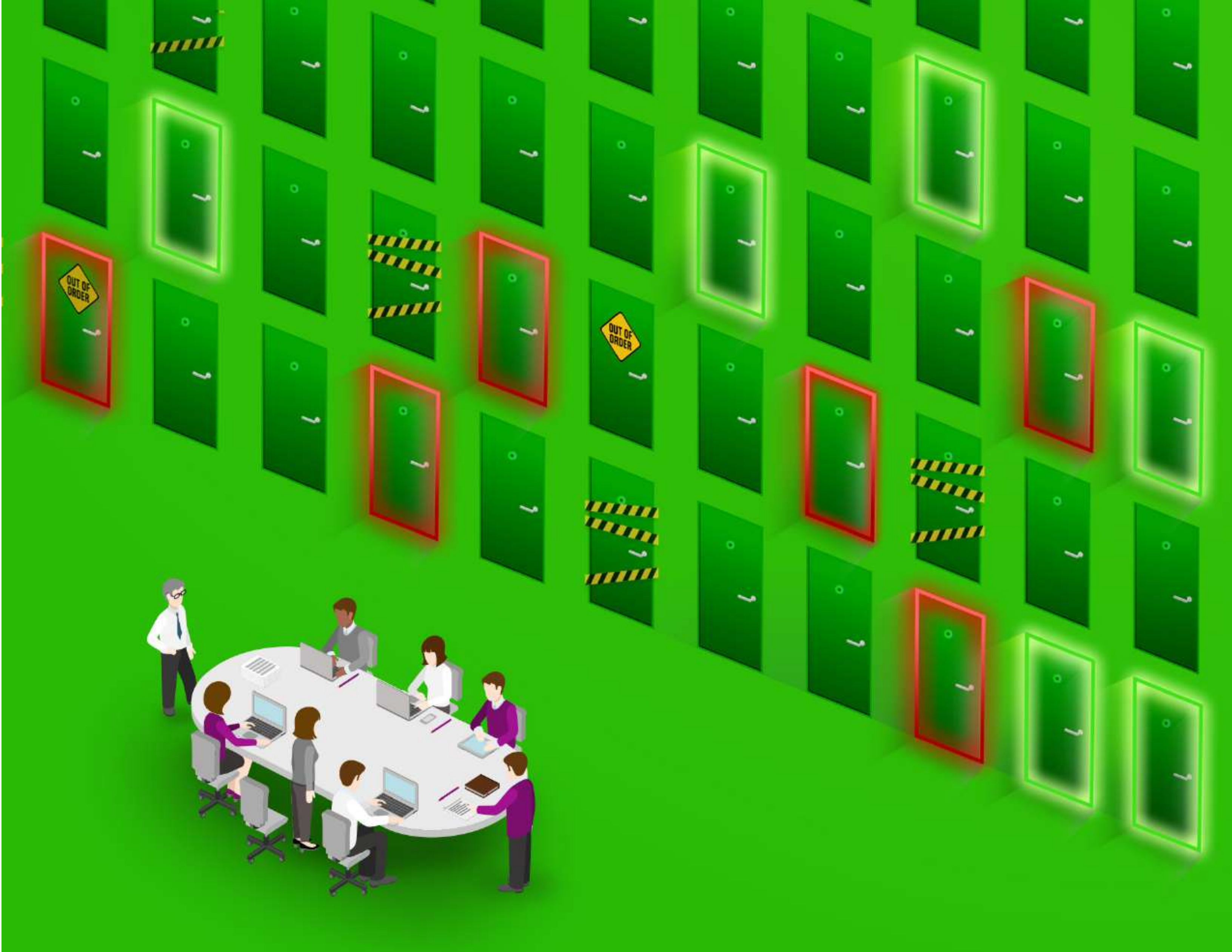


KEYFACTOR

The Critical Trust Gap

How a series of bad compromises is putting companies' systems and data at risk

The model for enterprise security is changing - and fast.

As more organizations shift operations to the cloud, sensitive information is no longer contained behind network firewalls. It flows between the core IT system and business applications, both on-premises and in the cloud. From there, it's shared across hundreds or thousands of mobile and endpoint devices owned by employees, partners, vendors and customers. Increasingly, data is also making its way into the more than 75 billion IoT devices that will be in use by 2025.

Cloud computing delivers the easy-to-scale, convenient access that today's employees and customers demand, but it also changes the security paradigm. While firewalls are still essential, keeping critical data and applications safe is no longer just a matter of protecting the network perimeter. In a multi-cloud environment, every user, device, access point, server, container and piece of network equipment — internal and external — must be protected for companies to avoid exposure. It takes just one weak link to cause a breach. And the likelihood of experiencing one in the next two years has risen to 29.6%.

Breaches have become a greater threat because many organizations haven't aligned their security practices with today's multi-cloud reality. A security policy created for a traditional on-site data center doesn't always work when data is transferred to the cloud. Migrating apps and data to the cloud without modernizing security procedures often leaves your organization less safe than it was before. Digital certificates and cryptographic keys can help, but only if they're properly managed.

Achieving security in today's environment requires adopting a new paradigm —one that ensures you can secure, encrypt and control access to your data at all times. Most organizations don't really know whether their data and critical systems are safe. This is a **Critical Trust Gap** — the root cause of the growing exposure epidemic and its costly effects. Companies that don't address the gap leave themselves exposed to costly certificate-related outages, security exploits, audit failures, and other risks related to the increasing pace of change in cryptography and security.

Confidence of 603 IT and security practitioners and executives in the ability of PKI to support new initiatives such as Cloud First, DevOps, Zero Trust:

5.05/10

Identifying your Critical Trust Gap

Many companies learn that they have a Critical Trust Gap after they are unable to prove compliance with IT policies and industry mandates. Others find out only after experiencing a disruptive network outage or a breach.

Not all outages are the result of IT mishaps. A surprisingly frequent cause is expired or improper security certificates. In the 2020 Keyfactor-Ponemon Report, "The Impact of Unsecured Digital Identities," 73% of IT and security leaders said their digital certificates have caused unexpected downtime and outages in the past, and continue to do so. Over half reported experiencing four or more certificate-related outages in the past two years.

If your organization has experienced a certificate-related outage, you have a Critical Trust Gap. You also have a Critical Trust Gap if you cannot state with certainty that you know the location of every certificate and key you own — and that each one is up-to-date with current security standards.

Nearly every enterprise relies on public key infrastructure (PKI) and digital certificates to enable encryption, authentication and authorization across their business. PKI forms the backbone of internet security by protecting information and providing secure access for users, devices, and applications across connections and networks. Mismanaging digital certificates can cause serious consequences.

Outages are just one potential outcome. Another is theft or misuse of certificates and keys, which enables hackers to distribute malware that looks like it came from a trusted source: your company. In the same Ponemon-Keyfactor report, 90% of respondents said their organization has fallen victim to at least one incident involving the misuse or theft of code signing keys in only the past two years.

Worse still, cybercriminals may hack certificate authorities — the bodies that issue your digital certificates. Unless you take swift action to revoke these certificates, the attacker can alter them and set up a fake website impersonating your own. They can then use that fake site to scam customers out of personal information, credit card numbers and money.

How your Critical Trust Gap is Created

The Critical Trust Gap manifests itself in two ways: problems with digital certificate management and a lack of cryptography expertise.

The Management Challenge

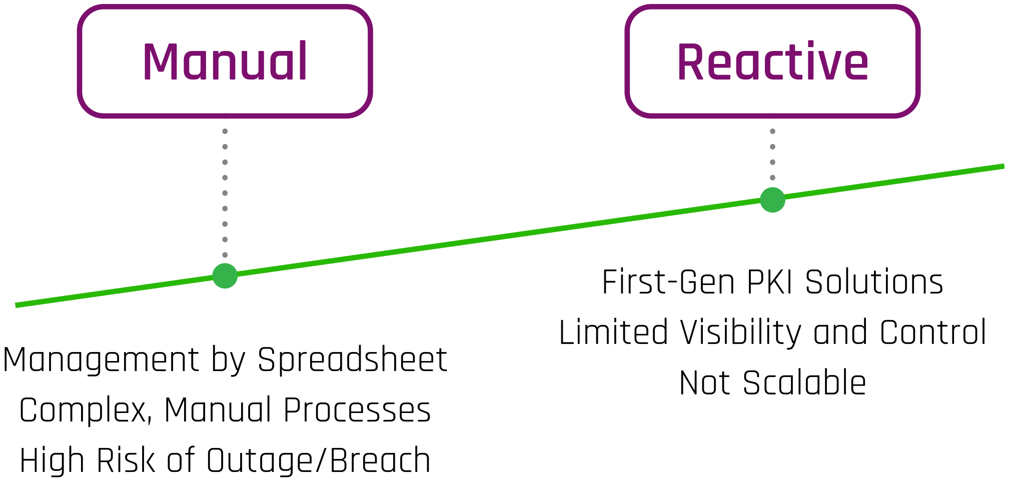
Many IT and security leaders feel helpless in the face of certificate-related security challenges. Over 75% of respondents in the Ponemon-Keyfactor report said that failure to secure keys and certificates is undermining the trust their organization relies upon to operate. Yet these companies continue to be plagued by theft, misuse and outages. Additionally:

- **Three out of four** respondents said they don't know how many keys and certificates their organization has or where they are; and
- **Fewer than half** are confident that they can scale PKI well enough to protect future in-house, cloud-based and IoT applications.

Safeguarding keys and certificates is critical to security, but it's not easy when companies have an average of 88,750 to manage, according to the report.

Companies manage their certificates with varying degrees of maturity and automation. Many still take a manual approach, using a spreadsheet-based approach to keep track of certificates to guide the process (See Figure 1 below.) This approach is not only resource-intensive and prone to human error, it also limits their scope to only known certificates, potentially leaving thousands of certificates unmanaged and unprotected.

Manual and Reactive Approaches to Managing Cryptography


Manual
Reactive
Management by Spreadsheet
Complex, Manual Processes
High Risk of Outage/Breach
First-Gen PKI Solutions
Limited Visibility and Control
Not Scalable

Other companies take a reactive approach, using a patchwork of CA-provided tools, internal PKI, and homegrown or first-generation solutions, which fail to provide complete visibility and consistent policy enforcement. Security teams also need to worry about developers and operations teams using unauthorized CAs or ignoring policies.

Another problem is scattered management of digital certificates, which is the norm today. Five or six teams outside the purview of security operations manage keys and certificates for various apps and business units. Their priority is to do this with as little effort as possible, so employees can return quickly to their regular job responsibilities. Unfortunately, such a mindset encourages people to cut corners. And that is never a good idea where security is concerned.

Safeguarding keys and certificates is critical to security, but itÕs not easy when companies have an average of

88,750

to manage

Common issues with manually managing keys and certificates

Extended certificate lifetimes

Instead of following company policy to set certificate lifetimes at one year, teams may generate 10-year, 15-year or even 99-year certificates. This set-and-forget model doesn't work with certificates because the cryptography algorithms they depend on must change frequently to remain one step ahead of cybercriminals.

Manipulating certificate lifetimes is like changing the expiration date on a bottle of milk. It may *look* safe, but anyone who tastes it knows immediately that it isn't. Especially cyberattackers.

Missed expiration dates

Companies must maintain constant vigilance of certificate expirations, but with so many other things to do, their internal teams often lose track. Your regular corporate activities, as well as passing time, may cause expiration. For example, if a merger or acquisition leads to a corporate name change, every certificate will immediately expire if it isn't swapped out.

When a certificate expires, the application or service it's attached to abruptly stops working. Downtime and lost productivity ensue as IT frantically works to solve the problem. Because IT and security teams may have no visibility into your organization's certificates and no means of knowing whether they are safe or up-to-date, resolving the issue can take many hours or even days.

Decentralized PKI

This practice is becoming more of a problem as organizations turn to a zero-trust framework to manage security in the cloud. A zero-trust system does what it sounds like — it trusts no user, application, server, IT process or device until strict identification and authentication procedures are followed.

But zero trust only works when digital identities are managed from a central location. PKI, the lynchpin of security, cannot be included in a zero-trust framework when management is distributed among business units.

Clearly, scattered PKI management does not align with modern security best practices. With no visibility into certificate security, organizations are blindsided by the problems that inevitably occur. And with no central authority in charge of PKI, no one has accountability.

According to the Ponemon-Keyfactor Report, 61% of respondents are unable to drive enterprise-wide PKI best practices.

Emailed keys and certificates

Teams that do follow security standards must still manage hundreds or thousands of devices and applications when it's time for certificate renewal. The process requires logging on to each device or app separately to securely replace its certificate.

To save time, employees may send certificates and keys by email. Remember: these are the keys to your organization's most valuable assets. If someone's email account is compromised, those assets can easily fall into the hands of outsiders and criminals.

The Expertise Challenge

PKI is a niche technology whose rules differ significantly from those of normal IT operations. For this reason, many companies lack the expertise they need to maintain it. Over half of organizations say they are unable to hire and retain enough qualified IT staff to manage their PKI, Ponemon-Keyfactor found.

Real-World Examples of the Expertise Gap

EXAMPLE # 1
Mishandling of Critical Certificates

At a large insurance company, a new PKI team discovered a server that wasn't powered on or even plugged in. It was just sitting on the rack gathering dust. So the team threw it out.

It turned out the discarded server contained the company's root certificates. Issued by select certificate authorities, root certificates adhere to exceptionally strict requirements and have the ability to issue other certificates. They are the most critical component of PKI.

The server containing these root certificates was deliberately kept offline to isolate it from potential attack and meant to be plugged in only for occasional maintenance. A PKI team with a better understanding of cryptography would not have allowed this error to occur. Fortunately, the company had backups.

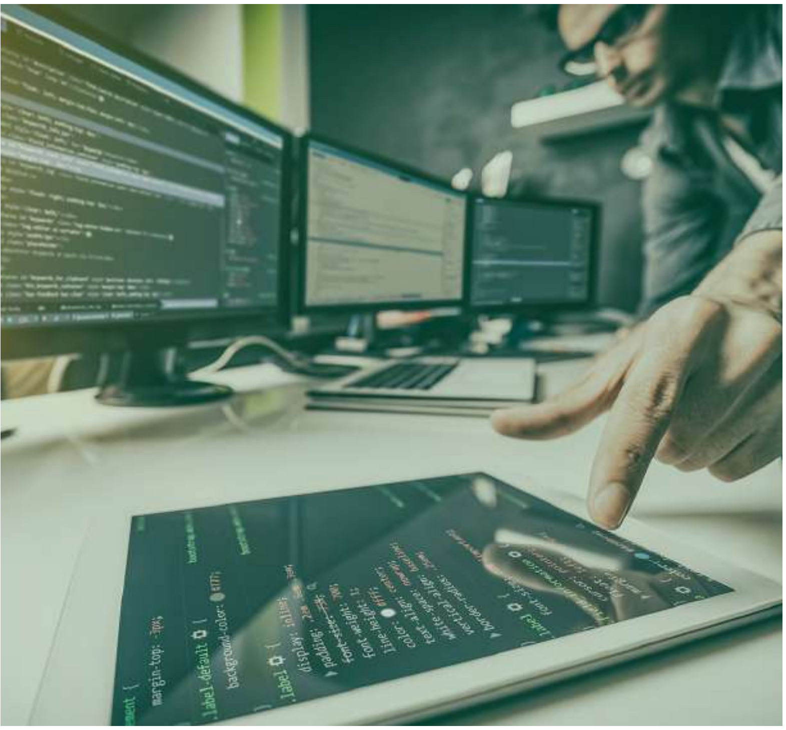
EXAMPLE # 2
Manual Management Processes Backfire

As a test, a company wrote a script to issue certificates to a firewall. But the script didn't end the test and continued to issue commands for certificates over 120,000 times an hour, preventing legitimate requests from going through. The company's server soon ran out of disk space, and by the next morning, no one could log on to the network.

A lack of digital certificate expertise also comes into play among DevOps teams, who are increasingly using Docker or other light-weight containers to manage certificates for the applications they are creating.

Once a certificate is in a container, developers can use Kubernetes or another engine to automate deployment and scaling. But they may not realize that application and certificate updates don't operate on the same schedule. Software updates may be released monthly, quarterly, or at irregular intervals as developers test and build, but certificates must be renewed annually.

In addition, application development eventually comes to an end, but certificates must be renewed for the life of the application. Who will manage them after the final release? Certainly not the DevOps team. But that problem is often an afterthought — if it is considered at all.



A lack of PKI expertise isn't confined to DevOps. It affects your entire organization. Each certificate that isn't properly guarded gives hackers a new opportunity for theft and expands the attack surface, creating a major security risk that your organization is completely unaware of until it's too late. In the past two years, organizations experienced certificate authority compromise or rogue certificates and man-in-the-middle or phishing attacks an average of five times, the Ponemon-Keyfactor report found. Certificate and key misuse were almost equally common.

Sometimes hackers don't even need to steal certificates. They may be inadvertently included in product firmware and sent to customers, which happened at D-Link.

These are just some of the problems that can occur when the individuals tasked with managing PKI lack in-depth knowledge of how it works. To truly close the Critical Trust Gap, organizations must find in-house experts to take control of their PKI operations -- or use a managed service

Impacts of the IoT and Quantum Computing

In a recent IDC survey, 85% of companies reported having budgets allocated for IoT projects. IoT products open the door to exciting new services and additional revenue opportunities, but they also create exponentially greater security threats. IoT devices are typically hacked within five minutes of being plugged into the internet and are targeted by specific exploits within 24 hours.

In the Ponemon-Keyfactor report, respondents ranked authenticating and controlling IoT devices as their No. 1 digital priority. But only 31% are confident in their ability to manage IoT devices (and the cryptography associated with them) over the devices' lifetimes.

That means today's organizations must dramatically scale their certificates and keys as the IoT brings more products and services online. Most current devices will long outlive their certificates, and they may pass through the hands of many users whose identities are not registered. But controls are typically weak or missing altogether. The OWASP Foundation ranks insecure ecosystem interfaces, including weak or nonexistent encryption, third on its list of the top 10 IoT threats. The National Institute of Standards and Technology (NIST) says a new cryptography standard must be developed to offer adequate protection for IoT devices.

In the meantime, printers, routers and video cameras have all been hacked, creating mistrust with customers and damaging companies' reputations. Researchers have also found that implanted medical devices such as defibrillators and pacemakers can be compromised, causing potentially life-critical problems.

How can IT and security leaders control the millions of endpoints of IoT devices? Using centralized, automated certificate management is a must. But managers must also remain knowledgeable of the cryptography innovations that are set to transform this sector.

Most companies are not yet worried about quantum computing, the next disruptive phase of technology that will have a dramatic impact on cryptography and security. Fewer than half of respondents in the Ponemon-Keyfactor survey conceded that the rise of quantum computers will require significant changes to key and certificate management.

The truth is this: Quantum computing's unprecedented processing speeds will make the algorithms that secure digital certificates obsolete, leading to the universal failure of PKI as we know it. That could happen in as few as five years.

Experts are already preparing for this emergency by developing new, agile models of PKI that can incorporate encryption methods as they emerge.

38%

of organizations are confident in their ability to manage IoT devices

It's Time to Rethink Your Security Strategy

The cloud, containers and new technologies like IoT and quantum computing are transforming organizations of all sizes. They radically increase efficiency and create innovative new business models. But they also introduce security challenges that require modern companies to change their approach to fundamental systems like PKI.

To avoid costly outcomes from the exposure epidemic, organizations must close their current Critical Trust Gap — and prevent a future gap from forming. They must unify their PKI, and store certificates and keys in one, safe location, under the direct control of the security team. And they must embrace a more comprehensive crypto-agile approach that can scale with continued digital innovation, and all that comes with it.

Most organizations don't really know whether their data and critical systems are safe.

KEYFACTOR

How does your company's Critical Trust Gap compare with the industry?

Find out with Keyfactor's Critical Trust Index calculator, which uses a 10-point scale to determine a company's ability to effectively manage PKI and digital identities critical to their business.

Take five minutes to complete the survey, and we'll show how you compare with your industry, based on the responses of more than 600 IT and security professionals. And we'll provide practical guidance to close your Critical Trust Gap.

Calculate your score at benchmark.keyfactor.com

Keyfactor

empowers forward-thinking companies to escape the exposure epidemic by securing data from trusted devices, people and apps that are critical to their business and people's lives. Keyfactor customers are free to unlock value from the exponential growth of connectivity without compromise. And they can adapt with agility and ease to dynamic business and technology environments.

Learn more at www.keyfactor.com.

KEYFACTOR

▶ www.keyfactor.com

▶ +1.216.785.2990

Keyfactor Headquarters

6150 Oak Tree Blvd., Suite 200 Independence, OH 44131