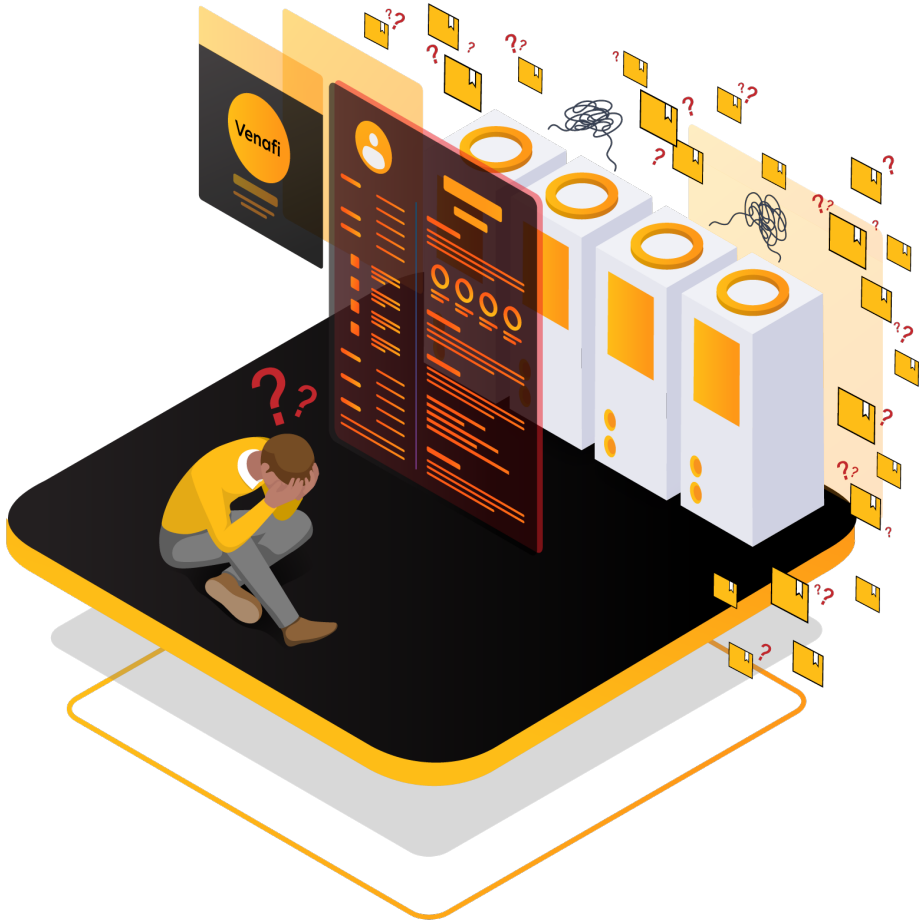
GET STARTED

Step 0: Discovery

Before performing the practical steps, it's important to architect your organization's existing landscape, including which CAs exist on-premise and what the current setup looks like. This architecture should help answer questions like:

- Where do on-premise CAs live?
- What kind of certificates do they issue?
- Are there any self-signed certificates lingering anywhere?

If your organization plans to migrate to a cloud, PKI as-a-Service setup, look at whether it will be more of a "lift and shift" or a true greenfield approach representing a bigger change to the current setup. These are all important conversations to have early on to help identify budgets and other variables before any work begins.



KEYFACTOR

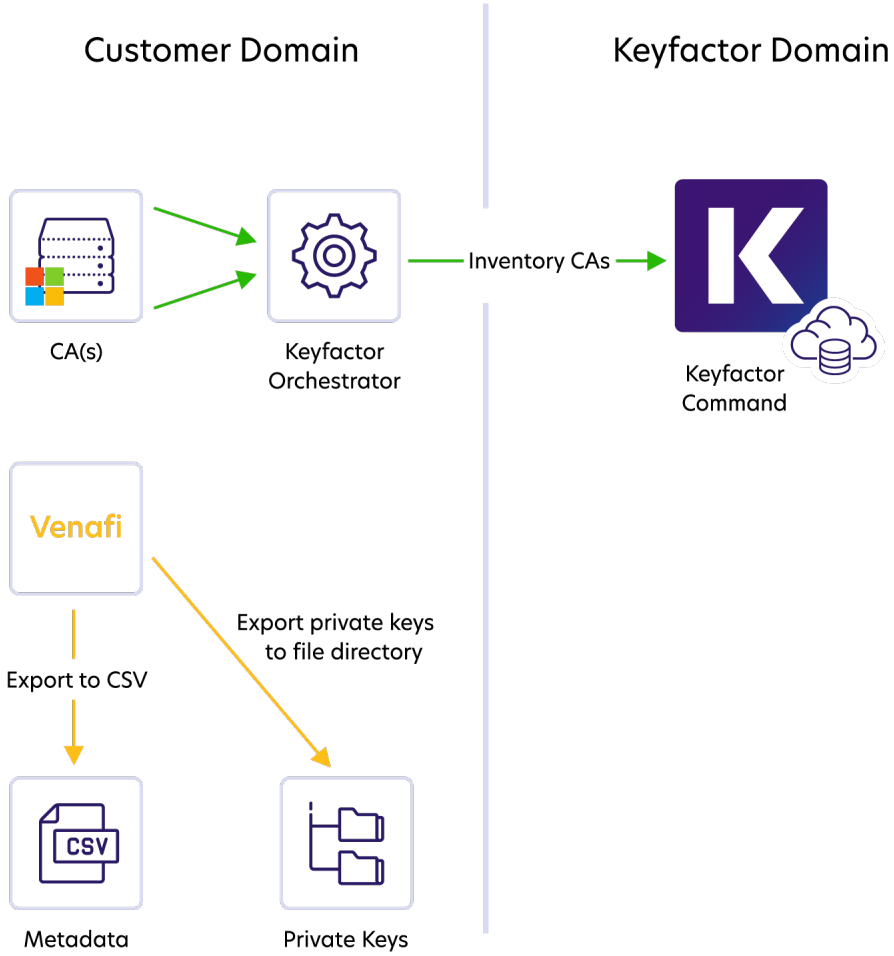
Step 1: CA Sync

Once this discovery is complete, we'll run a CA sync to determine the best way to export all current certificate authority records to the Keyfactor database.

By using low resource orchestrators, we're able to inventory all of the CA's you have on-prem back to one of our cloud-hosted databases. This allows your team to start extracting value right out of the gate by understanding what certs you have and where they live.

This sync gains visibility and auditability over all existing certificates, so you can ultimately manage them alongside any new ones issued from Keyfactor.

Next, we'll export any certificate metadata and private keys out of Venafi.



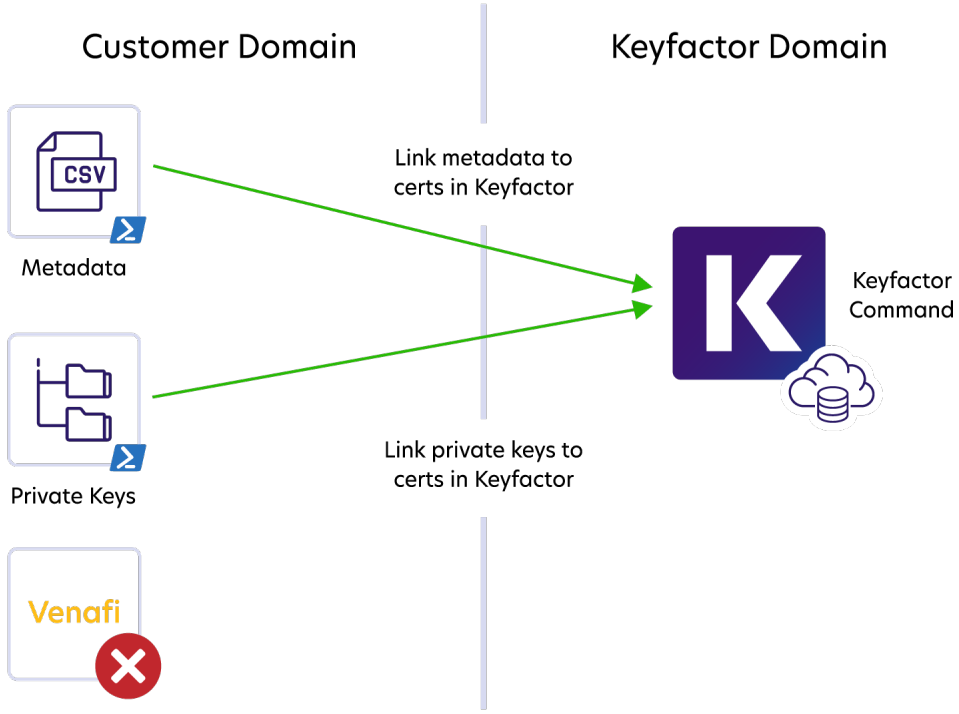
KEYFACTOR

Step 2: Data Import

Once the data is extracted, we can begin to import all the metadata and private key association from Venafi into Keyfactor. This helps you track when certificates will expire, assign business cases to them, and add any other information that's essential to your lifecycle management efforts.

One of the most important considerations when doing this type of migration is your organization's cut off date with Venafi.

Preferably, you want to complete the full migration before that cut off occurs so you have time to live in both systems and transition the management as needed to work out any issues. This overlap provides a safety net to protect against any unforeseen issues or elements your team may have missed during scoping, and it gives your team time to get up to speed on the new solution.



That said, if you don't sunset Venafi right away, you can continue to sync it on a periodic basis over time to ensure information remains consistent. This allows you to effectively manage your entire crypto program until you are ready to sunset your legacy solution.

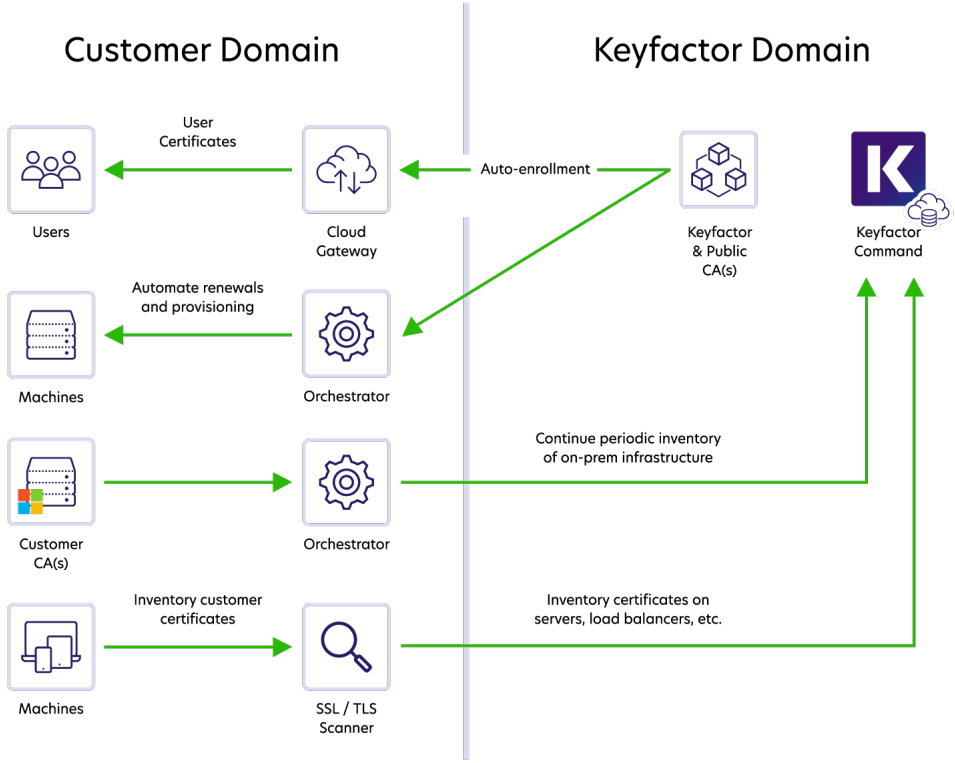
KEYFACTOR

Step 3: Production Ready

Finally, it's time to enhance processes in your new environment.

If your organization moves to the cloud, this will include expanding what you had on-premise with new capabilities, such as:

- Enable auto-enrollment of user and machine certificates via our Cloud Gateway
- Continuously inventory and monitor existing on-premise CAs
- Scan endpoints and servers for unknown SSL/TLS certificates
- Automate renewals and provisioning with Keyfactor orchestrators



When it comes to these types of activities, you'll work hand in hand with Keyfactor to determine the best way to manage your machine identities and facilitate the distribution of certificates to those machines.

KEYFACTOR

Switch from Venafi to Keyfactor Today

Keyfactor has migrated Global 1000 organizations from Venafi and has developed a deep understanding of how all the technical elements must come together to make this possible.

Contact us today to see a demo of the Keyfactor platform, and how we can help you with your migration from Venafi.

REQUEST A DEMO

KEYFACTOR

Keyfactor is the leader in cloud-first PKI as-a-Service and crypto-agility solutions. Our Crypto-Agility Platform empowers security teams to seamlessly orchestrate every key and certificate across the entire enterprise.

We help our customers apply cryptography in the right way from modern, multi-cloud enterprises to complex IoT supply chains. With decades of cybersecurity experience, Keyfactor is trusted by more than 500 enterprises across the globe.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook. Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter and advocate of growing a trusted, secure, diverse and inclusive workplace.

Contact Us

- www.keyfactor.com
- +1.216.785.2990