EXECUTIVE BRIEF

// Ten Questions to Ask Your PKI Team About Machine Identities

Are you protecting machine identities as diligently as human identities?

Is your organization too focused on protecting usernames and passwords while leaving the keys and certificates that serve as machine identities vulnerable? If your PKI team isn't enforcing security policies, you could be exposing machine identities to exploit or expiry.

Another question: Do you know how much machine identity risk you have? Compare your identity and access management controls for humans to those you use for machines, and odds are you'll reveal many significant security gaps.

Because machine identities safeguard machine-to-machine communication, protecting them is critical to your overall security. But cybercriminals know the value of using trusted machine identities in attacks. Without adequate machine identity management, attackers can misuse machine identities in a variety of undetectable cyberattacks. Weak machine identity management can also cause outages, which are triggered by expired certificates and affect network reliability.

Here are 10 questions security executives should ask their PKI teams to better understand their machine identity risk:

1. Do we have visibility into all of our machine identities and know where they are installed?

Your company maintains a complete inventory of all usernames and passwords to prevent unauthorized access. But do you know where all of your machine identities are installed, who owns them, and how they are being used? A complete inventory of all keys and certificates will equip your PKI team to detect unauthorized access, certificate misuse or upcoming expiry dates. Ready access to certificate intelligence will also help them react quickly when a security or availability issue is found.

2. How strong are the keys and certificates used by our machine identities?

Just like weak passwords, weak key strength, cryptographic algorithms, hash algorithms and cipher strength are primary targets for attackers. These weaknesses undermine the strength of your encryption and can facilitate compromises. Your PKI team should only use strong cryptographic keys and algorithms.

3. Do we have central control of all machine identities across environments?

One weak password can be the door through which attackers breach your defenses. In the same way, siloed machine identity policies can lead to inconsistent enforcement of privileged access, which can also allow attackers to exploit your organization's weaknesses. It's critically important that your PKI teams centralize the management of consistent security policies for machine identities.

4. What measures do we use to keep machine identities secret?

If users are careless with their passwords, they can be compromised more easily. Private keys must be kept secure because if attackers gain unauthorized access, they can impersonate a trusted corporate system. To avoid this type of compromise, you should use automated processes that remove the need for manual access. And when possible, keys should also be stored in hardware security modules (HSMs) to prevent compromise by an attacker.

5. How often do we rotate machine identities?

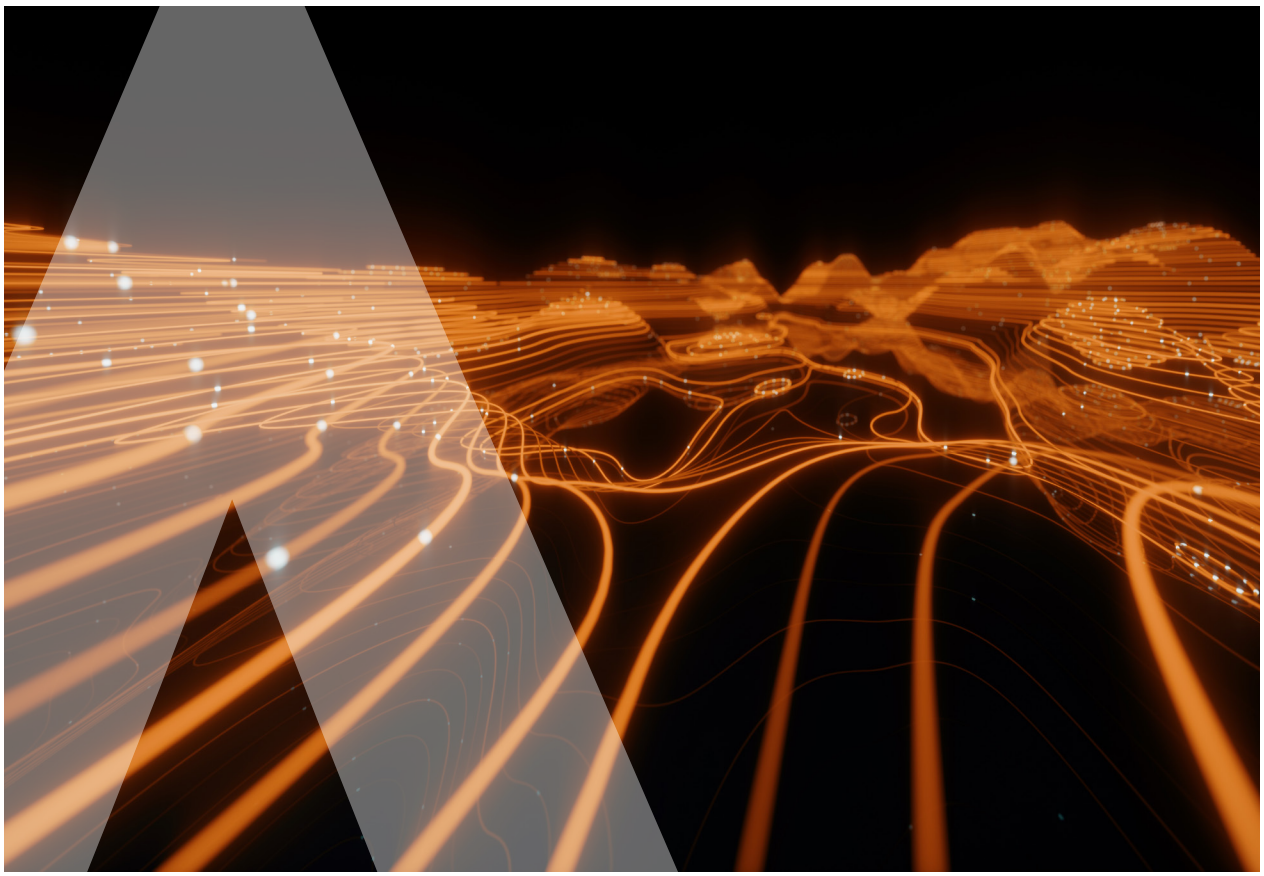
If passwords aren't changed regularly, attackers have a greater chance of compromising them. The same is true for machine identities which are often set with lengthy validity periods. In many companies, machine identities are not updated frequently or revoked when system administrators are reassigned or terminated. To minimize the risk of compromise, it is imperative that certificates and keys be changed at least once a year.

6. Do we have a plan for changing machine identities if they are compromised?

If users suspect that their passwords have been compromised, they must change them right away. The same is true when a Certificate Authority (CA) is compromised, a cryptographic algorithm is broken, or a cryptographic library bug is discovered. Machine identities that are exposed to these types of security events can no longer be trusted. Your PKI team should be prepared to quickly change certificates and keys when needed.

7. Are we duplicating machine identities across multiple systems?

If cyber attackers compromise a machine identity that is used across multiple systems, they automatically gain access to each account on those systems. To avoid unauthorized access, PKI teams should restrict the copying of machine identities across multiple systems to only those cases where it is absolutely required.



8. How quickly can we remove access to machine identities?

When an employee is terminated, you disable all user accounts and access as quickly as possible. You should do the same when administrators who have direct access to private keys are terminated or reassigned. Your PKI team should limit direct access to private keys, or at least immediately change keys and certificates, upon termination of anyone with privileges.

9. Do we limit who issues our machine identities?

You already take steps to ensure that user accounts, especially those that control access to corporate assets, are only given to authorized personnel. Likewise, machine identities should only be issued when requested by an authorized CA administrator. If not, attackers can take advantage of lax certificate issuance and review processes, requesting and installing a rogue certificate without your knowledge. Your PKI team should carefully review the issuance of certificates and keys to ensure that requesters and issuing CAs are authorized.

10. Have we configured our systems to limit where and how machine identities can be used?

For high-value applications and data, you carefully control how and where a user account can be accessed. You should do the same with machine identities, where misconfigured servers, applications and keystores may leave otherwise secure keys and certificates open to compromise. If not, an attacker who has access to a compromised private key may be able to use that key from another location. Proper configuration of machine identities and their supporting infrastructure should be regularly validated to ensure security.

Conclusion: Next Steps

Were you surprised by any of the answers to these questions? Does your PKI team have the tools they need to enforce critical machine identity security policies as effectively as you enforce policies for usernames and passwords?

Venafi offers a security platform that will help your PKI teams strengthen machine identity management and bring it to par with human identity protection in your IAM program. If you're ready to radically improve your machine identity management, learn more at **venafi.com**.

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.

Learn more at venafi.com