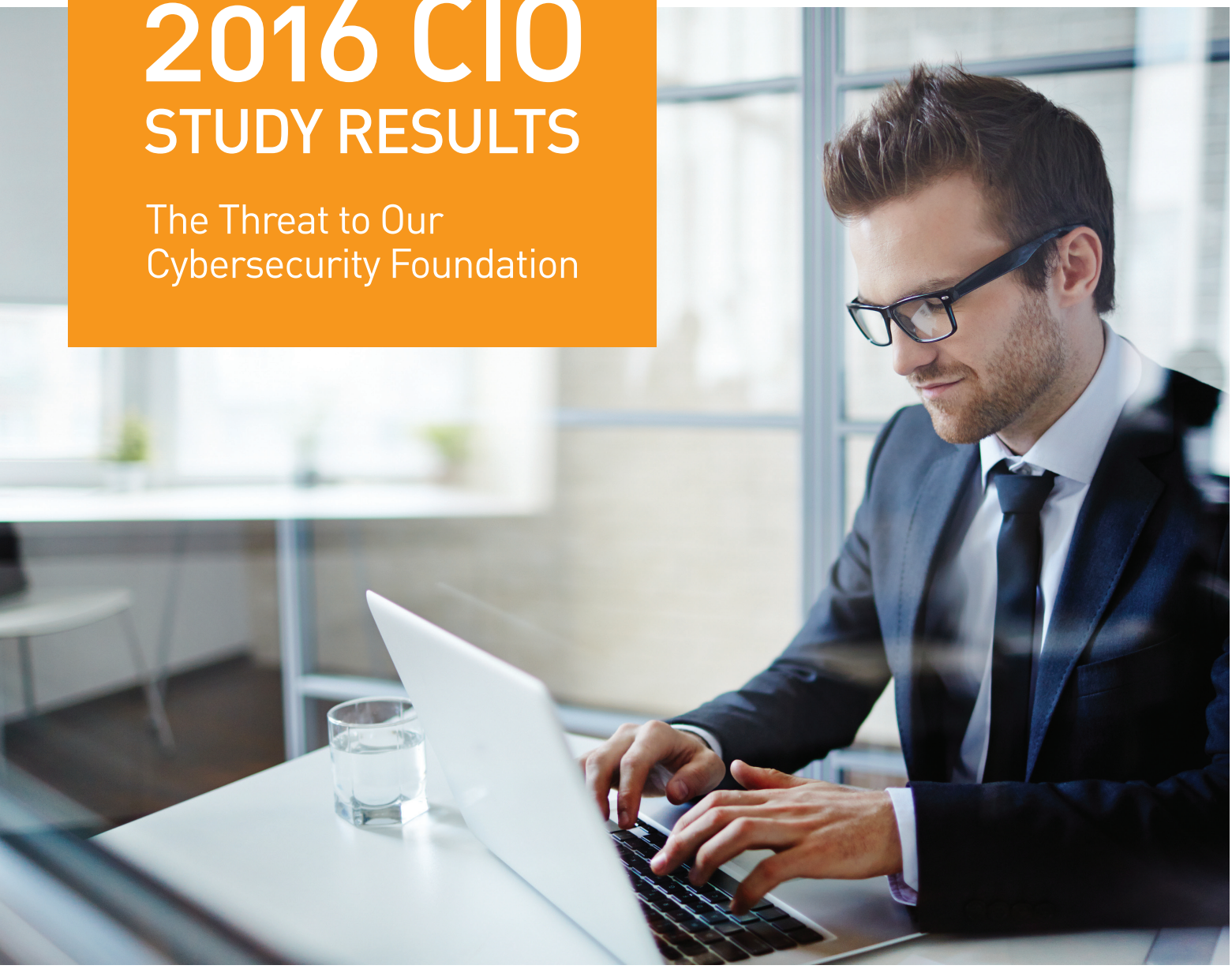
VansonBourne

2016 CIO STUDY RESULTS

The Threat to Our Cybersecurity Foundation



CIOs Admit to Wasting Millions on Cybersecurity that Doesn't Work on Half of Attacks

IT executives overwhelmingly agree that they have a fundamental flaw in their cybersecurity strategies. Research shows organizations are not protecting the technology that determines if software, devices, clouds, and applications are good or bad, friend or foe—cryptographic keys and digital certificates. This gap allows cybercriminals to use these unprotected keys and certificates in half of network attacks to hide their actions and bypass security controls.

Ultimately, this undermines costly security investments, which are expected to total $83 billion in 2016,[1] leaving the Global 5000 blind to these threats and unable to defend their businesses.

VENAFI®

www.venafi.com

CIOs Are Wasting Millions on Inadequate Security Tools

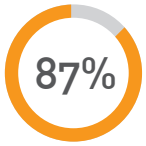
As organizations layer security controls to protect their business, 90% of CIOs admit to wasting millions on inadequate cybersecurity. Why? Keys and certificates—the foundation of cybersecurity that determines if software, devices, clouds, and applications are good or bad, friend or foe—are being left unmanaged and unprotected. The bad guys are taking advantage of this fatal flaw in enterprises' security foundation and using keys and certificates to hide their actions and circumvent security controls.

Organizations are implementing IT initiatives such as Fast IT, DevOps, and Encryption Everywhere strategies, which are responsible for exponential growth in the amount of software and an increase in encrypted traffic of nearly 100%. This is causing a dramatic rise in the sheer numbers of keys and certificates, up 34% between 2013 and 2015, with over 23,000 keys and certificates in today's average enterprise. And 54% of IT security professionals admit to not knowing where all of their keys and certificates are located, who owns them, or how they are used.[2] This is creating chaos and compounding risk exposure, jeopardizing the success of these strategic plans and exposing businesses to attacks.

IT executives understand their cybersecurity approaches are failing and agree they are wasting money on inadequate security controls.

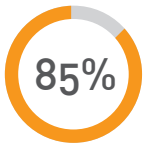
THE SITUATION: Our Cybersecurity Foundation Is Crumbling

A January 2016 survey conducted by Vanson Bourne, an independent technology market research provider, asked 500 enterprise CIOs in the U.S., U.K., France, and Germany how the demand for encryption and exponential growth in cryptographic keys and digital certificates are impacting their cybersecurity efforts. The results show IT executives understand their cybersecurity approaches are failing and agree they are wasting money on inadequate security controls.

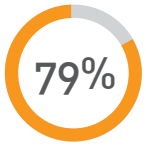


of CIOs believe their security controls are failing to protect their business
Even with layered defense, respondents believe their security controls are less effective because they cannot inspect for malicious activity or data exfiltration inside encrypted traffic.

of CIOs have already been attacked or expect to be by bad guys hiding in encryption
By using unprotected keys and certificates bad guys are able to use encrypted traffic to disguise their actions.



of CIOs expect criminal misuse of keys and certificates to get worse
Today's security controls are designed to blindly trust keys and certificates, and the vast majority of organizations have little to no awareness about or control over their keys and certificates. The result is attackers are increasingly using keys and certificates to hide in encrypted traffic and gain trusted status to access critical systems and data.



of CIOs expect the speed of DevOps to make it difficult to know what should be trusted
As DevOps quickly delivers new IT services, keys and certificates used to secure those services explode. But when developers, and not security professionals, are left to manage and secure these keys and certificates, the result is chaos that causes security blind spots and new vulnerabilities.

KEYS + CERTIFICATES = The Foundation of Cybersecurity

Keys and certificates are the basis of trust for websites, virtual machines, mobile devices, and cloud servers.

Blind Trust

Today's security controls blindly trust keys and certificates, not indicating which are good or bad, safe or unsafe.

$ WASTING MILLIONS

Enterprises are wasting millions on security as bad guy use keys and certificates to undermine network defenses.

WHAT'S HAPPENING: Security Controls Are Being Undermined

CIOs surveyed admit that their current defenses are inadequate. This is bad news for the defense-in-depth, layered security approach which is ubiquitous in today's global enterprises. Organizations are investing in endpoint protection, advanced threat protection, next generation firewalls, intrusion detection systems, data loss prevention, and many other security controls. Gartner estimates that information security spending will exceed $83 billion in 2016.[2] With these investments, enterprises expect their network security to know what is trusted and safe, and what isn't. But these security controls are blind to attacks that use compromised, stolen, or forged keys and certificates to undermine network defenses.

Keys and certificates represent the foundation of cybersecurity; enterprises rely on tens of thousands of keys and certificates as the basis of trust for their websites, virtual machines, mobile devices, and cloud servers. The technology was adopted to solve the original Internet security challenge of needing to know what could be trusted online and how to keep communications private. From online banking, secure communications, and mobile applications to the Internet of Things, today everything IP-based depends upon a key and certificate to create a trusted and secure connection.

But organizations do not understand how vital keys and certificates are to the foundation of cybersecurity. There is little to no awareness of where they exist and how they are used. This means they are left unsecured, only managed though manual methods or home grown solutions. The result is bad guys use unprotected keys and certificates to hide in encrypted traffic, spoof websites, deploy malware, and steal data.

Why do these attacks succeed? Today's security controls blindly trust keys and certificates, not indicating which are good or bad, safe or unsafe. And these controls are unable to inspect threats in encrypted traffic because the location of all keys and certificates is unknown or they can't be securely distributed for decryption and inspection. This lets cybercriminals use keys and certificates to gain trusted status with security controls. This fatal flaw in the enterprise security foundation devalues enterprise security investments and exposes the business to breach and compromise.

The results from the 2016 CIO cybersecurity research found that IT executives are waking up to the shortcomings of their security controls and the need to protect keys and certificates, especially as the demands for more encryption and faster IT services increase.

50%

of Networks Attacks
will use encrypted traffic by 2017.[3]

$1000

PER CERTIFICATE[5]

Most CIOs (86%) believe keys and certificates are the next big hacker marketplace.

3 out of 4 BUSINESS
will have added fast IT by 2017.[7]

THE THREAT: Growing Risk of Attack

The risk from attacks using keys and certificates is only growing. More cybercriminals are using encryption to hide their attacks. And as enterprises expand IT initiatives around Encryption Everywhere, DevOps, IoT, enterprise mobility, and other agile, fast IT strategies, the explosion of keys and certificates provides cybercriminals with more opportunity to compromise keys and certificates for use in their attacks.

More Attacks Using Keys and Certificates

Simply put, current threat detection strategies aren't working at least half of the time. By 2017, Gartner expects 50% of networks attack to come over encrypted traffic.[3] Cybercriminals are well aware that SSL/TLS encryption creates security blind spots and are using it to their advantage to hide attacks, evade detection, and bypass critical security controls. So it's not surprising that the CIO survey found that 9 out of 10 IT executives admit that they have experienced attacks misusing keys and certificates, or expect to soon.

Certificates: The Next Big Hacker Marketplace

When asked if they agreed that the next big market for hackers would be keys and certificates, 86% of CIOs said yes. Intel's Matthew Rosenquist echoes this CIO sentiment, agreeing that keys and certificates are the next big underground marketplace for hackers, because of their importance, lack of protection, and the ability for bad guys to collect them en masse and monetize them quickly.[4] Prices in this black market continue to rise—by the end of 2015, the cost of a certificate was $1000.[5] In addition, IBM Security's X-Force research team has found that large numbers of code-signing certificates are also now a hot commodity in the black market.[6]

Fast IT, DevOps, and Encryption Everywhere Initiatives Multiply Keys and Certificates

New IT initiatives are dramatically increasing the numbers of keys and certificates in enterprises. The speed of IT is changing with increased demands on the delivery of fast IT services within organizations. Gartner reports that by 2017, 75% of businesses will have strategic initiatives that cause IT to run in two separate groups: one that continues to support long-term, existing apps that require stability, and another that delivers fast IT and supports DevOps teams that are focused on innovation and business-impacting projects.[7]

79% of CIOs

Nearly 8 in 10 CIOs expect the speed of DevOps to make it more difficult to know what is trusted or not.

23,000

Today's average enterprise has more than 23,000 keys and certificates (up 34% since 2013).

54% Unaware

Businesses don't know the location, ownership, or use of all of their keys and certificates.

When asked if the speed of DevOps makes it more difficult to know what is trusted or not in their organizations, 79% of respondents said yes. Why? With DevOps, software grows exponentially. Applications, containers, and all types of software need keys and certificates to know what is trusted or not and establish secure communications. So as DevOps causes software to grow, keys and certificates also grow in orders of magnitude. However, with developers in charge, and not IT security professionals, key and certificate chaos ensues, creating new security blind spots and new vulnerabilities.

Unless key and certificate issuance and revocation are automated using secure systems, not just any framework or open source tool, DevOps becomes another point of risk—a conclusion 79% of CIOs now understand.

Similarly, Encryption Everywhere strategies, driven in large part by Edward Snowden's revelations and breach of the NSA,[8] are increasing the number of keys and certificates. In light of Encryption Everywhere plans, 95% of CIO respondents indicated that they are worried about how they will securely manage and protect all encryption keys and certificates. Ironically, this effort to secure communications by encrypting all traffic is also creating more opportunities for cybercriminals to misuse keys and certificates in their attacks.

Leaving Keys and Certificates Unprotected Results in their Misuse

As the number of keys and certificates in an organization increase, so does the risk of their misuse—but only if keys and certificates are left unprotected. A 2015 study by the Ponemon Institute reveals that the average enterprise has more than 23,000 keys and certificates (up 34% since 2013), and 54% of IT security professionals admit to not knowing where all of their keys and certificates are located, who owns them, or how they are used.[1]

One result from a lack of visibility into all keys and certificates is enterprises cannot conduct SSL/TLS inspection to eliminate encryption blind spots. Next generation firewalls, sandboxing, authentication, behavioral analytics, and other security controls can't look inside encrypted traffic for threats if they don't have access to all of the enterprise's keys and certificates. This allows cybercriminals to keep their actions cloaked and bypass security controls. This lack of visibility also prevents the detection of key and certificate misuse—enterprises can't know which keys and certificates should be trusted and which shouldn't, leaving enterprises vulnerable.

Cybersecurity IS FAILING

Because the foundation—**keys and certificates**—is unprotected.

90% **of CIOs**

admit to WASTING MILLIONS on inadequate cybersecurity

DROP IN STOCKS

The HACK cybersecurity ETF has dropped by 25% since November 2015.

THE FINANCIAL IMPACT: Failing Security Investments Cost Millions

These survey results show overwhelming consensus that IT executives understand that cybersecurity is failing and agree they are wasting money because the foundation of their cybersecurity—keys and certificates—is unprotected.

The security controls built on this foundation are being bypassed by cybercriminals who misuse keys and certificates to cloak their actions—slipping right through in encrypted traffic. Is it a coincidence that 90% of CIOs admit to wasting millions on inadequate cybersecurity at the same time the HACK cybersecurity ETF drops by 25% since November 2015—well ahead of the overall market downturn (a 10% decline in the S&P500 index during the same period)? Not likely. Both show a lack of confidence in cybersecurity solutions.

Wall Street has taken note of this slump in cybersecurity stocks. Of the 34 cybersecurity companies in the PureFunds ISE Cyber Security ETF (NYSE: HACK), 33 have had their stocks fall in 2016. Advanced threat protection providers like FireEye are off even more.[9]

THE SOLUTION: Restoring the Foundation of Trust

Enterprises rely on tens of thousands of keys and certificates as the foundation of trust for their websites, virtual machines, software, mobile devices, containers, and cloud servers. Used properly, they ensure trust in digital communications and connections. Yet it is this very trust that cybercriminals want to exploit, not only to evade detection, but to achieve authentication and trusted status that bypasses other security controls and allows their actions to remain hidden.

If only one critical key or certificate is compromised, an organization's digital trust is eliminated. Without trust, organizations can't operate.

- The good can't be differentiated from the malicious
- Security systems are blind to attacks
- Critical security controls are undermined
- Blind spots open doors to compromise

When trust is lost, companies lose customers and the brand and business are damaged, creating a huge problem for CEOs, their boards, and Wall Street.

IMMUNE SYSTEM FOR THE INTERNET

Protects keys and certificates

- Know instantly which ones can be trusted
- Secure those on datacenters, desktops, mobile and IoT devices, and in the cloud
- Automate the issuance and renewal process
- Make their security easy, automated, and fast

HOW YOUR BUSINESS BENEFITS

- Stop certificate-based outages
- Migrate to SHA-2
- Inspect SSL traffic
- Deliver security for fast IT—cloud, DevOps, and IoT
- Maximize your security investments
- Protect your customers, business, data, and brand

But enterprises can eliminate these security blind spots and know what is good or bad, trusted or untrusted. They can safely expand the use of encryption and keys and certificates while maintaining online trust. How can this be accomplished? Organizations need ongoing protection, an immune system for the internet, that, like a human immune system, lets them know instantly which keys and certificates should be trusted and which shouldn't, making security easy, automated, and fast.

Keys and certificates must be secured and protected in the datacenter, on desktops, on mobile and IoT devices, and in the cloud. The entire issuance and renewal process should be automated with policy enforcement and workflows, enabling new encryption-dependent applications to be scaled quickly. This approach to key and certificate protection supports fast IT while improving enterprise security posture with increased visibility, threat intelligence, policy enforcement, and faster incident response for certificate-related outages and compromises leveraging misused keys and certificates.

With continuous monitoring for misuse, an immune system for the internet establishes which keys and certificates are "self" and trusted, and which are not and potentially dangerous, enabling enterprises to investigate, remediate, and return to a trusted state.

What would an immune system for the internet mean to businesses?

It means having a reliable, adaptive solution that is ever-vigilant and constantly watching. Whether stopping certificate-based outages, migrating to SHA-2, inspecting SSL traffic, or delivering fast security for cloud, DevOps, and IoT, this immune system for the internet provides visibility and control of keys and certificates that eliminates security blind spots. This would restore the true value of keys and certificates; once again allowing them to be the solid cybersecurity foundation that strengthens all the security controls built on that foundation. Organizations could then maximize their security investments, protecting their customers, business, data, and brand.

Learn more about how Venafi can help your company protect its security foundation.

Visit www.venafi.com

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

About Venafi

Venafi is the Immune System for the Internet™ that protects the foundation of all cybersecurity—keys and certificates—so they can't be misused by bad guys in attacks. Venafi does this by constantly assessing which keys and certificates are trusted, protecting those that should be trusted, and fixing or blocking those that are not.

RESOURCES

[1] Gartner, Inc. *Forecast Analysis: Information Security, Worldwide, 3Q15 Update.* January 16, 2016 (G00296286).

[2] Ponemon Institute. *2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point.* 2015.

[3] Gartner, Inc. *Security Leaders Must Address Threats from Rising SSL Traffic,* December 9, 2013 (G00258176).

[4] Rosenquist, Matthew. Intel IT Expert Blog. *Stealing Certificates to Sign Malware will be the Next Big Market for Hackers.* December 23, 2014.

[5] Koyfman, Tanya. Sensecy Blog. *Malware is Coming to the Trusted Software Near to You—Trade in Code Signing Certificates is on the Rise on the Russian Underground.* October 13, 2014.

[6] Kessem, Limor. IBM Security Intelligence Article. *Certificates-as-a-Service? Code Signing Certs Become Popular Cybercrime Commodity.* September 9, 2015.

[7] Gartner, Inc. Press Release. *Gartner Says CIOs Need Bimodal IT to Succeed in Digital Business.* November 10, 2014.

[8] Bocek, Kevin. Venafi Blog. *Venafi Analysis of Snowden NSA Breach Confirmed—2 Years Later.* January 14, 2016.

[9] Bloomberg News. *Cybersecurity Stocks Slump Into New Year.* February 4, 2016.

APPENDIX:
Survey Demographics

A Global Problem

This 2016 CIO cybersecurity study is based on a January 2016 survey conducted by Vanson Bourne with 500 CIO respondents:

- 200 in the U.S.
- 100 in the U.K.
- 100 in France
- 100 in Germany

The vast majority of IT executives across all regions showed an awareness and understanding of the danger of unprotected keys and certificates.

Larger Enterprises Suffer Bigger Risk

Large enterprises with over 3,000 employees are more likely to be impacted by security blind spots created by unprotected keys and certificates:

- More likely to have suffered an attack that misused keys and certificates
- More likely to believe their security controls are less effective because they cannot detect threats in encrypted traffic

Industry Results: Retail versus Financial Services

Retail responses were consistently lower than the survey average across almost all questions:

- Suffered fewer attacks (and have a lower expectation of future attacks)
- Have fewer concerns about the effectiveness of their security controls
- Have fewer concerns about the increased use of encryption to hide attacks

The one area retail respondents express more worry was in the need for increased key and certificate management and security as enterprises embrace Encryption Everywhere projects.

Financial Services responses were above average on most questions:

- Suffered more attacks that misuse keys and certificates (7% greater than the next industry)
- Worry more about the added key and certificate management and security required by Encryption Everywhere projects (9% above the average)

Regardless of these differences across demographics, all respondent groups revealed a definitive consensus that cybersecurity is failing and businesses are wasting money on layered cybersecurity defenses because the foundation of cybersecurity—keys and certificates—is unprotected.

©2016 Venafi, Inc. All rights reserved. Venafi and the Venafi logo are trademarks of Venafi, Inc.