VENAFI®

// Venafi Study: Machine Identities Drive Rapid Expansion of Enterprise Attack Surface

Commoditization of Machine Identity Malware Drives
Unprecedented Increase in Security Risks

// Executive Overview

The Venafi Threat Intelligence Team analyzed public data on 110 machine identity threats over a five-year period from 2015 to 2019. They uncovered a profound change in the number, type and frequency of the three primary threat types: malware, vulnerabilities and cyberattacks. These trends, coupled with the exponential growth in the number and types of machines used on enterprise networks, serve as a serious warning to organizations that have not invested in a comprehensive machine identity management strategy as a cornerstone of their holistic, defense-in-depth security program.

Key Trends:

- The combined growth across all three types of machine identity threats between 2015 and 2019 is 478%.
- Cyberattacks and APTs that misuse machine identities have increased 1600% over the last five years.
- Vulnerabilities that leverage machine identities have increased 260% over this five-year period.
- Malware that leverages machine identities have increased 300% over the same five-year period, especially malware abusing SSH and code signing machine identities.
- Nearly 1 billion records have been breached by machine identity-related attacks.

Weak machine identity management programs are already costing enterprises millions of dollars. In early 2020, catastrophe modeling and risk assessment firm AIR Worldwide demonstrated that unprotected machine identities caused global economic losses of between $51 billion and $72 billion a year, with large companies suffering the highest proportion of losses.[1] These losses are expected to get worse as the number of machine identities enterprises require—and opportunities to exploit them—grow.

// Introduction

Nearly every organization is deploying digital transformation strategies to achieve business-critical initiatives, such as migrating IT infrastructure to the cloud and implementing DevOps methodologies to meet vital business objectives. Trusted machine identities are critical because every digital business initiative relies on machines. These initiatives are a key driver in the exponential increase in the number and types of machines on enterprise networks over the last few years. Such strategies have also evolved the type of machines that require identities as business networks diversify from traditional servers and PCs to include mobile and IoT devices, as well as software-defined workloads, online applications, containers and APIs. Already there are more than 31 billion IoT devices in service worldwide,[2] and the number of connected mobile devices is expected to grow to 12.3 billion by 2022.[3] Between 2018 and 2023, 500 million new logical apps will be created—a sum that's roughly equal to the total number of apps built over the previous 40 years.[4]

Like people, machines need to authenticate their identities to ensure safe communications with one another. Unlike people, who authenticate their identities through usernames, passwords and multifactor authentication, machines rely on cryptographic keys and digital certificates to connect and communicate securely. In a July 2020 report titled *Hype Cycle for Identity and Access Management Technologies, 2020*, research firm Gartner writes: "As environments become more digital and cloud-enabled, security leaders will need to ensure that they can manage the increase in volume and velocity of machine identities that will be required to support their digital business needs."[5]

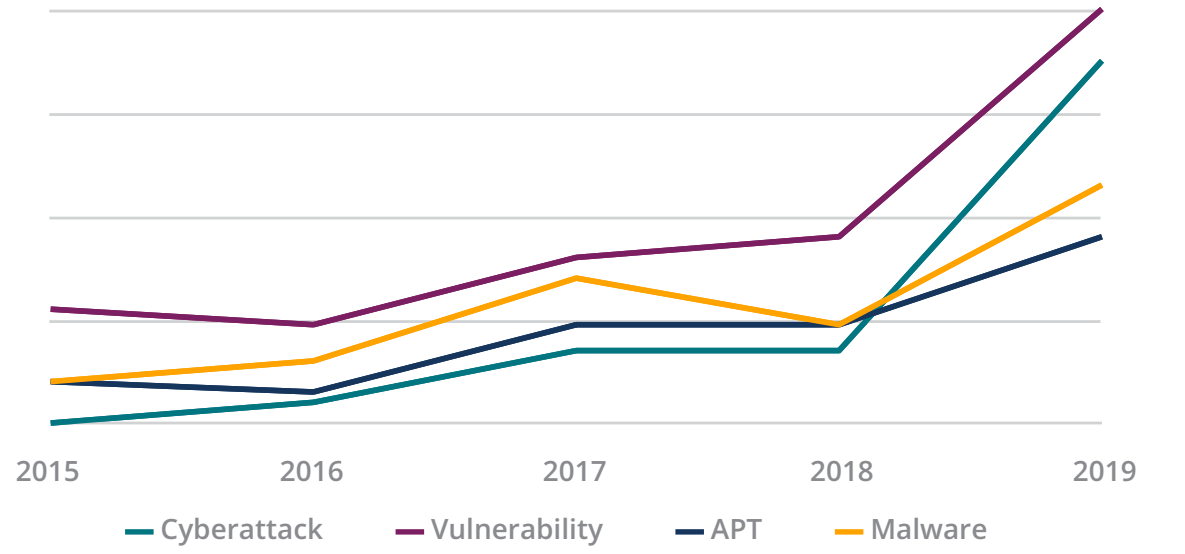
And as key and certificate populations continue to explode, organizations are just beginning to realize that machine identities need the same level of management protection as human identities—and that effective machine identity management is becoming a more complex undertaking than managing human identities. One of the reasons for this complexity is that machines use three different types of identities to connect and authenticate themselves:

- SSL/TLS certificates, which are used by websites and other online machines, as well as cloud workloads and containers.
- Secure Shell (SSH) keys, which are used to control access to remote servers and other devices.
- Code signing keys, which are used to authenticate code within applications.

The bigger the universe of machines, the more complicated it is to manage machine identities. TLS certificates expire and need to be replaced frequently to avoid service disruptions. In fact, TLS certificate lifespans have been dropping rapidly—from five years in 2012 to one year in 2020. This shift alone dramatically increases the challenge of managing these identities effectively. In contrast, SSH keys never expire and are rarely removed, creating a different kind of security risk, particularly in the cloud. And although code signing keys must be protected at all times, the developers responsible for signing code too often aren't cognizant of the potential security risks these keys can pose.

This massive proliferation in the number and type of machine identities has triggered a corresponding increase in the machine identity threat attack surface, which has ballooned over the last five years. As a result, threat actors—from common hackers to nation-state entities—are increasingly targeting these critical security assets. Forged, fraudulent or compromised machine identities give threat actors the power to gain initial access to networks and, once in, allow them to pivot across multiple systems. Errant machine identities also offer threat actors the potential to create persistent back doors, while cleverly evading existing defense mechanisms.

All Threat Types



Because most organizations lack comprehensive machine identity management strategies, the number of threat actors that are focusing on exploiting weaknesses in machine identity management is rising rapidly. In the same Hype Cycle report, Gartner recommends: "An enterprisewide machine identity management strategy is needed to support digital transformation in modern IT environments."[6]

// Machine Identity Threat Analysis Methodology

To map out the machine identity attack surface from 2015–2019, the Venafi Threat Intelligence Team analyzed publicly reported attacks, security incidents and vulnerabilities that involved machine identities. The team based their analysis on the MITRE ATT&CK framework as the foundation for documentation, description and analysis of the threats, as well as information uncovered by Venafi's threat intelligence team.

The challenge with analyzing public data is that many—and perhaps even most—attacks are not publicized. Among the relatively small number of attacks that are disclosed, most don't include threat details that involve machine identities.

Although the number of threats analyzed for this paper is relatively small—110 total—they represent a fraction of all attacks involving machine identities in the wild. More importantly, this small data set shows a clear, upward trend in machine identity threats over the last five years, with a significant spike in 2018 and 2019.

3 Critical Machine Identity Threats Faced by Organizations

This analysis looks at three groups of machine identity threats that can be used by a threat actor to undermine an enterprise's security posture:

- Security vulnerabilities
- Malware
- Organized cyberattacks and APTs

All of these threats leverage at least one of the following types of machine identities: TLS certificates, SSH keys or code signing keys. "As we move to a machine-led world, machine identity management and protection problems are only going to get bigger," Kevin Bocek, vice president, security strategies and threat intelligence at Venafi, says.

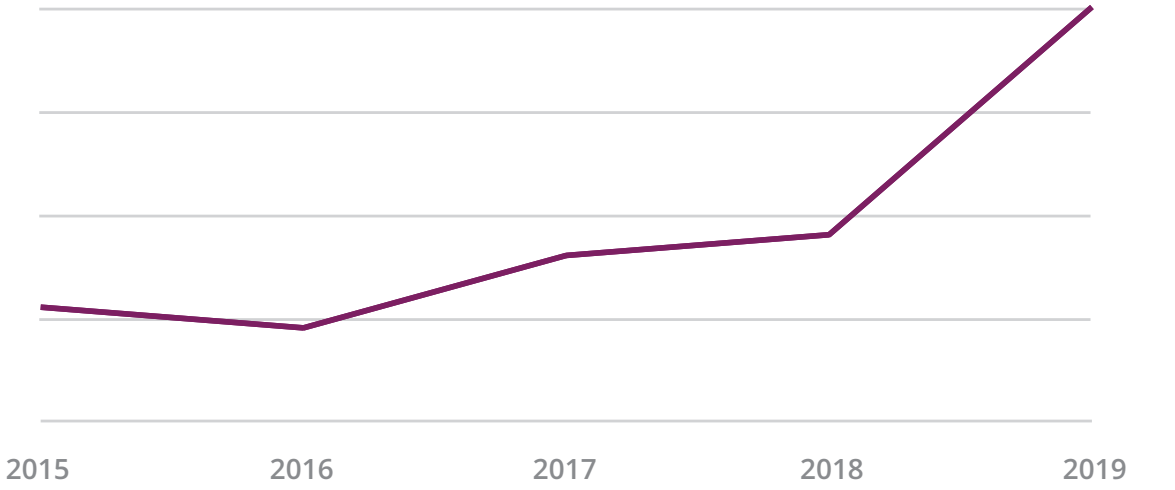
Cyberattack and APT events typically use a combination of discovered machine identity vulnerabilities and malware that exploit weak or improperly managed machine identities to achieve their goals. So, it isn't a coincidence that the rise in these types of malware and vulnerabilities are rising at a similar rate—or that resulting cyberattacks are rising at an even greater one.

// Machine Identity Vulnerabilities Jump 260%

Vulnerabilities that involve machine identities have become increasingly common. Even though machine identities are required for just about everything on enterprise networks, many IT and InfoSec teams don't understand their importance to the overall security posture of their organization. Taking advantage of this lack of organizational knowledge has encouraged cybercriminals to actively search for machine identity vulnerabilities to exploit.

Perhaps the best-known machine identity-related vulnerability, Heartbleed, was first reported back in 2014. Heartbleed resulted from a flaw in OpenSSL that allowed anyone on the internet to read the memory of a vulnerable system and extract the private key used to encrypt traffic. According to Yana Blachman, principal threat intelligence analyst at Venafi, "Malicious actors were able to access a server's private encryption key—and just one exploit of this bug exposed 4.5 million patient records at the hospital group Community Health Systems."

Vulnerability Trends



The recent rapid increase in machine identity vulnerabilities is particularly alarming. Over the last five years, the number of vulnerabilities involving machine identities grew by 260%, increasing by 125% between the years 2018 and 2019 alone. In fact, it's likely that the problem is significantly worse than the data shows. While some vulnerabilities can be difficult for cybercriminals to exploit, Blachman explains that "attackers and black hats stay very quiet about the vulnerabilities they can exploit so they can remain stealthy. Often, it can be years before we know if a vulnerability has been exploited in the wild."

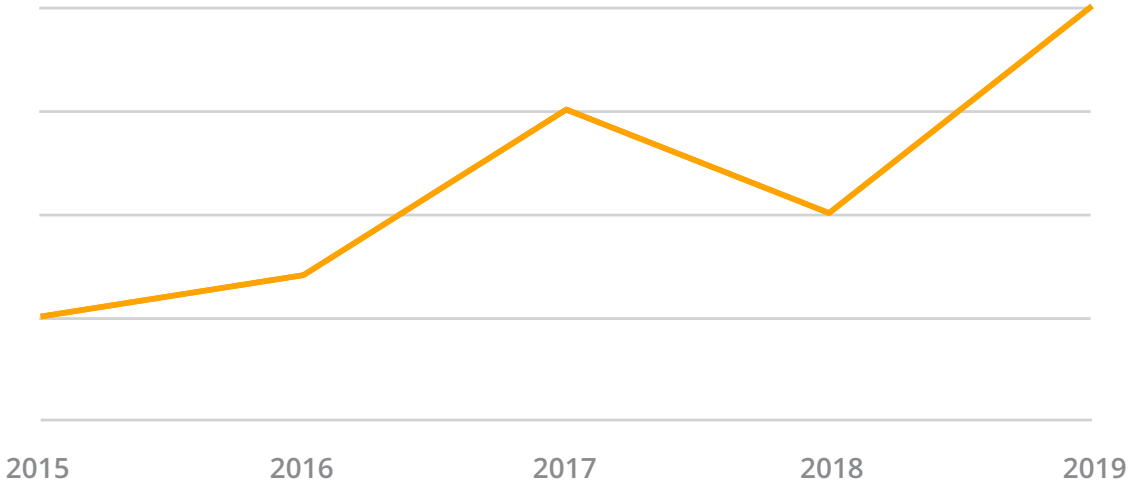
// Machine Identity Malware Soars by 300%; Becomes Key Component of Cybercriminal Toolkits

The malware analyzed in this paper refers specifically to high-profile campaigns that target enterprise users and involve a machine identity component in their design. To be clear, this paper defines malware as any type of malicious software—such as a Trojan, cryptominer, worm, ransomware or Remote Access Tool (RAT)—used by malicious actors as part of an attack on a target or network for the purpose of monetization, cybercrime, cyberespionage or sabotage. In light of the rise in the number of machine identities that are relatively unprotected, malware authors are introducing more and more machine identity capabilities.

Over the last couple of years, sophisticated machine identity capabilities have become a larger part of the arsenal of "commodity" malware used in cybercriminal toolkits. This is a significant and ominous change in the machine identity threat landscape; prior to 2015 the use of machine identities in malware was largely limited to attacks conducted by nation-states and other well-funded cybercriminal operations.

Malware types that abuse machine identities doubled between 2018 and 2019.

Malware Trends



SSH Machine Identities Increasingly Abused by Malware

Malware that abuses SSH keys is becoming increasingly popular with cybercriminals for two reasons. First, SSH keys don't expire and are rarely monitored closely. Second, the same SSH key is often used to access multiple machines; this is a common practice with cloned virtual machines (VMs). Without a comprehensive machine identity management program in place to provide visibility into how SSH keys are issued and used and a program to automatically rotate or revoke orphaned, compromised or unneeded keys, organizations leave themselves vulnerable to severe business risks. And these risks become even more pronounced as organizations move more workloads to the cloud where SSH keys are required for a wide range of basic tasks.

SSH-based malware is designed not only to infect as many targets as possible, but also to provide attackers with the ability to pivot into other areas of target networks, where it can steal SSH keys from the target or insert back doors for attackers to exploit at a later time. In 2019 alone, some of the highest profile malware campaigns, including the infamous Trickbot[7] and Skidmap,[8] introduced SSH components to their modules—enabling attackers to seize SSH keys and seek associated information that would allow them to pivot to other connected machines.

Cybercriminals Hiding Behind TLS Machine Identities

Stolen and fraudulent TLS certificates are also a key element of the cybercriminal toolkit. For years, threat actors have obtained fraudulent or stolen TLS certificates to support malicious activity, including Man in the Middle (MiTM) attacks and data exfiltration.

Another common tactic is to set up phishing websites with spoofed "lookalike domains" that appear to be legitimate. Recent Venafi research showed that lookalike domains more than doubled in number from 2018 to 2019. Moreover, the total number of certificates used in lookalike domains was more than 400% greater than the number of the authentic domains they were spoofing, making these phishing sites appear to be legitimate.

Misuse of Code Signing Machine Identities Is Rampant

Stolen and fraudulent code signing keys and certificates have also become an increasingly common component of machine identity-based malware. Initially used only by advanced threat actors, such as the nation-state attackers behind Stuxnet, malware that takes advantage of poorly protected code signing keys and certificates grew increasingly popular as the last decade progressed.

In order to appear valid, more and more malware authors sign their software with legitimate code signing certificates that were either fraudulently obtained or stolen from other companies in a separate campaign. For example, the notorious LockerGoga ransomware from 2019 was reported to be signed with a stolen code signing certificate most likely obtained in a related, parallel campaign.[9]

// Cyberattacks and APTs Surging

For this analysis, a cyberattack is any attempt by a malicious actor to misuse machine identities to interfere with a machine belonging to a company or an individual. These attacks are designed to achieve a variety of goals, such as accessing a machine without authorization, stealing or corrupting data, or pivoting from one machine across the network in order to eavesdrop on encrypted traffic or steal sensitive data, among other types of damage.

Machine Identity Cyberattacks Skyrocket by 1600%

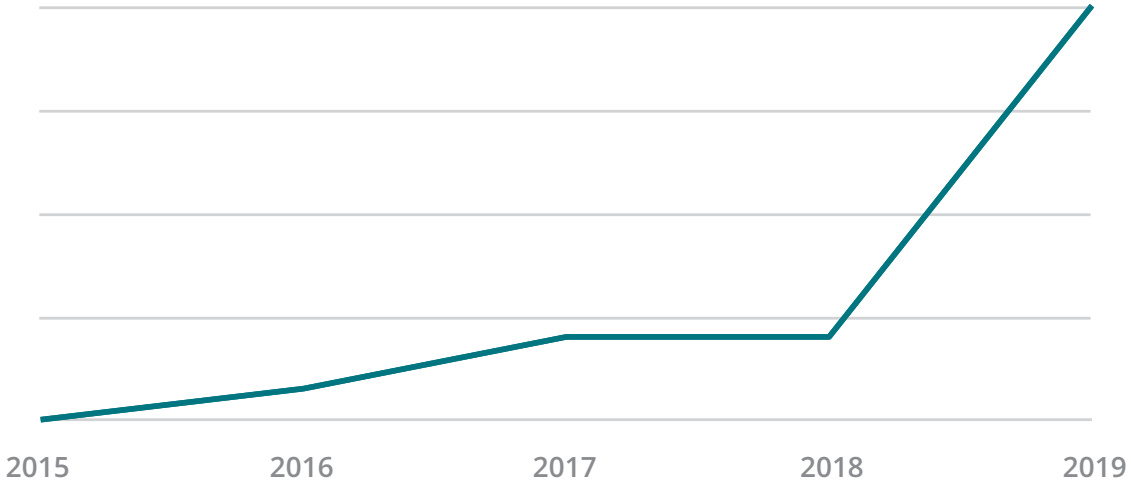
Cyberattackers typically wield a wide range of tools and vulnerabilities to penetrate networks, gain a foothold within them and then use this access to obtain whatever end their perpetrators want to fulfill. With the rapid rise in machine identity malware and vulnerabilities, it should come as no surprise that rapid increases in attacks that rely on poorly managed or improperly protected machine identities are increasing rapidly.

Threat actors have leveraged weakened machine identities to make their cyberattacks more effective since the beginning of the last decade. In 2010, malicious actors repeatedly hacked domain registrar VeriSign in an attempt to compromise the operational integrity of the Domain Name System (DNS). More recently, in 2017, Equifax suffered a large-scale data breach[10] caused by an expired TLS certificate. Due to the lack of an effective machine identity management program, this massive breach wasn't discovered for almost a year after the machine identity expired.

Cyberattacks that leverage machine identity weaknesses jumped dramatically toward the end of the five-year period studied, as more and more threat actors discovered how effective improperly managed machine identities can be in executing successful attacks. Stolen or forged TLS certificates now sell for as much as $1,600 on the dark web[11] because they significantly increase the likelihood of a successful attack. For example, cybercriminals can manipulate machine identities to evade detection—by hiding in encrypted traffic or impersonating a trusted machine.

Several recent successful cyberattacks used machine identities as a key element in their exploits. In 2018, the hotel chain Marriott[12] learned that attackers had been dwelling in their network since 2014 with access to the private records of 357 million customers after stealing encryption keys. Similarly, in 2020,[13] domain registrar and web hosting provider GoDaddy revealed that cyberattackers, after stealing a vulnerable SSH key on the company's servers, proceeded to steal almost 30,000 SSH credentials from its customers.

Cyberattack Trends



In fact, between the year 2015 and the year 2019, the number of reported cyberattacks that utilized machine identities grew by more than 1600%, with this amount increasing by 433% between the years 2018 and 2019 alone.

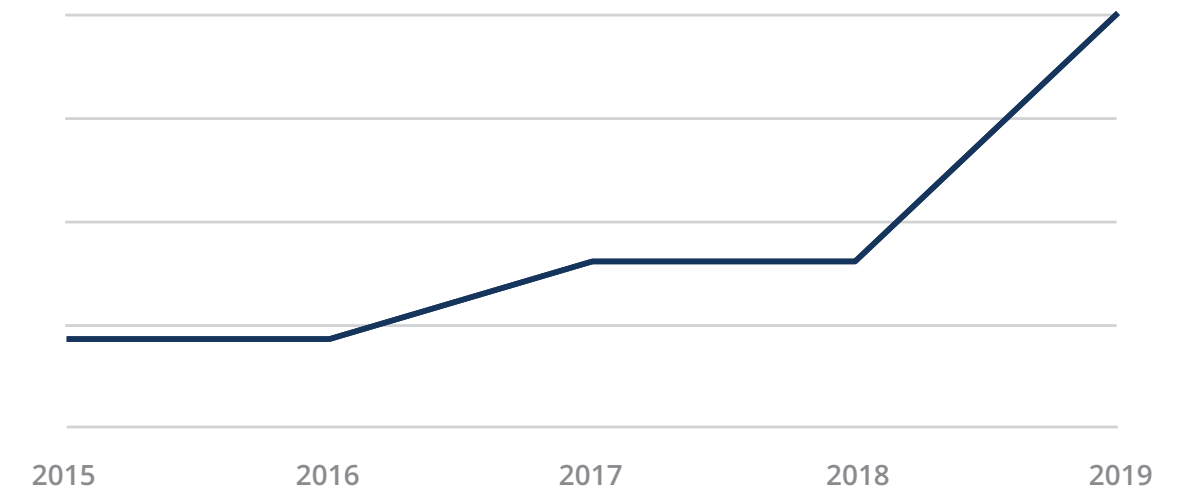
APTs Continue to Target Machine Identities; Jump by 400%

APTs have been tallied separately from other types of cyberattacks because of the difference in the motivation and intent of these attacks. A primary goal of an APT attack is to remain persistent on the victim's network. "APT attackers need just one point of entry to wage their campaign, and machine identities are extremely useful because they support and enable persistence, lateral movement and defensive evasion," Blachman says. "Successful attackers can often create a 'back door' into victim networks that can remain viable for months or even years, without being discovered or exposed."

The prototype of APT attacks that leverage machine identities is the legendary Stuxnet attack, which (as discussed earlier in this paper) hijacked code signing keys to bring down the Iranian nuclear program.[14] Other well-known APTs include the infamous Russian state-sponsored cyberespionage threat group Turla[15] and their RAT tool Reductor[16] that was designed to compromise a TLS connection "on the fly," either from within the victim's network or on the ISP level, and Operation Shadowhammer, which created malicious backdoors in more than 1 million ASUS computers by exploiting improperly protected code signing keys in 2019.[17]

"By stealing 'trusted' machine identities from global technology companies, perpetrators of APTs can execute effective attacks that don't raise any alarms until well after the damage is done. That's why machine identities must become a core component of any organization's security posture—because there's no doubt we're going to see a lot more of these attacks in the future," Bocek says.

APT Trends



Between 2015 and 2019, the number of reported APTs grew by 400%. Reports of these attacks increased by 150% between the years 2018 and 2019 alone.

// Conclusion

The global COVID-19 pandemic has brought the risks posed by the rapid expansion in the machine identity attack threat surface to the forefront of cybersecurity concerns. "For many enterprises, the global pandemic has compressed years-long strategic change into months, even weeks. For others, it has forced them to adopt approaches that they'd previously been cautious about," Gartner writes in their Hype Cycle report.[18]

Blachman supports Gartner's recommendations. "The rising number of machine identities correlates with the acceleration in the number of threats—the two lines rise in tandem. As a result of our increased reliance on machine identities, every organization's attack surface is growing ever more quickly, especially with the additional pressures brought about by COVID. Unless organizations boldly respond to this challenge, things will get a lot worse," she says.

The power of threats that leverage machine identities is evident in the sheer number of records compromised by the relatively small number of threats studied. Over the last five years, nearly 1 billion records have been breached in attacks that leverage machine identities, and these attacks were among the most serious and damaging.

Automating full lifecycle machine identity management is especially important given that the three primary types of machine identities—TLS, SSH and code signing—each come with unique challenges relative to one another. Venafi Trust Protection Platform currently is the only commercial enterprise solution on the market that provides a full lifecycle machine identity management platform for all machine identity types—even in large, complex networks—that fulfills this new guidance.

If your enterprise organization needs help managing your machine identities—or you're otherwise interested in learning how Venafi has helped hundreds of the world's most security conscious organizations build effective machine identity management programs, contact us at **venafi.com**.

Trusted by

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

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

References

1. AIR Worldwide. The Economic Impact of Machine Identity Breaches. February 2020.
2. IDC. Worldwide Spending on Digital Transformation Will Reach $2.3 Trillion in 2023, More Than Half of All ICT Spending, According to a New IDC Spending Guide. October 28, 2019.
3. Cisco. Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022. February 18, 2019. Document ID:1486680503328360.
4. IDC. IDC FutureScape: Worldwide IT Industry 2019 Predictions. October 2018. Document Number: US44403818.
5. Ant Allan. Hype Cycle for Identity and Access Management Technologies, 2020. Gartner. July 16, 2020. 20.
6. Ant Allan. Hype Cycle for Identity and Access Management Technologies, 2020. Gartner. July 16, 2020. 19
7. SentinelOne. SentinelLabs Identifies Hidden Link Between TrickBot "Anchor" & Purported North Korea "Lazarus" Tool Deployment. December 11, 2019.
8. Remillano, Augusto; Urbanec, Jakub and Luy, Wilbert. Skidmap Malware Uses Rootkit to Hide Mining Payload. Trend Micro. September 16, 2019.
9. Greenberg, Andy. A Guide to LockerGoga, the Ransomware Crippling Industrial Firms. Wired. March 25, 2019.
10. Krebs, Brian. Breach at Equifax May Impact 143M Americans. Krebs on Security. September 7, 2017.
11. Maimon, David; Wu, Yubao; McGuire, Michael; Stubler, Nicholas and Qiu, Zijie. Evidence-Based Cybersecurity Research Group at the Andrew Young School of Policy Studies at Georgia State University and the University of Surrey. SSL/TLS Certificates and Their Prevalence on the Dark Web (First Report). 2019. 6.
12. Meyer, Sarah. Half a Billion Guests Affected by Massive Marriott Data Breach. CPO Magazine. December 3, 2018.
13. Corfield, Gareth. GoDaddy hack: Miscreant goes AWOL with 28,000 users' SSH login creds after vandalizing server-side file. The Register. May 5, 2020.
14. Zetter, Kim. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Wired Magazine. July 11, 2011.
15. Osborne, Charlie. Russian APT Turla targets 35 countries on the back of Iranian infrastructure. ZDNet. October 21, 2019.
16. Blachman, Yana. The Latest on Reductor: Turla-Associated RAT Uses Novel Method to Compromise TLS Connections to Mark and Monitor Its Victims. Venafi Blog. October 17, 2019.
17. GReAT and AMR. Operation ShadowHammer: a high-profile supply chain attack. Kaspersky SecureList. April 23, 2019.
18. Ant Allan. Hype Cycle for Identity and Access Management Technologies, 2020. Gartner. July 16, 2020. 3.