Venafi Digital Transformation Package

Accelerating digital transformation by bringing DevOps, cloud and InfoSec together

Venafi Digital Transformation Package At a Glance

The Venafi Digital Transformation Package accelerates your DevSecOps digital transformation and future-proofing against rapidly changing DevOps, security and cloud technology stacks.

- Professional services expertise for strategy and implementation
- Out-of-the-box integrations between leading DevOps, cloud and security technologies
- Single-vendor customer support of integrations
- Ready-made blueprints, templates and patterns

Digital transformation creates new challenges for the InfoSec team and can magnify traditional InfoSec challenges. DevOps, cloud deployments, open source technologies and a rapid pace create a dynamic and elastic environment that can be difficult to keep secure.

Benefits

- Reduce security risks that often accompany digital transformation
- Future-proof against rapidly changing tools and workflows
- Provide innovation while building security into digital transformation efforts
- Shorten time-to-value when implementing digital transformation
- Decrease total cost of ownership

The Venafi Digital Transformation Package builds on the value already provided by your investment in Venafi. This package adds additional critical components to help you accelerate your digital transformation while minimizing your risks. We start at the top—our experts deliver strategic guidance to your CISO and InfoSec leadership team as your company journeys through DevOps and cloud transformation. At the same time, we provide blueprints for enterprise architects, tactical assistance and templates for implementers, rapid deployment services, and key integrations from Venafi and trusted third parties. These comprehensive packages come with streamlined, single-source support for everything that is included.

This package of professional services, customer support, processes and technologies accelerate the work of development teams and speed the deployment of applications and services to cloud platforms. It enables trusted machine-to-machine authentication and bulletproof encryption—at the speed and scale of digital transformation initiatives—and ensures the unrelenting increase in the number of machine identities being created 24x7 are secure and protected.

The War Between InfoSec and Digital Transformation

CISOs and InfoSec leaders are caught in a brutal tug-of-war. While digital transformation initiatives drive applications and workloads through rapid DevOps practices and into hard-to-assess cloud platforms, cybersecurity professionals are stuck. They often have no visibility, receive limited security intelligence and have no way to automate some of the foundational security controls they’ve relied on in their traditional on-premises environments. This is especially true for the thousands of TLS certificates needed to assure the confidentiality, integrity and availability of online application and services.
In the most severe cases, these tectonic shifts have left cybersecurity professionals behind the technology curve. They lose influence and lack the solutions needed to guide the business through a newly porous, perimeterless world that they remain responsible for defending.

CISOs and InfoSec leaders have long relied on Venafi to establish, assure and manage the protection of machine identities, from TLS certificates and keys to SSH keys and code signing certificates. At the same time, cloud and application development teams have learned to rely on do-it-yourself methods and native tools to achieve the speed and agility they rely on. For them, wrangling complex encryption keys and TLS certificates has been viewed as less crucial in short-lived environments, as a slow-down to CI/CD pipelines and as a burden that requires developers to reinvent their own PKI for every integration.

The Venafi Digital Transformation Package is designed to enable InfoSec teams, accelerate developers, support dynamic and elastic workloads, and adapt to constantly changing DevOps environments. We start with integrations built by Venafi and trusted ecosystem partners to integrate with the DevOps tools you use today and with native cloud platform integrations. All packages include a built-in service engagement to ensure they're up and running at customer sites and are supported—for product issues or for issues with third-party integrations—by the Venafi Customer Support team.

Challenges

InfoSec and development teams in fast-moving cloud and DevOps environments are often at odds. InfoSec is responsible for securing application software development, but development teams want to avoid security processes that can bog them down. This disconnect results in significant machine identity risks for all teams.

Outages. Unbridled cloud and DevOps projects often use unauthorized certificate sources. One common result is their applications experience certificate-related outages because the keys and certificates they use aren't centrally managed. InfoSec teams need a way to deliver certificate and key management services and policies that are compatible with fast, automated cloud and DevOps workflows.

Speed. Cloud and DevOps teams can't—and shouldn't—be slowed down if they are expected to deliver on the promise of digital transformation. Developers must be able to access machine identities from within their native toolchain environments.

Auditability. Because of the critical security roles they play, machine identities are increasingly subject to policies and regulations that focus on certificate management and security. Without InfoSec visibility into and a means to meaningfully enforce certificate lifecycle policies for machine identities in use in cloud and DevOps environments, organizations risk failing key audits.

The Solution: Venafi Digital Transformation Package

The Venafi Digital Transformation Package extends the Venafi Trust Protection Platform to cloud and DevOps teams, enabling InfoSec to deliver machine identity protection services to the fastest-growing parts of their business. These services are delivered in native toolchains and environments, making it possible for both teams—development and InfoSec—to meet their goals with fast, secure application delivery in any environment.

Accelerates development. The Venafi Digital Transformation Package automates the procurement and installation of cryptographic keys and digital certificates from within their native development toolchains. This allows cloud and DevOps teams to deliver on the promise of fast development without sacrificing machine identity security.

Removes the security burden from developers. Prebuilt integrations with cloud infrastructure and DevOps tools are vetted, validated and supported by Venafi. Cloud and DevOps can focus on critical work instead of searching for and building their own security infrastructure for protecting machine identities.

Provides fast time-to-value. Advisory services, templates and blueprints combine guidance on the Venafi Platform with guidance for third-party resources and developer integrations. These tools and services support the extension of the machine identity protection service to cloud and DevOps teams.
Supplies InfoSec visibility and policy enforcement. By delivering machine identity visibility, InfoSec teams can now define, maintain and enforce policies that align with corporate, regulatory and NIST policies—while being easily consumed by cloud and DevOps teams.

Eliminates certificate-related outages. By automating the procurement, installation and management of machine identities in cloud and DevOps environments, the Venafi Digital Transformation Package ensures enterprise security policies around keys and certificates are met. At the same time, it eliminates the risk of certificate-related outages.

What’s Included With the Venafi Digital Transformation Package

Venafi-Developed Open Source Integrations
Ecosystem-Developed Open Source Integrations
Trust Protection Platform
First-Line Support Through Venafi on All Integrations
Strategic Guidance
• CISO Strategic Blueprint
• Technical Advisory Service
• Templates and Tools

Strategic Guidance
The Professional Services included in the Venafi Digital Transformation Package helps InfoSec teams deliver a machine identity protection service that can be consumed at the speed of business. It combines guidance for the Venafi Platform with guidance for third-party resources and developer integrations to support a machine identity protection service structured specifically for the specialized needs of these teams.

The package defines and delivers a comprehensive set of services spanning discovery, solution project planning, solution design and configuration, and referenced design patterns. It also provides an overall test plan for the use of Venafi within the customer’s environment.

Service deliverables included in the Venafi Digital Transformation Package includes:

• **Advisory Workshop**: To identify and align the issues and requirements of a machine identity protection service from InfoSec, DevOps and cloud perspectives.
• **Blueprints**: To document the vision, architecture, integrations and components for the service being built.
• **Service Test Plan:** To detail how the service will be tested to ensure it meets the objectives outlined in the blueprint.

• **Service Design Patterns:** To deliver the specific guidelines, templates and other materials to deploy the integrated machine identity protection service in your unique environment. Each integration included has its own service design pattern.

**Technology Integrations**

To ensure machine identities are created, issued and utilized appropriately by cloud platforms or CI/CD tools, these technologies must be seamlessly integrated with the Venafi Platform. This ensures they’re managed and protected regardless of the scale, dynamics and elasticity of the workloads created.

Cloud platform integrations include load balancers, container orchestration services and other services, such as Amazon’s CloudFront global content delivery network, AWS Certificate Manager (ACM) and AWS Private Certificate Authority (PCA) and more. Templates for automation tools make it easy to deploy consistent instances of the Venafi Trust Protection Platform across various cloud providers like Amazon, Microsoft and Google without being tied to a single vendor’s solution.

Tools like HashiCorp Terraform, a popular development tool for building, changing and provisioning infrastructure safely and efficiently, and Kubernetes cert-manager, a native Kubernetes certificate management controller, are also included.

For DevOps teams to effectively use Venafi for machine identity protection, the Venafi Digital Transformation Package seamlessly integrates the Venafi Platform with tools they already use in their CI/CD pipeline. Integrations include automation tools like OpenStack and Ansible; secrets storage like HashiCorp Vault; and output visualizations like Apache Kafka.

As DevOps platforms and tools change, so will the integrations available in the Venafi Digital Transformation Package. It will evolve to continually meet machine identity protection challenges in constantly changing cloud and DevOps environments.

**First-Line Support**

The Venafi Customer Support team provides first-line support for the Venafi Platform and all technical integrations within the Venafi Digital Transformation Package, including those developed by ecosystem partners. First-line support means Venafi is right there with you each step of the way—even in the event of an escalation.

**Two Options for your Business Needs**

The Venafi Digital Transformation Package is designed to be deployed across every part of your infrastructure, from multiple hybrid cloud environments to complex DevOps teams, while accommodating and even accelerating the dynamic nature of digital transformation. Whether infrastructures are created and torn down on a weekly basis or short-lived certificates are issued for ephemeral workloads, the Venafi Digital Transformation Package makes sure that every machine identity is protected.

**Venafi Digital Transformation Package: Enterprise**

Our Digital Transformation Package offers one annual subscription rate that covers service, support, strategic guidance and an unlimited number of individual machine identities managed through this solution. Customers don’t need to count certificate issuance or instances. (See license terms and usage guides for more details.)

**Venafi Digital Transformation Package: Professional**

For customers that already have an ELA with Venafi for machine identity licenses, this option offers one annual subscription rate that covers service, support and strategic guidance. (Refer to the terms of your ELA for license terms and usage guides for more details.)
Reduce Time-To-Value

Business-changing initiatives, like application architecture modernization, cloud migration and the shift to DevOps, can put a strain on every part of the business. The rewards are massive, but the challenges are difficult. Security can get sidetracked along the way.

Venafi’s Plus Packages support your digital transformation initiatives, protect machine identities before, during and after your transformation, and reduce the time-to-value of these critical efforts.

The Venafi Platform

The Venafi Platform delivers the machine identity and risk intelligence necessary to automatically safeguard machine-to-machine communications. It secures keys and certificates—SSL/TLS, SSH, IoT and mobile—that serve as machine identities and continuously collects the comprehensive intelligence needed to accurately assess security and availability risks and their remediation.

The Venafi Digital Transformation Package is an extension of the Venafi Platform, accelerating development teams both in the cloud and within application DevOps processes. The package relieves developers of the burden of building or supporting security infrastructure so teams can move faster and scale more easily—all while remaining secure.

The Venafi Platform is a mature solution that:

- Scales up to 1 million certificates with a load-balanced architecture
- Is supported by over 30 machine identity-related patents
- Is Common Criteria certified
- Uses network zone partitioning
- Enables multifactor authentication and single sign-on

As the foundation of all Venafi products and services, it delivers permissions, logs, notifications, integrations and many other capabilities that align Venafi products with security and operations systems.
Next Steps

Are you rapidly moving applications and services to the cloud to better manage costs? Or adopting DevOps practices and tools to accelerate the creation of applications and services? Then the Venafi Digital Transformation Package may be ideal for you. It is available now for existing Venafi customers. Contact your Venafi representative for details.

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

Learn more at venafi.com