MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THE RISE OF THE MACHINES

PROTECTING YOUR MACHINE IDENTIES

Tammy Moskites

Managing Director and Senior Security Executive - ACCENTURE

TAMMY MOSKITES

Managing Director, Senior Security Executive @ Accenture Security

- Over 30 years of IT/security experience
- Distinguished Fellow, Ponemon Institute
- Certified Information Security Manager (CISM)
- ITIL-F Certification
- ISACA Cybersecurity Taskforce Member
- MIS|TI InfoSec World Conference Advisor
- Attivo Networks Company Advisor
- Venafi Company Advisor
- CISO Magazine Editorial Advisor
- ISE North American Peoples Choice Winner x2
- Speaker, Author, Entrepreneur
- TWITTER - @QueenofCandor

InfoSecWorld Conference & Expo 2018

The Future: Machines

MACHINE IDENTITIES

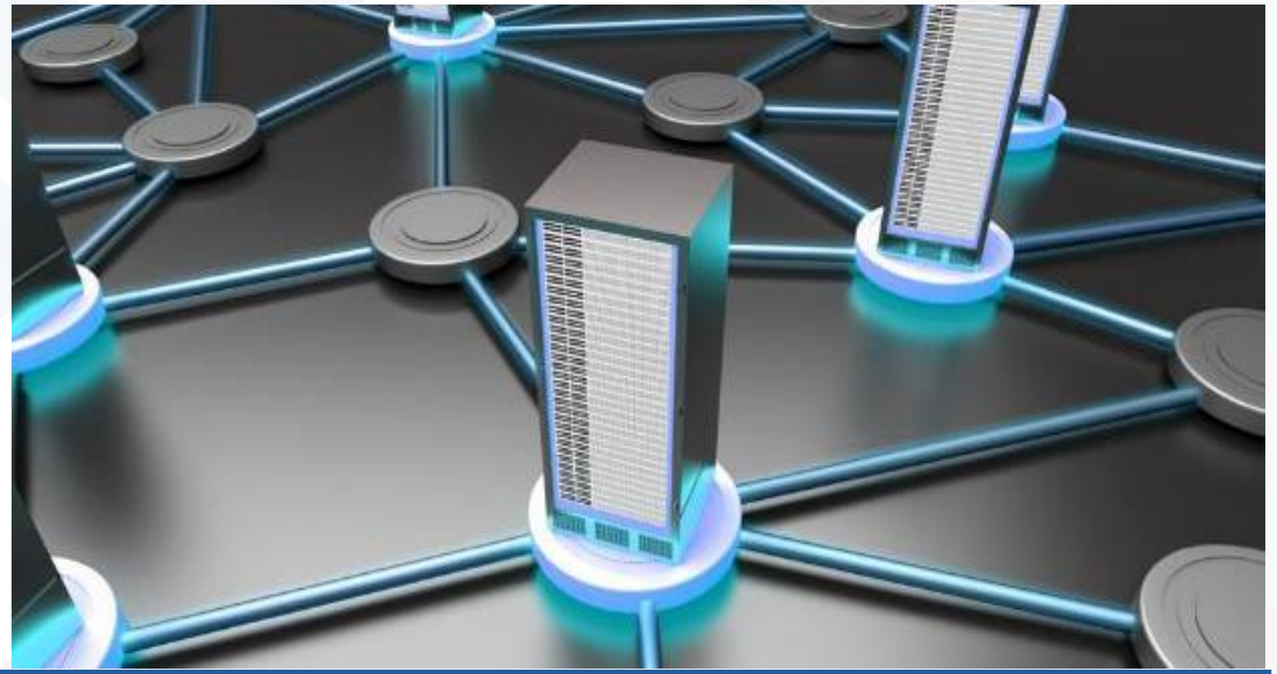
Ask yourself if you're protecting all your machine identities.

And if you're not protecting all of them, we'll discuss what you can do about it and why.

TWO ACTORS ON A NETWORK: IDENTITY and ACCESS

People
Usernames & Passwords

Machines
Keys and Certificates



Secure and Protect Identities – People and Machines

$7 BILLION ANNUALLY ON IDENTITY AND ACCESS MANAGEMENT

We spend billions protecting user names and passwords.

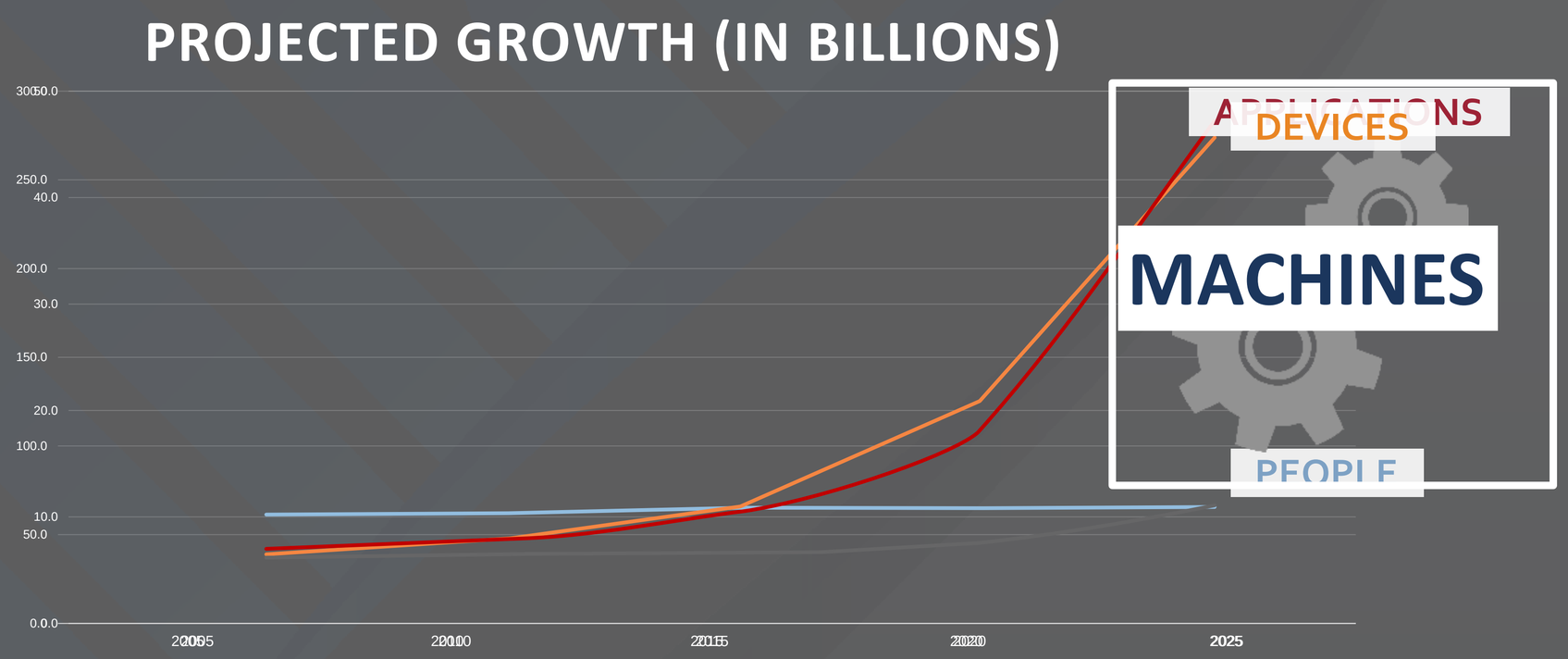
But almost nothing protecting machine identities which secure our critical systems and data.

Source: MarketsandMarkets.com. Identity and Access Management Market by Component, by Organization Size, by Deployment, by Vertical, and by Region - Global Forecast to 2020. March 2016.

THE NETWORK IS GROWING EXPONENTIALLY

Growth Factors

- Cloud
- Virtual Machines
- Containerization
- DevOps
- Mobile Devices
- Internet of Things
- Industrial IoT
- Data Access
- Privacy Laws



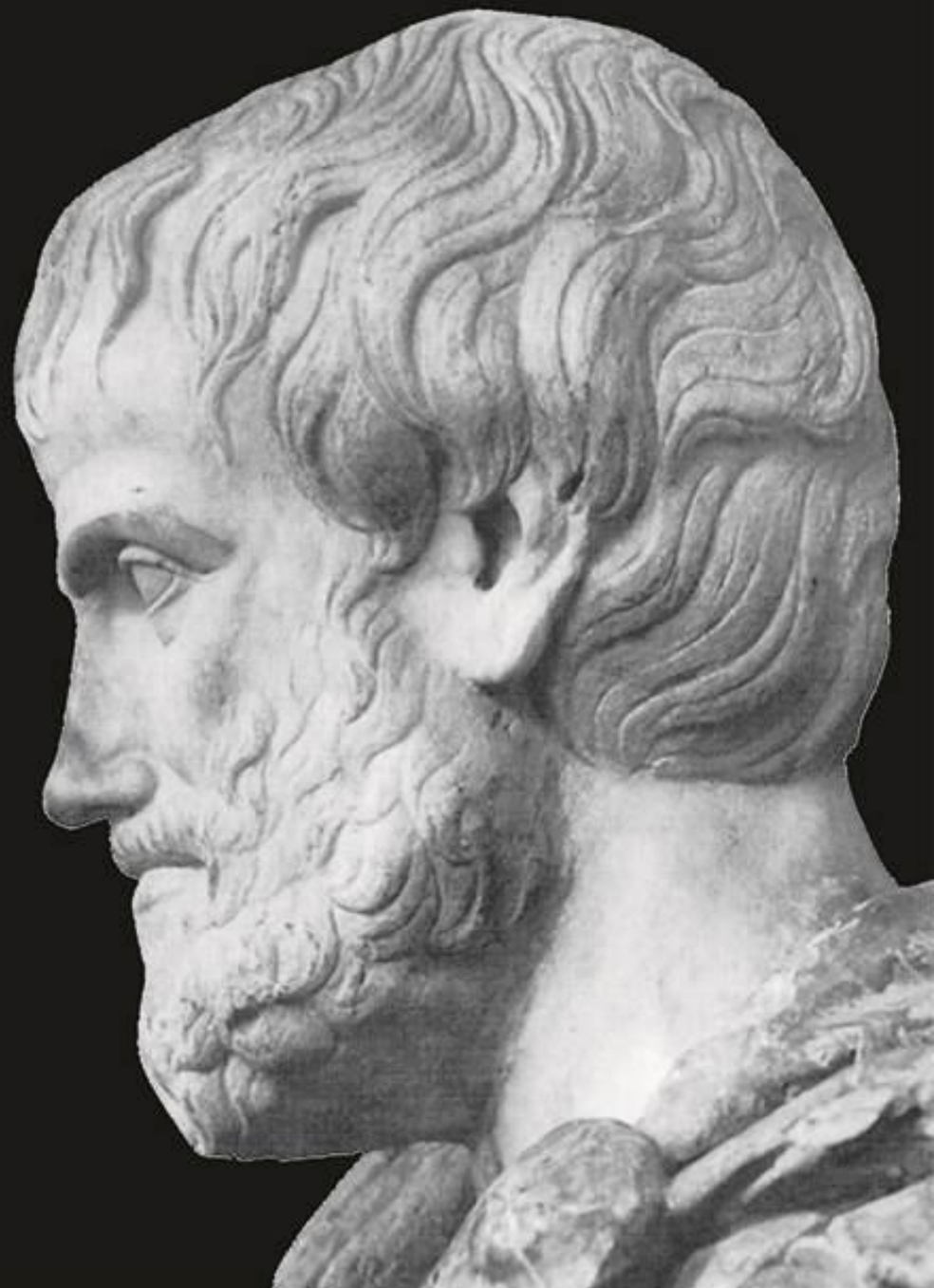
Gartner estimates that >20 billion IoT devices will be in use by 2020!

An entity without an identity cannot exist because it would be nothing

Aristotle

Law of Identity

Metaphysics, Book IV, Part 4



WHAT ESTABLISHES MACHINE IDENTITIES?

SSL/TLS Certificates

SSH Keys

Code-signing Certificates

Mobile & IoT Certificates

Key and Certificate Types = Machine Identities

Machine Identities

MACHINE IDENTITIES ARE EVERYWHERE
A DAY IN THE LIFE…

Mobile Phone Apps

Car Systems

WiFi and VPN Access

Encrypted Email

Remote Sysadmin Access

Industrial IoT

Medical Records & Devices

Online Banking & Shopping

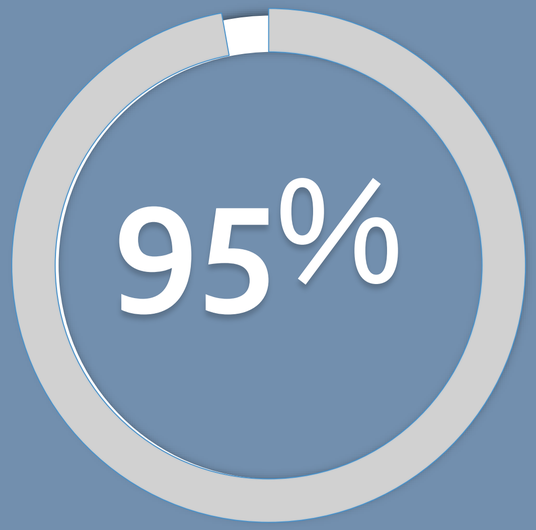
Travel

Home Internet of Things

And so much more…

InfoSecWorld Conference & Expo 2018


T50
127.116.27.251
E5847
T-44
T84
T14
T53
T18
172.229.99.114
125.201.98.217
174.229.37.129
290.116.74.182



…of organizations don't know where machine identities are active in their networks[1]

Global 5000 companies have **1,000s of SSL/TLS certificates** and keys on average[2]…

With a 25% annual growth rate[3]

Many organizations have **millions of SSH keys**[1]

1. Venafi Professional Services. 2017.
2. Ponemon Institute. 2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point. 2015.
3. Dimensional Research. Survey on Growth of Cryptographic Keys and Digital Certificates. 2017.

Would your organization tolerate **any user ID and password** with

- No awareness
- No policies
- No control

Would your organization tolerate **any key and certificate** with

- No awareness
- No policies
- No control

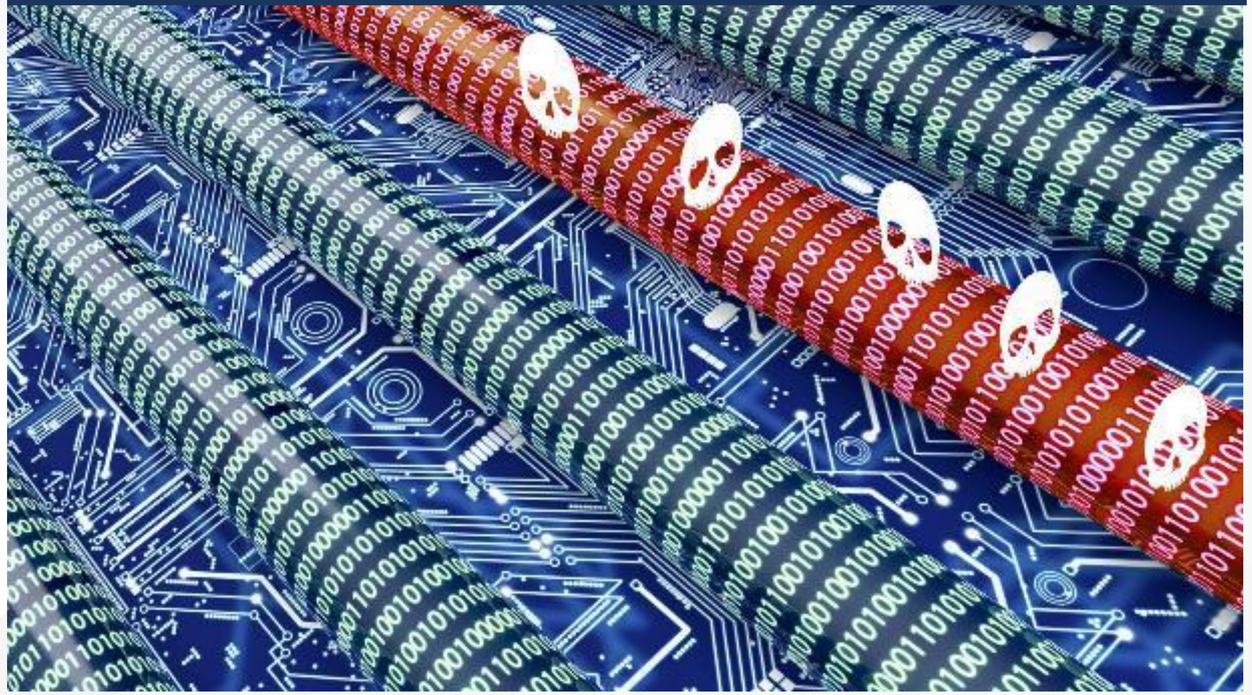
CRIMINALS PRAY ON UNMANAGED/UNPROTECTED KEYS AND CERTIFICATES

Hijack access to tunnels

Eavesdrop via man-in-the-middle attacks

Make their own malicious tunnels

Hide in encrypted traffic to get malware in and sensitive data out



DOESN'T KEEP UP WITH

- *THE VOLUME OF MACHINE IDENTITIES*
- *THE SPEED OF BUSINESS*

Methods of Certificate Management

Machine Identity Protection Requires Automation

RISKS OF INACTION

- **Code-signed malware** bypasses security controls
- **Man-in-the-middle attacks** are enabled by misused certificates
- **Compromised CA's** threaten trusted status
- **SSH keys** leave with terminated employees
- **Spoofed websites** use stolen or forged SSL/TLS keys & certificates
- **Outages** resulting from expired certificates


"70% OF MALWARE ATTACKS WILL USE SSL BY 2020"
Gartner
InfoSecWorld
Conference & Expo 2018

Common Challenges for Machine Identities

Certificate-related Outages

PKI Updates & Certificate-as-a-Service

Key and Certificate Audit Findings

Unprotected DevOps IT Services

Unmanaged SSH Keys

How Are We Doing?

VENAFI

Research by TechValidate

16,500 Unknown Keys & Certificates Found

On average, IT security professionals found 16,543 additional keys and certificates using Venafi that were previously unknown.

Source: TechValidate survey of 47 Venafi users

Published: **Oct. 14, 2015**

TVID: **363-53E-598**

SOFTPEDIA®

WINDOWS DRIVERS GAMES MAC ANDROID

Softpedia > News > Security

Let's Encrypt Hands Out 15,000 Fraudulent Security Certificates to Phishers

In the span of a year, Let's Encrypt managed to make people across the Internet feel safe on phishing sites

Mar 27, 2017 22:23 GMT · By Gabriela Vatu · Share:

Let's Encrypt, a free and open Certificate Authority, has issued close to 15,000 certificates containing the term "PayPal" for phishing sites.

The discovery was made by encryption expert Vincent Lynch, who says 96.7% of the 15,270 security certificates featuring the term "PayPal" issued by Let's Encrypt in the past year have been for phishing sites. The highest density of certificates was issued starting in November 2016, data shows.

COMPUTERWORLD
FROM IDG

NEWS

Microsoft's Azure service hit by expired SSL certificate

The company also reported service problems with Xbox Music and Video Store services

By John Ribeiro

Louis Motorrad | Bekleic

louis.de

Website identification

GeoTrust Global CA has identified this site as

www.louis.de

Your connection to the server is encrypted.

Should I trust this site?

Bestelltelefon: 040 - 734 193 60

2 J

torrad & Freizeit

Mein Bike

Sale % Markenshops Service

S

» Zu d

Top-Marken bei Louis

cardo SHOEI TOMTOM rukka

Louis Motorrad | Bekleic

louis.fail

Kostenloser Rückversand

Bestelltelefon: 040 - 734 193 60

2 J

FUN COMPANY Louis

Europas Nr.1 für Motorrad & Freizeit

Suchbegriff

Mein Bike

Bekleidung & Helme Technik & Freizeit Sale % Markenshops Service

Sie sind hier: Startseite

» Zu d

Top-Marken bei Louis

cardo SHOEI TOMTOM rukka

Louis Motorrad | Bekleic

louis.de

Kostenloser Rückversand

Bestelltelefon: 040 - 734 193 60

2 J

FUN COMPANY Louis www.louis.de

Europas Nr.1 für Motorrad & Freizeit

Suchbegriff

Mein Bike

Bekleidung & Helme | Technik & Freizeit | Sale % | Markenshops | Service

Sie sind hier: Startseite

Top-Marken bei Louis

cardo SHOEI TOMTOM rukka

Louis Motorrad | Bekleic

louis.fail

Website identification

DST Root CA X3 has identified this site as

louis.fail

Your connection to the server is encrypted.

Should I trust this site?

Bestelltelefon: 040 - 734 193 60

2 J

Europas Nr.1 für Motorrad & Freizeit

Mein Bike

Sale % | Markenshops | Service

Sie

Top-Marken bei Louis

cardo SHOEI TOMTOM rukka

Global Intelligence & Visibility

Extended Enterprise Discovery

Key Length, Signing Algo, etc.

Ownership

Weaknesses

Continuous Monitoring

Orchestration & Governance

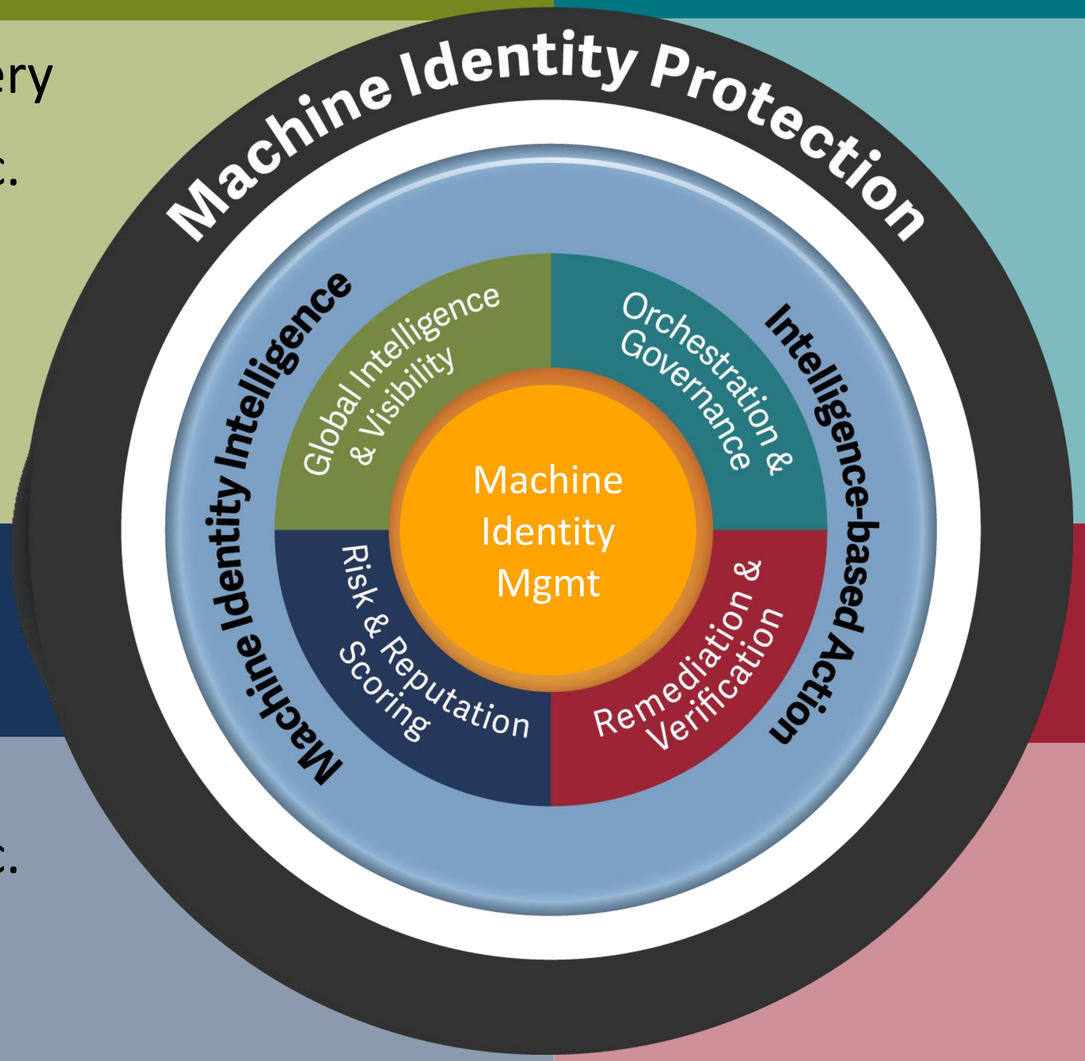
Lifecycle Orchestration

Policy Enforcement

Automated Workflows

Enterprise Access Policies

Certificate-as-a-Service



Risk & Reputation Scoring

Security Assessment:
Key Length, Signing Algo, etc.

Risk Analytics

Risk Prioritization

Continuous Reassessment

Remediation & Verification

Outage Prevention

Certificate Authority Agility

Automated Remediation

Validation Reports

Audit Readiness

TRADITIONAL VS. DEVOPS

Traditional IT

Multi-layer

Fixed infrastructure

Fixed number of keys &

Slow IT

1

Global

DevOps

>100,000

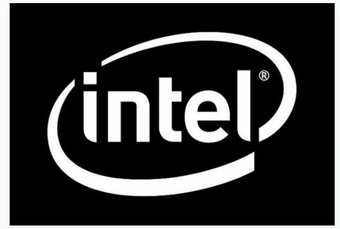
keys & certificates
and growing

If not fast and easy, developers will side step security and create new vulnerabilities

Threats of the Future

INTEL ® SAYS…

"Stealing Certificates will be the Next Big Market for Hackers"



BENEFITS OF MACHINE IDENTITY PROTECTION

Avoid Outages

Increase system availability

Improve Security

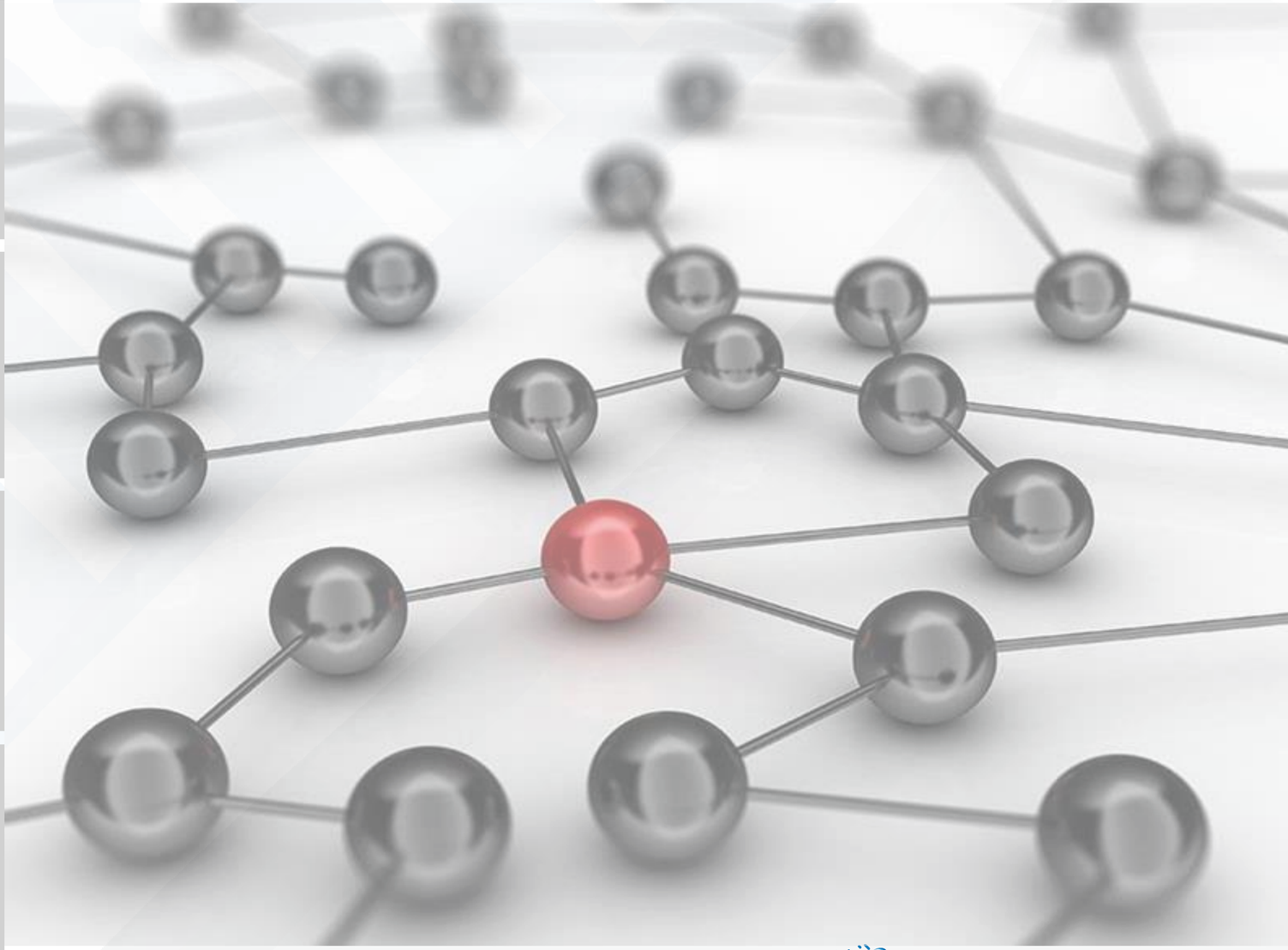
Shorten lifecycles
& enforce policies

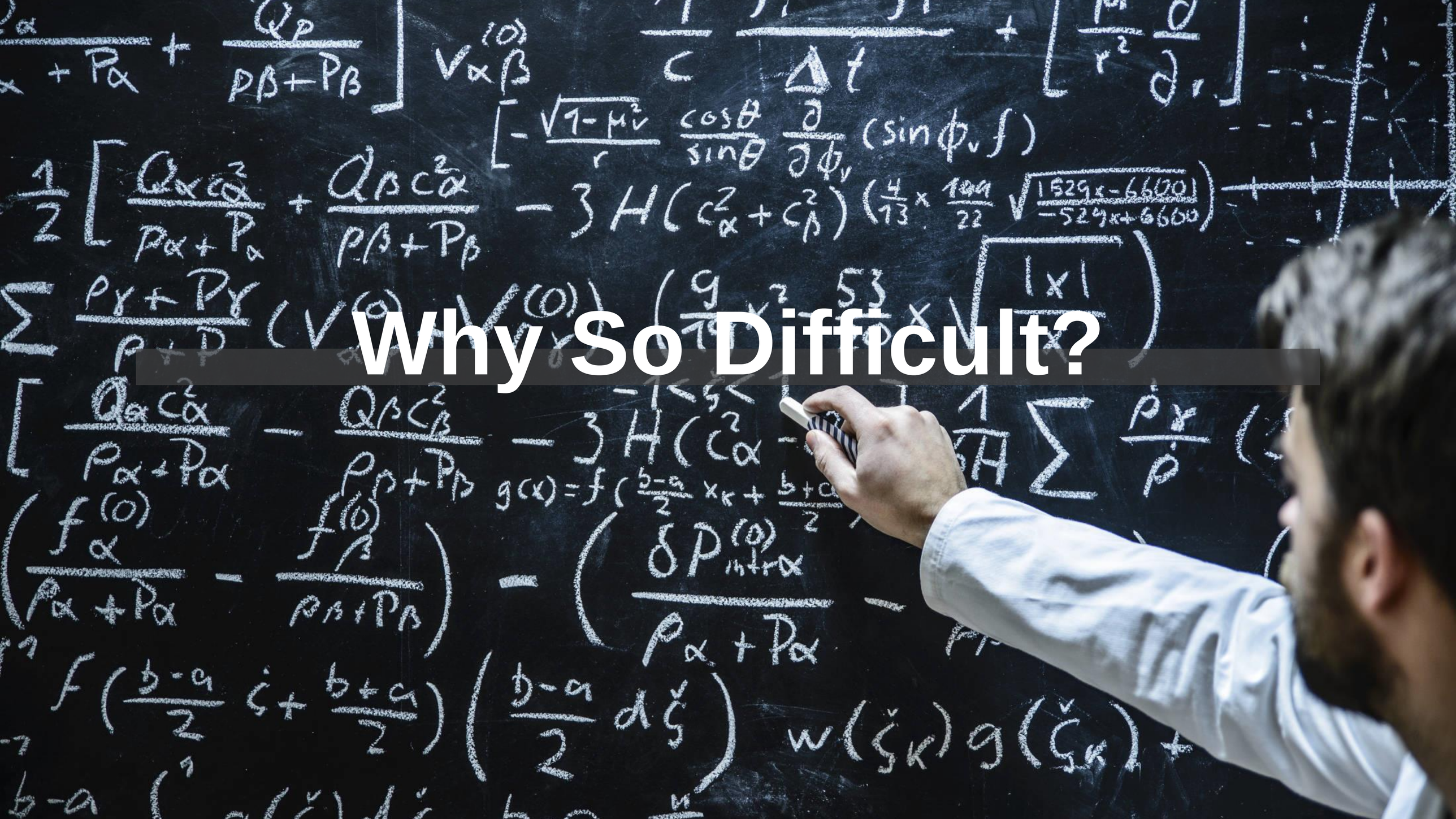
Strengthen Investments

Enable existing security controls

Achieve Compliance

Get visibility and
audit-ready reports




Why So Difficult?

THE POWER OF MACHINES

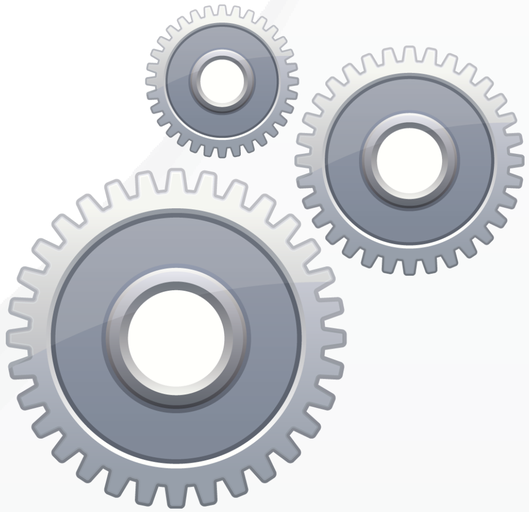
=

Efficiency, Productivity, Agility & Speed

Taking Action

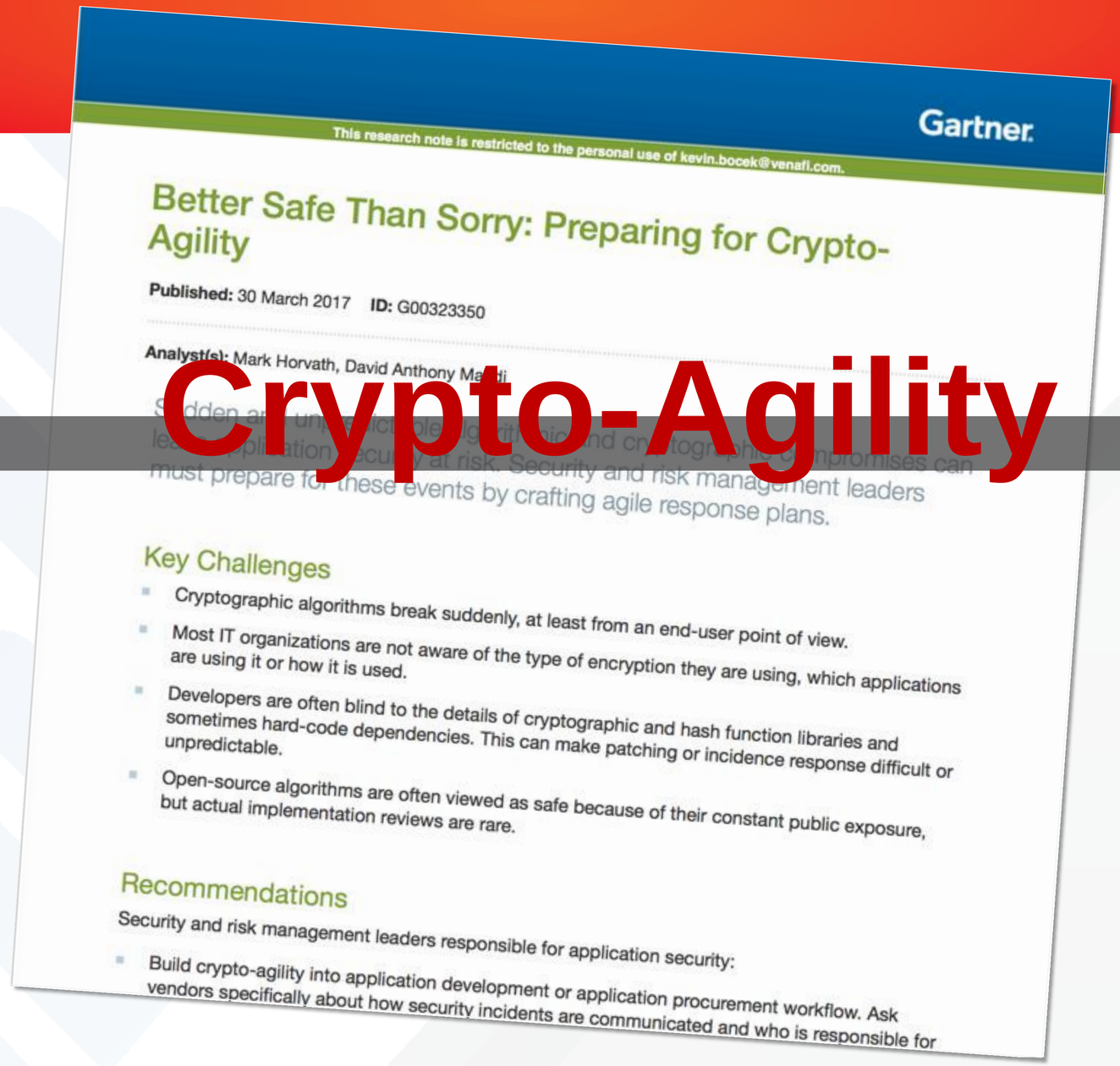
Find What's Out There

Set, Enforce a Policy



Automate

LEARN MORE



Gartner

Better Safe Than Sorry: Preparing for Crypto-Agility

Published: 30 March 2017 **ID:** G00323350

Analyst(s): Mark Horvath, David Anthony Ma[illegible]i

Sudden and unpredictable [illegible] and cryptographic compromises can leave application security at risk. Security and risk management leaders must prepare for these events by crafting agile response plans.

Key Challenges

- Cryptographic algorithms break suddenly, at least from an end-user point of view.
- Most IT organizations are not aware of the type of encryption they are using, which applications are using it or how it is used.
- Developers are often blind to the details of cryptographic and hash function libraries and sometimes hard-code dependencies. This can make patching or incidence response difficult or unpredictable.
- Open-source algorithms are often viewed as safe because of their constant public exposure, but actual implementation reviews are rare.

Recommendations

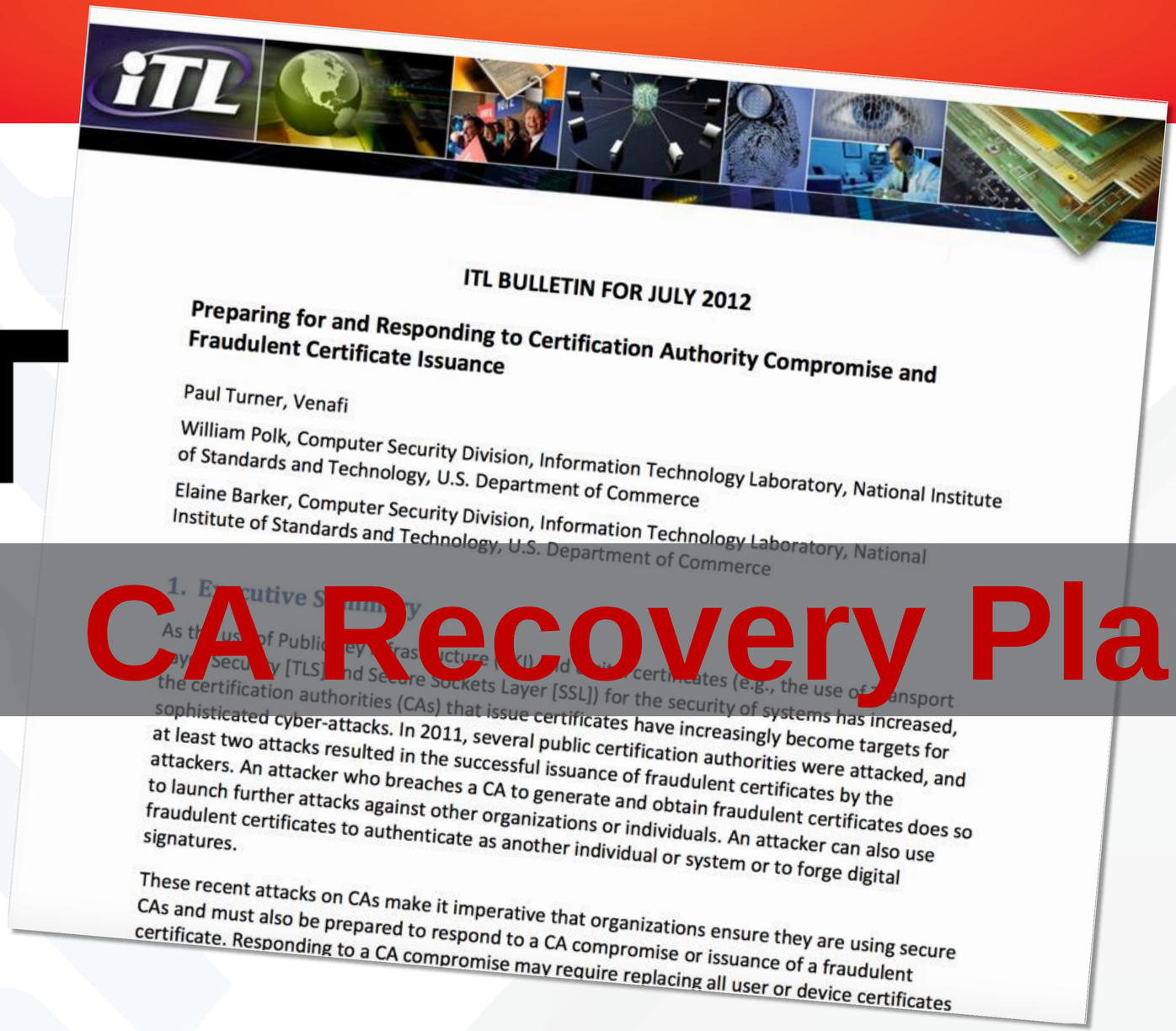
Security and risk management leaders responsible for application security:

- Build crypto-agility into application development or application procurement workflow. Ask vendors specifically about how security incidents are communicated and who is responsible for

Crypto-Agility

LEARN MORE

NIST



CA Recovery Plan

InfoSecWorld
Conference & Expo 2018

ROADMAP: CONTROL OF MACHINE IDENTITIES

Level 0:
Chaos
Have unquantified security risk, outages, expensive and manual processes, and compliance challenges

Level 1:
Control
Build a security foundation with focus on **known and trusted keys and certificates**

Level 2:
Critical Systems
Secure and protect all keys and certificates **on business-critical infrastructure**

Level 3:
Enterprise Protection
Protect and automate **all keys and certificates enterprise-wide** and further reduce costs and extract more business value

Level 4:
Machine Identity Protection
Rapidly respond to internal and external threats and security incidents related to keys and certificates

Endpoint/Mobile
Servers
Virtual Machines
Cloud

InfoSecWorld
Conference & Expo 2018

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

accenture

High performance. Delivered.

Tammy Moskites

Managing Director and Senior Security Executive – ACCENTURE

@QueenofCandor

Tammy.Moskites@Accenture.com