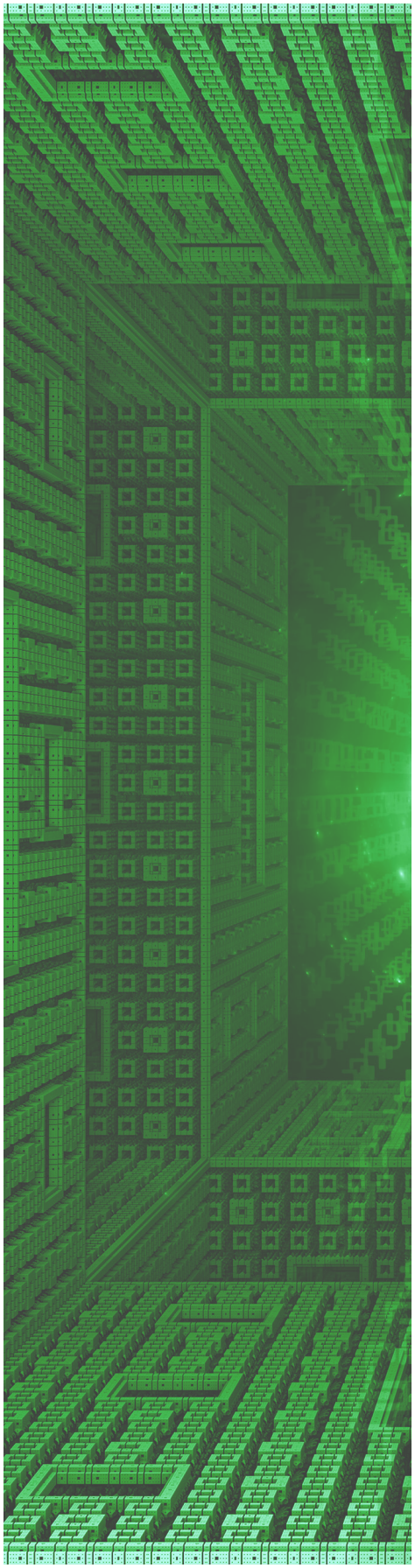
White Paper

VENAFI®

The Machine Identity Crisis

How the explosion of machines is affecting the security of machine-to-machine communications



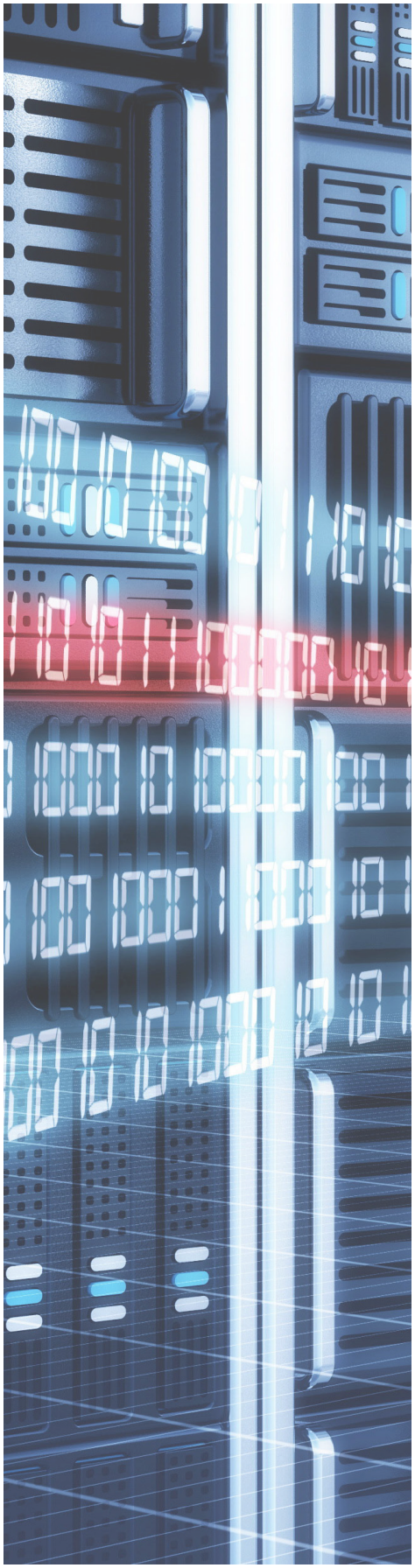
Executive Overview

The use of machines is driving unprecedented improvements in business efficiency, productivity, agility and speed. With businesses increasing their reliance on machines, the number of machines on enterprise networks is growing exponentially. To communicate securely, each machine needs a unique identity to authenticate and secure communications. However, organizations' abilities to create, manage and protect these machine identities is simply not keeping up with the pace of their evolution.

Our increased dependence on machines is so profound that even the definition of machine is undergoing radical change. The number and type of physical devices on enterprise networks has been rising rapidly, but this is outstripped by the number of applications and services they host. At the same time, cloud adoption has spawned a tidal wave of virtual devices that are created, changed and destroyed. These changes have expanded the definition of machine to include a wide range of software that emulates physical devices.

Recently, the need to rapidly evolve business systems has also driven a radical new methodology designed to increase the speed of software development and delivery. In DevOps and Fast IT environments, software is developed as a suite of small, independently deployable software applications that run a unique process or provide applications with their own operating environments—creating a constant flow of compact machines that are deployed, changed and destroyed in moments at machine speed and scale. This evolution is stretching the definition of machine even further.

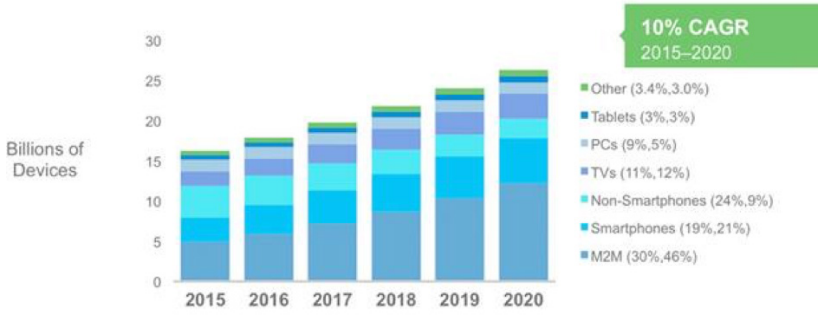
Secure and reliable machine authentication is needed to protect machine-to-machine communication. Because machines are now used to control nearly every aspect of our global digital economy, the need to create, install, rapidly assess and ensure the integrity of communications between machines is critical and must be able to scale instantly. However, organizations simply do not have the technology or automation needed to accurately monitor and protect the vast number of machines identities businesses now support. Cyber criminals understand this and target machine identities for use in a wide range of cyber attacks.



The Exploding Number of Machines We Can't Live Without

Globally, devices and applications are growing significantly faster than the human population. While the population of humans is projected to grow at a Compound Annual Growth Rate (CAGR) of 1.1 percent, devices and applications will race forward at a CAGR of 10 percent. This rapid growth of machines will even outpace the growth in internet users, (CAGR of 7 percent). This steep climb in the number and type of machines is driving an increase in the average number of devices per household as well as per internet user around the world. The Cisco Visual Networking Index also predicts the following:[1]

- Overall, IP traffic is expected to grow at a CAGR of 24 percent from 2016 to 2021. Machine-to-machine connections will be the fastest-growing category of IP traffic, more than doubling between 2016 and 2021 to 13.7 billion connections in 2021.
- The number of devices connected to IP networks will be three times as high as the global population by 2021. There will be 3.5 networked devices per capita by 2021, up from 2.3 networked devices per capita in 2016.
- Accelerated in part by the increase in devices and the capabilities of those devices, IP traffic per capita will reach 35 GB per capita by 2021, up from 13 GB per capita in 2016.



Growth in Automated Machine Communication

Four major trends are driving the growth in machine volume; each of these trends has a distinct and cumulative impact on the need to provide each machine with a unique identity and protect their communication:

- Mobile device growth
- IoT device expansion
- Cloud adoption
- DevOps continuous progression

Growing Number of Mobile Devices

Mobile devices fit the expected definition of a physical machine, and they've been around for years. Although mobile adoption is slowing, the number and variety of devices continues to expand. More importantly, the volume of sensitive personal and enterprise data which flows through these devices continues to climb.

- Mobile devices in use, including phones and tablets, will grow from over 11 billion in 2016 to over 16 billion by 2020 fueled by new form factors including tablets, phablets and updated laptop versions.[2]
- Global mobile data traffic is expected to increase sevenfold between 2016 and 2021, growing at a CAGR of 47 percent. Mobile data traffic volume is expected to reach 49 exabytes per month by 2021.
- The global mobile encryption market is expected to grow at 25 percent by 2022.
- Global mobile data traffic has grown 18-fold over the past 5 years and will represent 20 percent of total IP traffic by 2021.[3]

Although mobile devices have been a fact of life on enterprise networks for over a decade, securing and protecting the sensitive corporate data which flows through these devices is an ongoing challenge. The difficulties of protecting mobile data are further compounded by the fact that many devices are owned by employees.

Organizations face an escalating pressure to uniquely identify and authenticate each device so they can authorize secure communication between mobile devices, enterprise networks and the internet. Unfortunately, most organizations do not have the tools necessary to accomplish this, reducing their ability to protect the sensitive data that flows through these devices.

Upsurge in IoT Devices

IoT devices encompass a wide range of physical devices with embedded electronics, software, sensors or actuators; many of them allow objects to be sensed or controlled remotely across networks. Businesses are becoming the top adopters of IoT solutions, motivated by lower operating costs and increased productivity.

IoT devices play a crucial role in the management of our global critical infrastructure, including smart grid devices and virtual power plants; intelligent transportation systems, including car navigation and traffic control systems; health monitoring; and emergency notification systems. Further adoption in critical infrastructure is expected to increase rapidly.

IoT devices require network connectivity so they can collect and exchange data. As a result, the volume of communication, and the need to uniquely identify each device so communication can be secured, is expected to explode over the next five years:

- Over 8.4 billion IoT devices will be connected in 2017, up 31 percent from 2016. Gartner predicts that 25 billion IoT devices will be in use by 2020,[4] and IoT devices will account for 70 percent of the devices on the internet.[5]
- Since industrial businesses and governments are the largest adopters of IoT,[6] public infrastructure including stoplights, bridges, water facilities, healthcare facilities and power plants are now viable cyber attack targets.
- Microsoft has called for a cyber security policy focused on IoT.[7] However, these efforts will take time to solidify, leaving enterprises grappling with how to secure communication between IoT devices already connected to their networks.

The real business value from the deployment of IoT devices is derived from the data captured by them. Because IoT devices typically have very limited CPU and storage capabilities, the data captured must be transmitted to a central location where it can be collected, stored and analyzed; and since much of the data from critical infrastructure is sensitive, it is imperative that these communications be authenticated and protected. However, as the number of IoT devices multiplies, enterprises face increasing challenges in securing communications between IoT devices, the internent and enterprise networks.

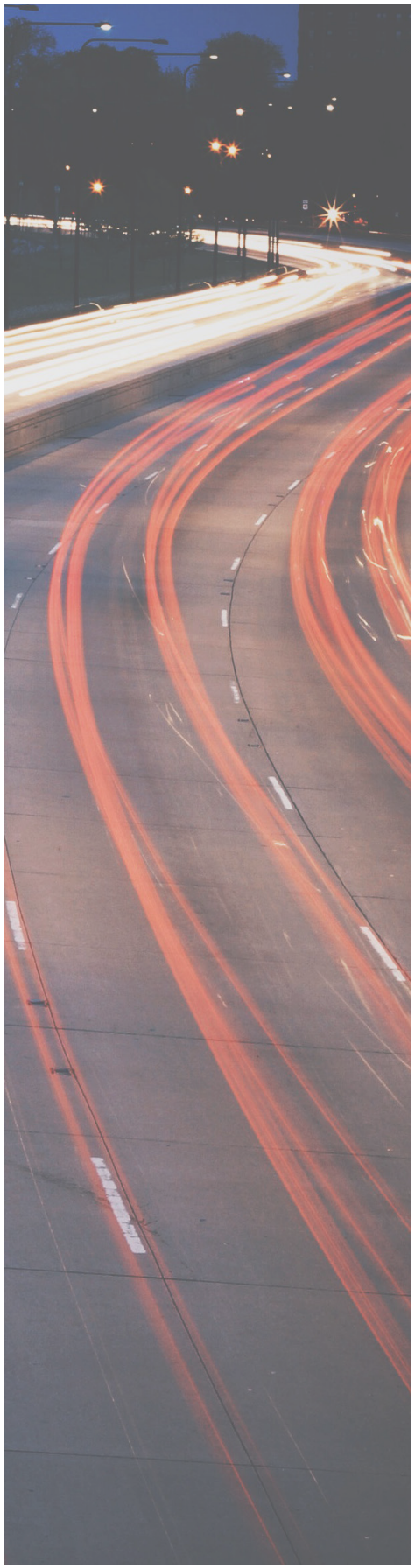
Dynamism of Cloud Computing

By leveraging shared pools of configurable resources, cloud computing allows enterprises to get their applications up and running faster, improve manageability, reduce maintenance and rapidly adjust resources to address fluctuations in business demand. This paradigm shift has stretched the definition of machine to include a wide range of software that emulates physical machines. In the cloud, people are no longer the limiting factor in the creation of machines; machines automatically create, configure and destroy machines in response to business demand.

The average lifespan of a virtual machine is just 23 days, in comparison to the expected three to five year life span of a physical device. This inherent dynamism in cloud environments complicates the task of uniquely identifying, authorizing and securing communication between physical and virtual machines. The rapid deployment, change and revocation of their identities exponentially increases the challenge of keeping communication to the cloud and between cloud servers secure and private.

- According to Gartner, overall demand for cloud computing is projected to grow 18 percent in 2017 and public cloud infrastructure services are expected to grow at 36.8 percent to $34.6B. The same report predicts that by 2020, 92 percent of workloads will be processed by cloud data centers; only 8 percent will be processed by traditional data centers.[8]
- IDC predicts that, from 2015-2020, public cloud spending will grow nearly seven times faster than overall IT spending growth.[9]
- Cloud workloads will more than triple (3.2-fold) from 2015 to 2020.[10]
- The market for cloud-based IT-as-a-Service technologies will accelerate over the next 2.5 years from $361B to $547B. At this pace, IT-as-a-Service will represent more than half of IT spending by 2021/2022.[11]

Although the business benefits of cloud computing are profound, to protect the security and privacy of cloud data, businesses must encrypt the data and adequately secure the machine identities that determine whether communication between enterprise network devices and cloud services can be trusted.



DevOps and Fast IT Adoption

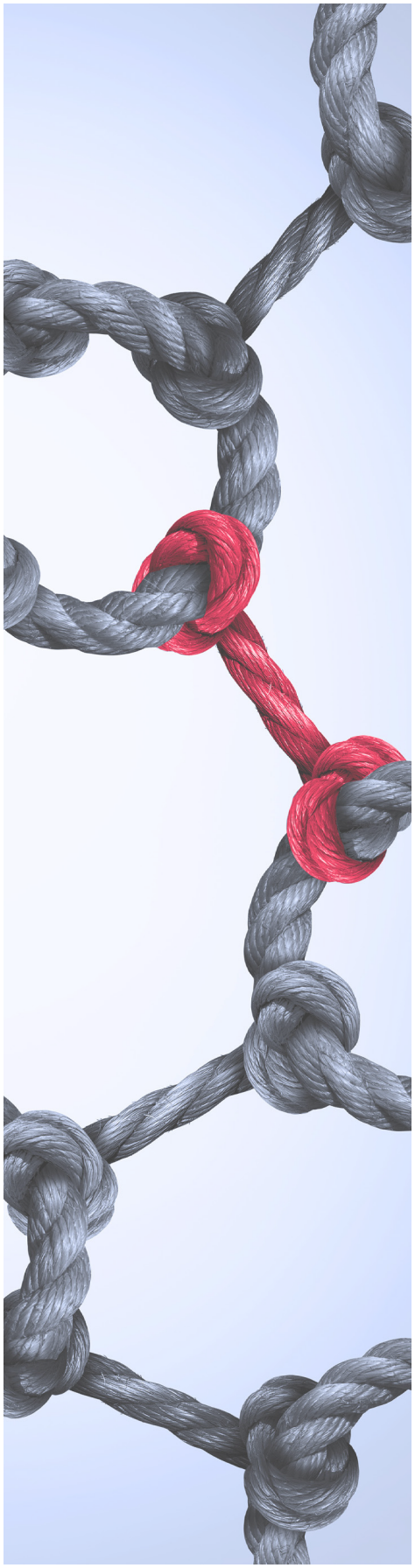
The business advantages that motivated widespread cloud adoption—speed, agility, efficiency and economies of scale—are also the driving forces behind DevOps (sometimes called Fast IT). These relatively new initiatives help remove the latency connected with software development by dramatically speeding up the delivery of software-driven business solutions. DevOps and Fast IT programs involve the continuous development of incremental change in smaller segments of software programs. Fast IT developers use cloud-based, self-contained runtime environments known as containers to run applications that consist of individual modules, also called microservices, ushering in an entirely new definition of machines—each of which requires a unique identity.

This evolution has sped up the creation of machines and multiplies the already complex task of securing machine-to-machine communication in the cloud.

- Gartner expects that by the end of 2018, 50 percent of enterprises will be running containers in their production environments.[12]
- A major driver for Fast IT is IoT-generated data. By 2021, IoT-enabled devices will increase data center traffic nearly 40 times.[13]
- The application container market is growing at a CAGR of 31 percent.[13]
- Forrester predicts that Linux containers will be available in every major public and private cloud platform in 2017.[14]

DevOps speeds up the creation of new types of machines by an order of magnitude. For example, while the life of a virtual server is just 23 days, the average life of a container is a fraction of that—just 2.5 to 5 days. This reliance on containers alone dramatically increases the challenge of safely generating and securing machine identities to meet their machine speed and scale.

This problem is particularly acute because many DevOps projects center on business critical applications. The containers and microservices used in these projects communicate constantly with each other and the network. Consequently, organizations need a new paradigm to help them protect this barrage of new machine identities that are an intrinsic part of DevOps and Fast IT projects.



The Accumulating Machine Identity Crisis

Organizations that were managing a thousands machine a few years ago are now trying to manage hundreds of thousands or even hundreds of millions today. These machines include a wide range of physical and virtual devices—each with a unique identity that must be protected.

This onslaught of machines is requiring that organizations protect evolving machine-to-machine communication but most don't have the visibility or technology necessary to do this effectively. To make matters worse, the trends driving this complexity—mobile, IoT, cloud, and DevOps—unique and cumulative complications and they all affect enterprise networks simultaneously.

Given the exponential growth of machines and their increasingly transient nature, machine identity protection is already overwhelming IT and security teams. Organizations need a solution that is as dynamic as the trends that drive it.

The only way organizations can solve these problems is with intelligent automation. Organizations must have complete visbility into every machine identity that touches their networks, be able monitor these identities in real time to detect misuse, and be able to automatically remediate any vulnerabilities discovered at machine speed and scale. This is the only way organizations can ensure the security of machine-to-machine communications.

Learn how Venafi solutions can help your organization secure machine-to-machine communication across every layer of your IT environment. www.venafi.com

TRUSTED BY THE TOP

5 OF 5 Top U.S. Health Insurers
5 OF 5 Top U.S. Airlines
4 OF 5 Top U.S. Retailers
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 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

References

1. Cisco Visual Networking Index: Forecast and Methodology, 2016–2021. September 15, 2017. Document ID:1465272001663118.
2. The Radicati Group, Inc. Mobile Growth Forecast, 2016-2020. January 2016.
3. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021. Updated March 28, 2017. Document ID:1454457600805266.
4. Pettey, Christy. Gartner. The Internet of Things and the Enterprise. August 31, 2015.
5. Camhi, Jonathan. Business Insider. BI Intelligence Projects 34 Billion Devices Will Be Connected by 2020. November 6, 2015.
6. Columbus, Louis. Forbes. 2016 Internet Of Things (IOT), Big Data & Business Intelligence Update. October 2, 2016.
7. Abendroth, Benedikt; Kleiner, Aaron and Nicholas, Paul. Microsoft. Cybersecurity Policy for the Internet of Things. 2017.
8. Gartner Press Release. Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017. February 22, 2017.
9. IDC. Worldwide Semiannual Public Cloud Services Spending Guide. Document ID: IDC_P33214_0817.
10. Cisco. Cisco Global Cloud Index: Forecast and Methodology, 2015–2020. 2016.
11. Deloitte. Technology, Media and Telecommunications Predictions 2017.
12. Brodie, Steve. The Enterprisers Project. DevOps Trends Emerging for 2017 and Beyond: DevOps Trends for 2017, Examined. January 19, 2017.
13. CISION PR Newswire. Application Container Market Growing at a CAGR of 31.26% During 2017 to 2021 Says a New Report at ReportsnReports.com. May 23, 2017.
14. Forrester. The Public Cloud Services Market Will Grow Rapidly to $236 Billion in 2020: 2020 Sizing Forecast Shows Strong Growth, But With Signs of Maturity on the Horizon. September 1, 2016.