VENAFI®

BUYER'S GUIDE

// Buyer's Guide for Machine Identity Management

How to choose the best platform to maximize flexibility, security and control

Organizations like yours are grappling with a tsunami of new keys and certificates necessary to support digital transformation. These critical security assets are used to identify and authorize machine-to-machine connections and communication, making them high value targets for cyber attackers and malicious insiders.

As the volume and variety of machine identities counts within the average organization continues to rise, it's not unusual for organizations to have tens or even hundreds of thousands of identities. This rapid growth makes it exponentially harder to gain enterprisewide control of your machine identities, including SSH keys and code signing certificates. You can't solve this challenge with point solutions that only address one part of the problem—you'll only increase your risk of outage, breach, development delays and more. You need a comprehensive, enterprisewide platform that delivers these four outcomes:

- Automate for Efficiency
- Prevent Misuse and Compromise
- Stop Outages
- Modernize with Speed and Agility

To realize these critical outcomes, your platform should deliver security, availability, and reliability and be designed for cloud first and cloud native environments. We've compiled a security checklist to help you select the most effective key and certificate orchestration solution for your organization.

Automate for Efficiency

Is it easy for certificate and key owners to request and deploy machine identities?
It can be challenging to effectively manage the rapid changes in key and certificate population without automating the entire lifecycle of these identities—especially when you support numerous machine identity types and owners.

RECOMMENDATION: Self-service portal
Providing self-service for certificate management will allow users to view dashboards for certificate status, view certificate inventory, receive email notifications for upcoming expirations and customized automation by group or by project.

Are you manually managing the lifecycle of your machine identities?
Using manual processes to deploy, install, rotate, and replace machine identities is inherently error-prone and resource intensive—making it impossible to track the progress of complex, multi-step processes across multiple systems.

RECOMMENDATION: Customize workflows
Automating the entire lifecycle of machine identities delivers significant resource and cost savings. You will need to adjust automation processes for specific teams, projects or groups. Make sure your solution allows you to customize the automation process and workflows to meet a variety of requirements.

How quickly can you remediate machine identity problems?
If a large-scale security event occurs, automation is the only way you can quickly make bulk changes to all affected certificates, private keys, and CA certificate chains. You may also need to remediate more focused security events, such as replacing a compromised certificate that's used across multiple machines.

RECOMMENDATION: Automate remediation
Automation is the only way to deliver the agility you need to rapidly respond to critical security events such as a CA compromise or zero-day vulnerability in a cryptographic algorithm or library.

Do all your machine identities comply with corporate security policies?
When you leave compliance in the hands of the various administrators who manage keys and certificates for the systems they control, the policy enforcement results will be inconsistent. You may also be challenged to automate enforcement of security policies across various business units and certificate management solutions.

RECOMMENDATION: Automate policy enforcement
Automating certificate requests ensures that all machine identities comply with preset policies and regulatory requirements—globally, by logical group, or by individual identity. You can quickly and automatically revoke and replace any machine identities that don't conform to appropriate policies.

Prevent Misuse and Compromise

Can you identify and react quickly to an outage or breach?
If you don’t have enterprisewide awareness of your key and certificate security posture, you will be unable to respond quickly to a misused certificate, an unplanned outage or a vulnerability to minimize the potential damage to your organization.

RECOMMENDATION: Real-time monitoring
Before you can effectively react to a security event or outage, you need a complete inventory of your certificates. Look for a solution that allows you to monitor your entire population of machine identities for any behavior that would indicate compromise or misuse.

Can you respond quickly to a CA compromise?
If you rely on a single CA to issue and manage your certificates, you’ll need to react quickly if that CA is compromised or distrusted. Unfortunately, this is not an infrequent event. And when it happens, it leaves many CA customers scrambling to find another CA and to convert all their keys and certificates.

RECOMMENDATION: Bulk remediation
Choose a solution that allows you to locate and prioritize all certificates that need to be revoked and replaced. The solution should also be able to automate the remediation process in bulk to accelerate the process and keep your business safe and productive.

Can you deliver real-time access to keys and certificates for SSL inspection?
Real-time SSL/TLS inspection can allow encrypted traffic to be decrypted, inspected and re-encrypted to detect threats without delaying communications. But this only works if your organization can share real-time access to keys within multiple applications.

RECOMMENDATION: Orchestration of keys
Choose an orchestration solution that has access to application keys. Look for a solution that centralizes key generation, management and storage as this is the only way to facilitate distribution to multiple endpoint applications.

Can you maintain consistent security across all keys and certificates?
Most certificate users generally don’t understand how to provision strong keys and certificates. They often revert to older, more familiar issuance practices, which may be based on less secure configurations or unapproved CAs.

RECOMMENDATION: A single pane of glass
Choose a solution that will give you ultimate flexibility in actively managing all your certificates from a single console. You’ll be equipped to implement consistent security policies across all CAs and deliver audit-ready reports.

```
            $tmp_studio_list = array();
            $shots_result = mysql::query("SELECT DISTINCT(studio) as studio, COUNT(*) as count FROM image WHERE day_id = '$day->id' AND enabled='y' GROUP BY studio");
            while( $studio_list = mysql::fetch($shots_result)) {
                $day_info = metadate::day_info($day->shot_date, $studio_list->studio,"quick");
                $tmp_studio_list[] = array("studio" => $studio_list->studio, "count" => $studio_list->count, "title" => $day_info->title);
            }
            $day->studio_list = $tmp_studio_list;
            $return[$day->shot_date] = $day;
        }

        return $return;
    }

    static function day_images_list($date, $studio) {
        global $global_studio_list;
        if(!in_array($studio, $global_studio_list)) die("error studio");
        $date = mysql::escape($date);
        if(mysql::count("image_date","shot_date = '$date'") != 1) die('date not found');
        $studio = intval($studio);
```

Stop Outages

Do you have real-time visibility into all machine identities?
With limited visibility and tracking, certificates can unexpectedly expire, triggering critical service outages. If you don't have the data you need to manage the entire certificate life cycle and proactively identify impending expiration dates, you can't create dependable, proactive certificate renewal processes.

RECOMMENDATION: In-depth Discovery
Look for a solution that helps you discover TLS certificates wherever they are across broad global infrastructures and notifies certificate owners and other stakeholders when escalation actions are needed.

Do you know who owns each and every certificate in your organization?
A lack of visibility can make it nearly impossible for you to track certificate ownership to prevent outages. Or, if an administrator who controls a machine identity resigns, is terminated, or is reassigned, certificate ownership is in limbo. When one of these certificates expires, you won't have enough information about the certificate to respond quickly.

RECOMMENDATION: Comprehensive inventory
With a solution that lets you locate and track certificate ownership, you'll know where to assign appropriate actions. So when there is a problem with a certificate—such as a pending expiration—you'll immediately know who is responsible for fixing it and you can track progress accordingly.

Does human error impact your compliance with security policies?
When you leave compliance in the hands of the various administrators who are responsible for the keys and certificates on the systems they control, policy enforcement will be inconsistent. And any lapse in policy compliance can leave a certificate vulnerable for an outage.

RECOMMENDATION: Policy-driven automation
Look for a solution that will help you minimize human error through automation. For the best results, automated policy enforcement should drive every aspect of your machine identity lifecycle.

Are you still trying to manually manage certificate workflows?
To avoid outages, it's important that you automate the entire machine identity life cycle. If you try to manage certificates manually, you will increase the risk of experiencing certificate-related outages and security breaches.

RECOMMENDATION: Customizable workflows
Automating the life cycle allows you to avoid error-prone, resource-intensive manual actions that can leave the door open to certificate outages, while improving operations and security.

Are you waiting too long to find out about a certificate issue?

To maximize availability, it's critical that you find and evaluate potential machine identity issues before they become business interruptions or exposures. Without alerts and notifications based on policy, you won't be informed of unauthorized changes or impending actions in time to prevent negative impact.

RECOMMENDATION: Automated alerts

Automated alerts allow you to be proactive, taking immediate action before outages happen or attackers take advantage of weak or unprotected machine identities.

Ability to integrate or support all key IT technologies

TLS certificates are used by nearly all the technology solutions that are deployed across your expanded network and security infrastructure. Each of these systems will go down if the certificates they are using expire.

RECOMMENDATION: Automated orchestration

You can improve the effectiveness of your network and security systems by integrating machine identity management and security, giving these crucial technologies easy access to up-to-date keys and certificates and machine identity intelligence.

Modernize with Speed and Agility

Do you have the agility to support modern development tools and methodologies?

Not all certificate management solutions are flexible enough to support the speed and agility requirements of application teams using containers and service mesh infrastructure. Plus, many of these solutions are not tightly integrated into DevOps and CI/DC pipeline tooling.

RECOMMENDATION: DevOps toolset integrations

Look for a certificate management solution that integrates with popular development tools, like Kubernetes, Jenkins, Istio and Ansible. You'll get centralized management, policy enforcement, and visibility of DevOps machine identities.

Are your developers tempted to prioritize speed over security?

Motivated by compressed timelines, application development teams often rely on ad hoc provisioning. Plus, they may resort to reusing keys and certificates, skip using them all together, or simply generate their own keys and certificates in a way that may violate policies and introduce unnecessary security risks.

RECOMMENDATION: Simplify provisioning

Choose a solution that speeds up the delivery of products and services within the self-contained runtime environments that developers prefer. Each of these microservices and containers should have a unique certificate to identify and authenticate it and to support encryption.

Does your organization have cloud first or cloud native teams or projects?
Cloud first and cloud native teams require the rapid creation and provisioning of machine identities to ensure secure computing and application deployment. You need to be able to automate the delivery and monitoring of machine identities in development environments to increase security while supporting the rapid deployment of new servers, applications, and containers.

RECOMMENDATION:
Look for an open-source solution like cert-manager that enables developers to easily request machine identities to secure applications. Certificates can be signed by public and private certificate authorities such as Let's Encrypt, and cert-manager handles the automation of the certificate lifecycle.

Can you easily find DevOps certificates wherever they exist
Ideally, your inventory should include machine identities both within development and production environments. This is especially important for code signing certificates, where you need to maintain strict controls to avoid threats such as those experienced by SolarWinds.

RECOMMENDATION:
Choose a solution that gives you a comprehensive, up-to-date view of all your machine identities, including those on virtual, cloud, mobile, and IoT infrastructures.

Choose the Best Management Solution for Your Machine Identities

Every organization is different, but many are struggling to manage the rapid growth of keys and certificates that you need to support mission-critical digital transformation across legacy infrastructure as well as cloud and DevOps initiatives. The good news is that the most demanding and security-oriented companies have already solved many of these problems using a flexible platform that delivers comprehensive visibility, intelligence and automation customized for your unique requirements. Choosing the right solution will help you avoid common machine identity management challenges like inefficient processes, expired certificate outages, misused or compromised certificates and slowing the pace of continuous development. And really, there's only one choice to accomplish all of that.

About Venafi

Venafi is the cybersecurity market leader in machine identity management, 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 venafi.com