

# Why CIOs Worry About Machine-Identity-Related Outages

Cryptographic keys and digital certificates serve as machine Identities. While these are critical to security, our CIO survey revealed that concerns about certificate-related outages plague nearly all organizations.

## OUTAGES SCOPE:

### How big is the problem?

#### PERSISTENCE

**60%**

CIOs who experienced a certificate-related outage in the last 12 months

#### COST

**\$5,600**

Average cost per minute of a critical infrastructure outage



## OUTAGES FORECAST:

### Will it get worse before it gets better?

#### INCREASED EXPOSURE

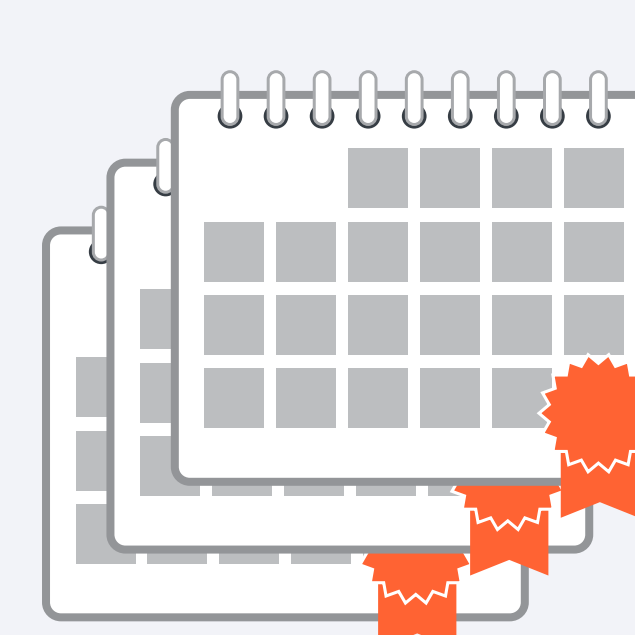
**55%**

CIOs expect a 50% increase in the number of certificates they use in 2019

#### SHORTER LIFECYCLES

**90-day**

Shorter certificate lifespans are becoming more common



#### LIMITED VISIBILITY

**57,420**

unknown keys and certificates are discovered, on average, when a machine identity protection solution is deployed



## OUTAGES CONCERNS:

### What do CIOs worry about most?

#### NEGATIVE IMPACT

**50%**

Unsatisfactory customer experience

**45%**

Consuming IT department time and resources

**43%**

Impact on revenue

**39%**

Lower worker productivity and company reputation

## OUTAGES EXPOSURE:

### Why are outages so prevalent?

#### WE'RE THINKING TOO SMALL

**70%**

Admit to tracking fewer than 50% of common machine identities types

#### IT'S COMPLICATED

**85%**

Believe IT system complexity will make outages more painful in the future

## OUTAGES AS A SECURITY SYMPTOM:

Certificate-related outages expose unmonitored machine identities which may also be vulnerable to hacker misuse.

## OUTAGES ACTION PLAN:

### How can you lower your risk?



#### 1. DISCOVER ALL CERTIFICATES

Look across your entire extended network, cloud and virtual instances, as well as CA implementations.



#### 2. CREATE A COMPLETE INVENTORY

Tracking and managing the status of all certificates makes it easier to rotate them before they expire.



#### 3. VERIFY SECURITY COMPLIANCE

Make sure that all certificates are governed by policies that ensure a regular cadence of renewals.



#### 4. CONTINUOUSLY MONITOR CERTIFICATES

Non-stop surveillance is the most efficient way to keep tabs on renewal requirements, as well as misuse.



#### 5. AUTOMATE RENEWALS

Automatically installing, configuring and validating certificates eliminates the risk of human error.

Worried about machine-identity-related outages? Venafi can help. Visit [venafi.com](http://venafi.com).

#### About the study

- Source: Study conducted by Vanson Bourne
- Respondents: 550 Chief Information Officers (CIOs) responsible for cryptographic assets across the USA, UK, Australia, France and Germany

<sup>1</sup><https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/>

<sup>2</sup>TechValidate, TVID: 997-36B-8D1

<sup>3</sup>Securing The Enterprise With Machine Identity Protection, a June 2018 commissioned study conducted by Forrester Consulting on behalf of Venafi