VENAFI®

// Speed and Scale: How Machine Identity Protection is Crucial for Digital Transformation and DevOps

Enabling Security Through Automation and Integration

Who should read this: InfoSec and DevOps leaders who need DevOps automated workflows to use proper machine identity protection policies and practices.

// Table of Contents

// How Digital Transformation Presents New Challenges

Digital transformation—driven by cloud computing, modern architecture such as containers, VMs, microservices and DevOps practices—requires new approaches to security, demanding the protection of machine identities that enable authentication and encryption required for secure machine-to-machine communication. Digital communication uses X.509 certificates that serve as identities for all components of the modern application infrastructure stack. However, the rapid consumption of certificates across the heterogeneous groups, networks and systems needed to support DevOps and applications in the cloud presents new and significant challenges.

DevOps practitioners struggle to comply with certificate security policies and mandates coming from Information Security teams because these processes were designed for physical infrastructure, and the processes can take hours or days. While these processes are effective for physical infrastructure, DevOps practitioners focused on delivery times measured in hours or minutes find them unworkable. As a result, they are forced to create their own ad hoc solutions that deliver certificates much more quickly. These unstructured approaches significantly increase the security and operational risks that result from certificates that are improperly issued, configured and managed. However, since these ad hoc solutions are created by DevOps practitioners, security teams rarely have enough visibility to understand the scope of the risk. And, in the rare cases where some visibility exists, security teams do not have solutions that deliver secure, protected certificates to DevOps practitioners in a way that allows them to meet their operational goals.

These problems are becoming more acute because security risks connected with poor machine identity protection are increasing. Sophisticated attackers target the weakest links they can find to penetrate a network and then leverage this initial access to pivot across the network. Because of this new reality, organizations can no longer rely on the combination of web application firewalls and HTTPS, which is often terminated at the load balancer, to protect sensitive communication and data. Encryption is needed for all machine-to-machine communications, including those that occur between microservices, containers and even serverless operations.

Encryption is especially critical for workloads that are handling and transmitting credit card data or other sensitive information. PCI-DSS 6.5.4 requires all applications to encrypt sensitive communications, whether or not these communications occur over open, public networks. The implementation of encryption across all sensitive communications is especially challenging in the new, highly automated and ephemeral DevOps world.

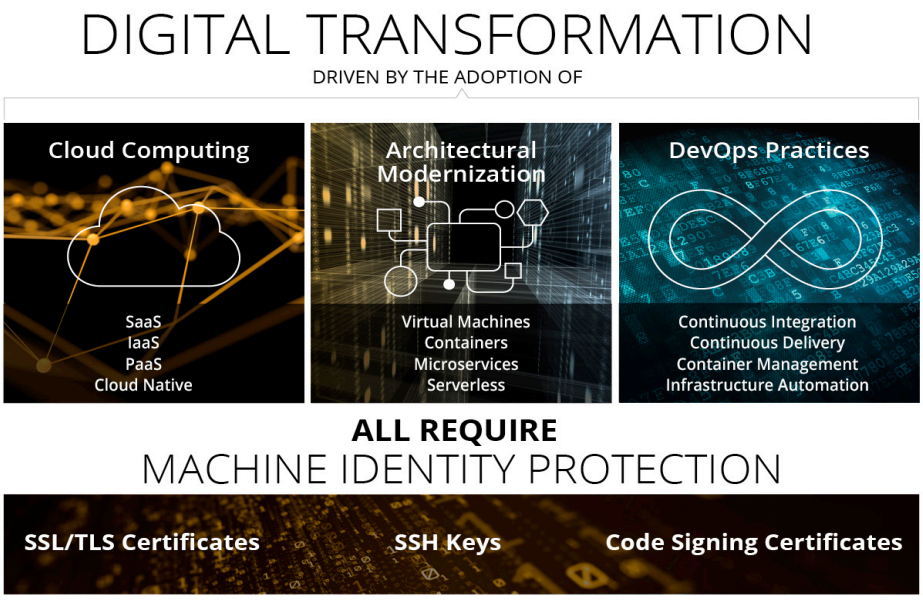
These problems exist because solving machine identity protection challenges within DevOps environments requires a fundamentally new approach. Information Security teams must deliver a frictionless, automated solution that allows DevOps engineers to seamlessly provision and manage certificates throughout the entire software development life cycle—from build to test to production. The goal of this solution should be to eliminate human error and increase the speed of certificate provisioning so that it doesn't hobble the speed of development. The only way to do this is to provide DevOps practitioners with a consumable, API-driven machine identity protection service that integrates seamlessly into existing DevOps toolchains.

By standardizing certificate provisioning across DevOps environments and teams, organizations can:

- Accelerate application development.
- Improve security by automating the issuance of trusted certificates.
- Comply with policies and regulatory frameworks.
- Eliminate certificate-related outages.
- Provide security with visibility into all certificates used across DevOps and cloud environments.

- Adhere to requirements regarding segregation of duties.
- Build infrastructure that allows organizations to easily migrate cloud workloads across vendors.

This paper will discuss real-world machine identity protection challenges facing security and DevOps practitioners as well as best practices that allow organizations to scale digital certificate provisioning. When done correctly, this approach allows organizations to embrace digital transformation and DevOps while also gaining visibility, automation and control of all machine identities across the enterprise.



// A Fundamental Disconnect

Information Security leaders are building programs that protect machine identities throughout their enterprise. This work has taken on a new level of urgency as a result of the volume of new identities required by digital transformation initiatives. As security teams grapple with these challenges, they have come to realize three things:

- DevOps initiatives are incompatible with slow-moving corporate certificate management processes.
- To deliver on the promise of digital transformation, DevOps practitioners can't and shouldn't be slowed down.
- Information Security teams need a way to bake certificate management policies into existing DevOps workflows.

This fundamental disconnect between Information Security teams and DevOps practitioners can be seen in the core pillars of DevOps. Automation, Transparency and Speed are highly prized, sought-after values. While these values aren't necessarily incompatible with security best practices and controls, they can introduce new risks. The larger problem is the rate at which DevOps priorities are completely transforming business expectations for time-to-market and time-to-value; this transformation means that many security practices must fundamentally change to keep up. For many CISOs, this shift is a cause for concern.

The InfoSec Perspective

While digital transformation is an undeniable force, another dramatic shift is occurring today. Recent breaches and outages have highlighted the need for sound machine identity protection strategies to safeguard the certificates responsible for machine-to-machine authentication and encryption. A few recent examples include:

- Equifax 2017: Government reports have shown that a prime factor in scale, severity and length of the Equifax breach comes down to a failure to protect a single machine identity. An expired certificate blinded security tools for months, transforming a manageable incursion into a catastrophe.[1]
- O2 and Ericsson 2018: In December of 2018, more than 30 million mobile customers of the U.K. company O2 lost network access and services. The outage started with failed machine identities used by Ericsson packet switching systems powering the network. Ultimately, this was due to another expired TLS certificate.[2]
- Microsoft and Sennheiser 2018: In November, Microsoft issued a security advisory warning that two applications by Sennheiser had accidentally installed root certificates on users' computers and then leaked the private keys. This could allow hackers to extract private keys from the apps, use them to issue forged certificates, and spoof the identities of legitimate sites and services.[3]

These incidents, and others like them, are regular occurrences for most organizations. Together these challenges are driving the need for stronger guidance on the policies and governance required to protect certificates and digital keys. This is exemplified by NIST's special publication, Securing Web Transactions: TLS Server Certificate Management.[4]

But even with better machine identity protection guidance, CISOs and CIOs know that the compulsory speed driving DevOps practices tends to inspire the use of shortcuts that weaken key and certificate security and create technical debt. In fact, 79% of CIOs expect the speed of DevOps to make it more difficult to know what is trusted and what is not.[5]

The DevOps Perspective

One of the promises of the DevOps revolution is to break down silos between teams to achieve a continuous, end-to-end cycle of innovation and value stream. When it comes to information security, yet another benefit emerges. As the authors say in the DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations, "DevOps may be one of the best ways to better integrate information security into the daily work of everyone in the technology value stream." [6]

Baking security in early has worked well for secure system design, secure coding practices and vulnerability assessment, but it hasn't been adapted for every aspect of information security. This is especially true for machine identity protection. To solve this problem, multiple issues must be addressed in a way that enables machine identity protection for DevOps practitioners but does not slow them down.

// Machine Identity Protection Challenges in DevOps

> **"A security or compliance breach will shock DevOps advocates, forcing greater focus on governance and toolchain oversight."**
>
> Betz, Charles and Rogers, Sandy. Forrester. Predictions 2019: DevOps. Adolescent DevOps Grapples with Governance. November 8, 2018.

DevOps Hampered by Incompatible Security Approaches

Even though DevOps practices are widely adopted, security often remains a siloed function applied outside of the continuous, collaborative work of DevOps practitioners. In most organizations, DevOps practitioners rely on internal PKI or crypto teams to issue certificates. Typically, these external teams don't share the speed and throughput expectations that are intrinsic to DevOps success. This disconnect means that using standard certificate issuance processes impedes timely software delivery. As a result, developers may use certificates in a variety of ways that negatively impact security, including:

- Not using certificates to secure connections and machine-to-machine communication.
- Creating their own certificate authorities (CAs) or using self-signed certificates.

- Using certificates from unauthorized CAs.
- Creating certificates with weak signature algorithms.
- Importing untrusted root CA certificates into certificate stores.
- Failing to adequately protect private keys of root CAs and intermediate CAs.

The Proliferation of Machines Complicates Security

In addition to the challenges connected with getting secure certificates quickly, DevOps practitioners are also using modern infrastructure to architect applications, and each component in the application stack needs to communicate securely. In most organizations, the definition of a machine has evolved from traditional servers in a data center to include:

- Virtual machines.
- Microservices running in containers.
- Serverless architecture.
- Cloud infrastructure-as-a-service.
- Other types of modern infrastructure.

In most DevOps environments, machines are instantiated and destroyed in minutes or seconds. The velocity and the volume of change make it impossible for manual certificate issuance processes to keep pace. DevOps practitioners are often expected to adhere to antiquated certificate provisioning processes that take longer than the life span of some of the machines they're meant to secure.

PKI Policies Can be Difficult to Apply in DevOps

Without a standardized API and CA infrastructure that works across development, test, staging and production environments, developers and operations team members often decide to create and maintain scripts for each environment and use case. This approach is time-consuming and often results in scenarios where individuals who aren't PKI experts are left to select certificate types, key length and key storage, and encryption algorithms. They may even elect to use certificates from unauthorized CAs, which frequently leak into production environments. Without easy access to an approved source for certificates, DevOps practitioners inadvertently put compliance and security at risk, even with the best of intentions.

The Problem with Unauthorized CAs

Unauthorized certificate authorities are CAs that are not organizationally approved for use. Rogue certificates from unauthorized CAs increase security and availability risks and may also impact usability of applications if their roots are not trusted, thereby triggering browser warnings. The use of unauthorized CAs is a strong indication that there are certificates in use that fall outside enterprise security policy.

Hybrid and Multi-Cloud Strategies Increase Heterogeneity

It's a given that hybrid and multi-cloud strategies increase complexity. Although organizations realize they should focus on building a cloud security strategy that can be used across heterogeneous public and private clouds, this doesn't always happen. When DevOps is first adopted, developers often choose to use certificates provided by cloud providers rather than those from a centralized, organizationally-approved source. Although using certificates from cloud providers (e.g., AWS, Microsoft Azure, Google Compute Platform) provides speed and convenience, this creates vendor lock-in. As a result, organizations are unable to seamlessly switch cloud providers. Because the code base is tied to a specific cloud provider, organizations pay the price when they are unable to:

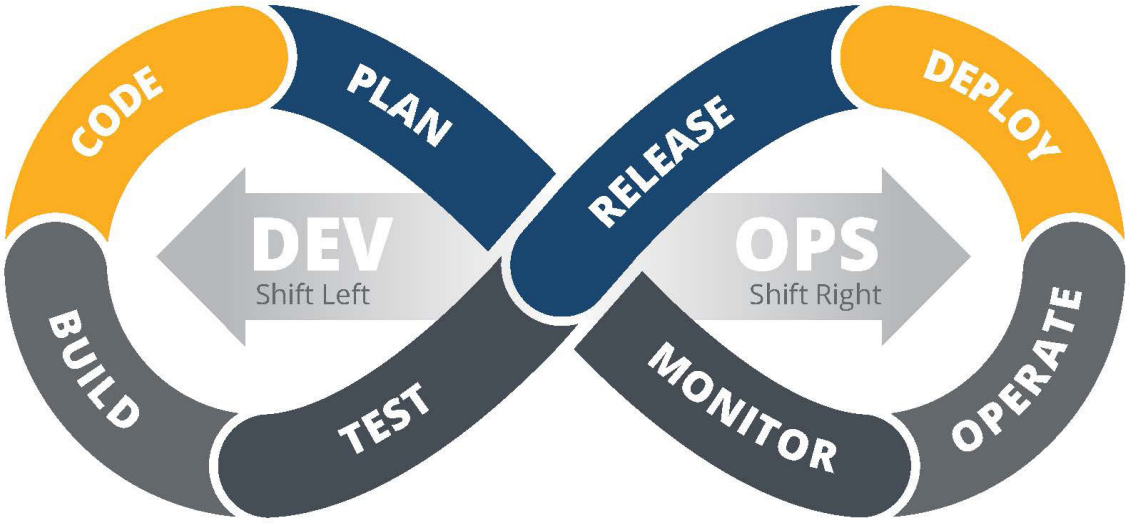
- Reduce costs.
- Respond to compromise.
- Easily rearchitect applications.
- Switch cloud providers.

Lack of Machine Identity Visibility

In large organizations, it's common for individual DevOps initiatives to pop up without centralized oversight, planning and coordination with Information Security. As each team starts up, they select the tools that best serve their needs. The lack of coordination creates a proliferation of key vaults, cloud instances, and individually maintained scripts for the various continuous integration/continuous delivery (CI/CD) pipelines.

Due to the variety of certificate sources, public cloud providers, vault instances and unauthorized CAs, the internal PKI, Information Security and governance teams are unable to respond to machine identity incidents and audit requests. And when they attempt to evaluate or enforce machine identity policies and standards consistently across the enterprise, they don't even know where to start.

Once security executives understand these challenges they begin asking themselves: "How do we align our machine identity protection policies with lean, fast DevOps practices?"



// "Shift Left" and "Shift Right"

DevOps practitioners use a set of DevOps flow concepts called "Shifting" actions. In this model, "Shifting Left" means moving practices to earlier in-development processes so that teams can focus on quality, work on problem prevention instead of detection, and begin testing earlier.

When we apply this model to machine identity protection, shifting left means implementing a standardized certificate service that is integrated into routine DevOps processes and workflows. It could also mean testing machine-to-machine authentication earlier in the development process to ensure the robustness of certificates and keys before they're deployed to production.

"Shifting right," on the other hand, could mean using real-time machine identity protection assessments designed to prevent the kind of certificate errors that caused failures at Equifax, O2 and Microsoft. Instead of a "set it and forget it" approach to creating machine identities, the shift would apply the same rigor to the entire machine identity life cycle that DevOps practitioners have successfully applied to vulnerability assessment, application monitoring and configuration management.

// Analysts Provide Direction

To make these kinds of shifts, better alignment between teams and tighter integration with the DevOps toolchain is required. But how should security and DevOps practitioners begin working together to solve this problem? There is a wealth of guidance available on this topic from industry analysts and experts. Gartner, in two separate reports, gives tips on how to lessen the friction between these teams:

- "Never make developers leave their native toolchain environment. This means integrating your testing with their integrated development environment (IDE) and CI/CD toolchain tools." [7]
- "Adapt existing secure development life cycle tools into the DevOps process by 'shifting them left' into small actionable steps that developers can take quickly, and 'shifting right' to automated tools and responses." [8]
- "Require all application security testing vendors to fully API-enable their solutions for automation and, ideally, provide explicit support for integration with common continuous integration/continuous development (CI/CD) tools." [8]

Analyst group Forrester seconds this notion by stating Information Security teams need to "leverage automation lessons from DevOps… As infrastructure becomes increasingly software-defined and administrators evolve into becoming developers, they can leverage some of the same tools and processes that drive development and operations (DevOps) efficiency." [9]

These are all great ideas, but how do organizations translate them into specific action that will improve machine identity protection?

// Best Practice Approaches for X.509 Certificates

> **"There should be absolutely no way that the Dev and QA environments don't match the production environment."**
>
> Kim, Gene; Behr, Kevin and Spafford, George. The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win. 5th Edition. February 27, 2018.

Standardize Machine Identity Processes

The first step in building an automated solution for machine identity protection requires standardizing machine identity processes. To deliver on the concept of Rugged DevOps—a term coined by Josh Corman and James Wickett—DevOps workflows need to be designed to accommodate the need for machine identities. By treating the provisioning of certificates as an essential step in configuration of modern infrastructure, organizations can easily encrypt machine-to-machine communications across all types of infrastructure.

Well-known DevOps shops such as Airbnb are building centralized services that standardize and abstract machine identity details away from developers. Not surprisingly, this approach is supported in the new guidance from NIST[4] which recommends establishing a certificate service. According to NIST, a certificate service "includes technology-based solutions that provide automation and that support certificate owners in effectively managing their certificates."

With a certificate service, enterprises can start to standardize and control certificates in use across the enterprise and improve operational efficiency, maintain compliance, and accelerate secure software delivery. To learn more about why organizations should care about the new NIST guidelines, watch this three-minute video by Paul Turner, a well-known cybersecurity, machine identity and compliance expert.

> **The central Certificate Service should support easy integration with and access from DevOps frameworks and other programming tools.**
>
> Souppaya, Murugiah; Haag, William; Turner, Paul and Barker, William C. National Institute of Standards and Technology. SP 1800-16B (Draft), Securing Web Transactions TLS Server Management. Published November 2018 and out for comment through February 18, 2019.

Centralize Certificate Provisioning for Visibility and Compliance

One key benefit of standardizing the certificate issuance process in a way that serves the needs of Information Security, Operations and Development is that issuance can be centrally controlled and managed. Once centralized certificate provisioning is in place, organizations can:

- Simplify provisioning of secure, compliant certificates.
- Integrate certificate issuance into DevOps toolchains to secure infrastructure as it is spun up.
- Abstract away the details to enable DevOps practitioners to move faster, while security keeps control over what type of certificates are issued and where they are located.
- Consistently enforce machine identity policies within DevOps environments.
- Report on certificate usage for compliance and audits.
- Eliminate certificate-related outages by monitoring and automatically renewing certificates before they expire.
- Reduce the mean time to restore (MTTR) for crypto-events like CA compromise.
- Switch CAs or cloud providers with no application code changes.

Use Automation to Cut Certificate Provisioning Time

An automated certificate service integrated with existing DevOps tools—such as Kubernetes, Docker, Chef, HashiCorp Terraform and Vault—gives DevOps practitioners programmatic, automated certificate issuance and provisioning within their existing tools. An additional benefit of working with an automated certificate service is that DevOps practitioners use the same service that provides certificates for the rest of the enterprise, so they automatically get certificates

that comply with corporate policies and standards. In this way, they leverage best practices from traditional PKI and production teams but receive certificates at the speed and scale of DevOps workflows.

The benefits of using automation to cut certificate provisioning time can be profound. For one large retailer, automation was able to cut certificate provisioning time from five days to just minutes. This kind of automation removes the incentive for DevOps practitioners to come up with creative ways to circumvent certificate issuance processes without impacting DevOps timelines or workflows.

In summary, centralized automated certificate processes offer the following benefits:

- Saves time for DevOps practitioners by standardizing their code.
- Provisions certificates as part of the software delivery life cycle.
- Secures infrastructure as it is spun up.

// Automating Machine Identity Protection for DevOps

Analyst group Forrester issued a stark warning for organizations relying on DevOps projects: "DevOps Practitioners Should Bet On A Breach: In their need to create speed, those DevOps practitioners that haven't shored up their end-to-end continuous delivery toolchains with mature solutions and policies will face attacks on their automated digital pipelines." [10]

Venafi has been solving machine identity protection challenges for the largest, most security-conscious companies in the world. Our solutions allow Information Security and DevOps practitioners to establish, assure and manage the protection of all of machine identities across the extended enterprise, including those used in DevOps projects. With Venafi's automated solutions, security and PKI teams don't need to worry about the configuration of TLS certificates or outages caused by certificate expirations. You can be confident that encryption levels conform to corporate policies and industry regulations so that sensitive data is always protected, even in fast-moving DevOps environments.

Venafi allows every organization to leverage the robust capability used by internal PKI teams for DevOps practitioners without interrupting their work or adding friction to DevOps processes. The results of this approach can be profound. When provisioning keys and certificates becomes part of the automated build process, DevOps practitioners can significantly reduce IT service delivery time. In a third-party survey, over half (57%) of Venafi customers used the Venafi Platform to improve their SLAs for internal IT services—and over one-third (34%) were able to change their SLAs from days to just hours.

To help security and DevOps practitioners work together to improve machine identity protection, the Venafi Platform delivers machine identity protection solutions that are accessible through comprehensive APIs and include deep integrations with existing DevOps toolchains, including Kubernetes, HashiCorp Terraform and Vault, Docker, UrbanCode, and Chef.

While these integrations address most DevOps requirements today, Venafi knows that the DevOps world is in a constant state of change. Venafi is committed to an aggressive, ongoing effort to protect organizations' business-critical applications and has launched a $12.5 million Machine Identity Protection Development Fund to sponsor the development of new integrations, accelerating the expansion of the Venafi's already robust integration ecosystem.

Every security team understands that instantiating modern infrastructure must go hand-in-hand with securing it. Venafi empowers your developers and your security team, making it simple for them to comply with corporate policies without delaying development so that your organization can excel at agility and security.

Table 1
Needs, Issues and Solutions for Digital Transformation and DevOps

Issues	Venafi Solution
Speed up certificate provisioning Establish a certificate service within the DevOps toolchain or via API.	• Centralized certificate policy enforcement, access control, workflow processes and audit logging. • Extensive DevOps ecosystem through native integrations with over one thousand applications and common APIs.
Compliance with policies and standards (PCI-DSS, NIST, GDPR, FedRAMP, etc.) • Integrate tools to enforce and monitor compliance. • Visibility and intelligence of certificates in use.	• Integration with popular DevOps tools and platforms—including Kubernetes, HashiCorp Terraform and Vault, Ansible, UrbanCode, and Chef—automating certificate requests, installations, renewals and revocations. • Tracking of certificates and how they are being used including affiliated metadata. • Orchestration of certificate rights and policies with customizable workflows to seamlessly ensure automation and maximize security.
Prevent certificate-related outages • Orchestrate the complete life cycle of certificates. • Provision certificates when infrastructure is instantiated.	• Full certificate and key life cycle as virtual systems and containers are commissioned and decommissioned. • Certificate provisioning, renewal and revocation, per policy.
Crypto- and cloud-agility • Centrally control certificate issuance. • Abstract certificate issuance away from developers.	• Standardized service abstracts issuer-specific requirements across all publicly trusted CAs and internal CAs. • Central control for setting policies governing certificate issuance. • REST API, WebSDK and DevOps toolchain integrations for standardizing code across all environments, cloud providers and CAs.

To learn more about Venafi's DevOps solutions, please visit **https://www.venafi.com/devops-solutions**. For details on our integrations, visit **https://marketplace.venafi.com**.

// References

1. United States Government Accountability Office. Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. August 30, 2018. Document ID:GAO-18-559.
2. Reichert, Corinne. ZDNet. Ericsson: Expired Certificate Caused O2 and SoftBank Outages. December 6, 2018.
3. Cimpanu, Catalin. ZDNet. Microsoft Warns about Two Apps that Installed Root Certificates then Leaked the Private Keys. November 28, 2018.
4. Souppaya, Murugiah; Haag, William; Turner, Paul and Barker, William C. National Institute of Standards and Technology. SP 1800-16B (Draft), Securing Web Transactions TLS Server Management. Published November 2018 and out for comment through February 18, 2019.
5. Venafi. 2016 CIO Study Results: The Threat to Our Cybersecurity Foundation. 2016.
6. Kim, Gene; Humble, Jez; Debois, Patrick; Willis, John and Allspaw, John. The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations. October 6, 2016.
7. MacDonald, Neil and Head, Ian. Gartner. 10 Things to Get Right for Successful DevSecOps. October 3, 2017. Document ID:G00341371.
8. Horvath, Mark; MacDonald, Neil and Tirosh, Ayal. Gartner. Integrating Security Into the DevSecOps Toolchain. November 16, 2017. Document ID:G00334264.
9. Gardner, Chris; Blankenship, Joseph and Cunningham, Chase. Forrester. Reduce Risk And Improve Security Through Infrastructure Automation The Bad Guys Use Automation — Fight Fire With Fire. June 22, 2018.
10. Betz, Charles and Rogers, Sandy. Forrester. Predictions 2019: DevOps. Adolescent DevOps Grapples with Governance. November 8, 2018.

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
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.

To learn more, visit www.venafi.com