KEYFACTOR

White Paper

The Role of Digital Trust in an Untrusting World

Building strong digital trust supports innovative new products and business opportunities

Table of contents

The role of digital trust in an untrusting world

Building strong digital trust supports innovative new products and business opportunities

C-suite executives are paying more attention than ever before to protecting their organizations from cyber threats.

There have been a number of high-impact cybersecurity breaches over the past several years that affected government agencies, international businesses, and companies of all sizes located all over the world. Because of that, most executives today are taking steps to address two key concerns: first, that their critical systems could either be breached by skilled attackers or infected by malware (which could then spread outside of their home network via connected systems), and secondly, that their systems could be taken down due to someone else's failure.

For example, the SolarWinds breach – which started in 2019 and came to fruition in 2020, blamed on Russian cyber espionage – graphically demonstrated how global software supply chains could be threatened by a single incident if it's strategically placed by skilled attackers. In the United States, the Colonial Pipeline ransomware attack in 2021 additionally proved that hackers can simply be criminals looking for a big payday, yet still have a devastating impact on millions of ordinary people. In October 2022, a dark web marketplace for stolen credit cards released more than 1.2 million card numbers.

In this landscape, finding ways to create trusted digital networks is essential. But even more fundamental is creating *digital trust*, defined by the World Economic Forum(WEF) as "individuals' expectations that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values."

Digital trust, then, is the only way to keep the digital ecosystem up and running. It's the only way to build a more successful and inclusive economy because it relies on securing the digital infrastructure and providing assurance to users that the devices, applications and data that they interact with are both accurate and secure from threats. When people have digital trust in the devices and networks they interact with, they are free to conduct business without the fear that they will be personally attacked or affected by threats. It thus removes any barriers to letting the digital economy flow while also providing real protection for devices, users, networks and data.

Challenges to digital trust

According to the Information Systems Audit and Control Association (ISACA) there is a disconnect between how highly most organizations value the concept of digital trust and how much effort they are currently putting in to achieve it. In fact, in ISACA's most recent 2022 survey of more than 2,700 business and IT professionals around the world, the gap between what organizations need and what they have in place with regard to digital trust is wider than ever. Almost all of the respondents (98%) to the survey said that digital trust is important, yet only 12% of their organizations have dedicated staff in that area or are even planning how to implement digital trust.

Looking deeper, the ISACA survey found that not enough training (53%), a lack of alignment with their enterprise's goals (44%), no leadership buy-in (42%), a lack of budget (41%) and too few technological resources (40%) all play a role in the gap between the acceptance and the actual advancement of digital trust.

And those are just the internal obstacles.

Externally, and strategically, global consultant PwC identified ten key digital trust challenges almost a decade ago. In technology terms, that's an eon – yet almost none of the challenges have been completely solved. Those ten challenges include:

- Getting the balance right between data privacy and data use
- The ethics of using data on people
- Identifying the limits of predicting and profiling people's actions
- Transparency and regulation of algorithms
- Building safeguards around AI
- Governing the internet (without breaking it)
- Cybersecurity and citizen privacy
- Building resilience when there are digital disruptions
- Redefining ownership in a virtual world
- Managing the downside of workplace automation

And that list makes no mention of the specific kinds of threats like phishing, ransomware, malicious insiders and others that C-suite executives know their organizations face every day. It's critical to be prepared for those kinds of threats, but they are tactical – every time a new threat emerges, the IT industry develops new response and remediation tools. The larger challenge for organizations is how to respond to the attacks in a way that protects users' (whether customers, vendors or employees) sense of digital trust.

Some of this is reflected in a 2022 survey by Rackspace Technology about why cybersecurity gets the most attention from the C-suite. Their greatest concerns are operations downtime (60%), loss of intellectual property/data (54%), damage to brand reputation (49%) and revenue loss (38%).

These all have a negative impact on digital trust. In fact, the consequences of losing digital trust are becoming apparent: CSO Online reported last year that almost half of the readers that they surveyed have left a vendor due to poor digital trust, and 84% of customers also said they would consider leaving a vendor that doesn't manage digital trust.

Globally, the European Union (EU) has taken the biggest steps toward establishing broad-based digital trust. In February it implemented the European Declaration on Digital Rights and Principles framework, and in May the lead EU privacy regulator fined Facebook's parent company Meta a record $1.3 billion over transferring data from European users to U.S. servers.

But achieving digital trust is just the first step, for countries and companies alike. The ongoing work of any organization will be to maintain it in the face of new threats arising almost every day. Further, the day is not far off where it might not matter that an organization is digitally trustworthy if the larger environment – the internet as a whole – is not.

What is digital trust?

The WEF identifies three elements that, when combined, create an environment of digital trust. Those elements include:

01 **Security and reliability**

02 **Accountability and oversight**

03 **Inclusive, ethical and responsible use**

The foundation for accountability and oversight is comprised of transparency, auditability and redressability – that is, being able to see that the organization is digitally trustworthy, that there is a process to remedy lapses or failures, and that all the processes meant to foster digital trust can be audited and corrected. The IT field is used to being audited, creating an electronic or paper trail to review events and transactions. However, many organizations as a whole have issues with increased transparency, whether because of their concerns about protecting intellectual property or because of an organizational culture that was either born into or which cultivates secrecy as a normal part of their operations. Redressability, on the other hand, can come from organizational action, regulation, or the courts.

The principle of inclusive, ethical, and responsible use is based on two factors: interoperability and fairness. Interoperability has a technological component, of course, since devices and software must be able to reliably connect to networks, data or the internet in order to transfer information and execute actions. Fairness, on the other hand, is a social construct, one which many societies struggle to articulate. It is more about pursuing fairness, even while acknowledging it is a constantly evolving standard, so having mechanisms to recognize and implement that changing standard becomes important.

Security and reliability falls squarely into the technology camp, incorporating privacy, safety, and cybersecurity. While technology must support inclusive, ethical, and responsible use, as well as accountability and oversight, those are policy actions for humans, not solely based on technology.

With IT, however, many activities are completely invisible to users, who are left to count on their devices, software, APIs, and networks being trustworthy – that is, their cybersecurity is strong, monitored, and updated, and that their data, whether at rest or in transit, is protected. They must also feel that their privacy is protected.

This is why all organizations, whether governmental or in the private sector, have a stake in strengthening their systems' reliability and security, so that users are not left to wonder if they are truly safe. When that kernel of doubt is present, it means digital trust does not yet exist.

How to achieve digital trust

All organizations are responsible for establishing and maintaining their own digital trust. This includes not only implementing policies but also investing in technologies that protect users, both internal and external.

It also means having policies that require vendors to implement their own digital trust measures. This is the rationale for the U.S. government's zero trust architecture mandate and issuance of requirements for federal agencies to establish security in the software supply chain.

Executive Order on Improving the Nation's Cybersecurity

Learn more ↗

Identity is central

In the zero-trust approach, a verified identity for every person, device, app, software and API is foundational. To support zero trust architectures, agencies must be able to manage machine identities in the same way they must protect employee and contractor identities through Personal Identity Verification 201 (PIV-201) requirements.

Public key infrastructure (PKI) and machine identities, such as TLS, SSH, and code signing certificates are core technologies to enable zero trust and enhance security in the software supply chain. The supply chain requirements in particular will ripple through the commercial IT ecosystem, as IT providers that look to meet the government standard will provide the same products and solutions to private sector customers.

For many, if not most organizations, the hardest part of identity management is actually on the technology side – both private and public sector entities know who their employees are, after all, but they often have no idea how many devices (both computer and IoT), servers, apps, containers, and APIs run in their networks, or which ones the organization owns and which belong to employees.

The push to automate is only going to make that worse. As Keyfactor reported in its 2023 State Of Machine Identity Management Report, More than 60% of respondents to our report said they do not know how many keys and certificates they have – which is 7% more than last year.

To achieve digital trust on the IT side, there are five steps to successfully issue and manage machine identities at scale. And "machine identity" includes everything in the IT ecosystem from computer and IoT devices to servers, apps, APIs, and containers.

01 Establish ownership of machine identity management (MIM), a working group or team to issue and maintain keys and certificates, including responsibility for policies to keep MIM current and incorporate new technologies as they are added.

02 Invest in MIM to improve visibility and accelerate incident response and productivity, including automating and standardizing security controls by integrating them with existing tools, workflows, and applications.

- This also means auditing the organizational machine identity landscape to find the gaps, and looking for tools and processes that fit the unique needs of each part of the organization.

03 Reduce the complexity of the PKI infrastructure, because technology has been changing so rapidly over the past two decades, many organizations are using multiple types of keys and certificates, which adds significantly to the burden of keeping them up to date while also incorporating new devices.

04 Many organizations are suffering from a skills shortage. Using managed services can ease the shortage and address cybersecurity requirements.

05 Include code signing security as part of a MIM strategy unless the private keys used by programmers to sign code are secure. There is always a risk that bad actors can compromise their software.

Examples of digital trust in key industries

1. Automotive

Vehicles, whether for personal or commercial use, are relying more and more on internal IT and IoT systems for everything from diagnostics to navigation and communications. And every vehicle's occupants are inherently trusting that the vehicle will perform as expected. Yet the increased production of connected vehicles also means the increase of potential attack vectors, while the cost of updating and patching security holes can be expensive.

Streamlining and managing hundreds of millions of certificates inside hundreds of thousands of vehicles in the event of a breach can be handled in as little as a week with a MIM architecture built around maintaining digital trust between the manufacturer and customer.

2. Healthcare technology

Many medical devices, from Fitbits to pacemakers and wearable glucose monitors (and many, many more), now rely on internal IoT devices to gather and share information. Each device requires identification and verification to handle secure data sharing and receiving software updates. The patient using the device, whether on their wrist or implanted in their chest, must count on it working properly at all times.

Using automated PKI and certificate platforms not only enables the devices to function securely, it lays the groundwork to create relationships between different components in the broader medical device ecosystem.

3. Manufacturing

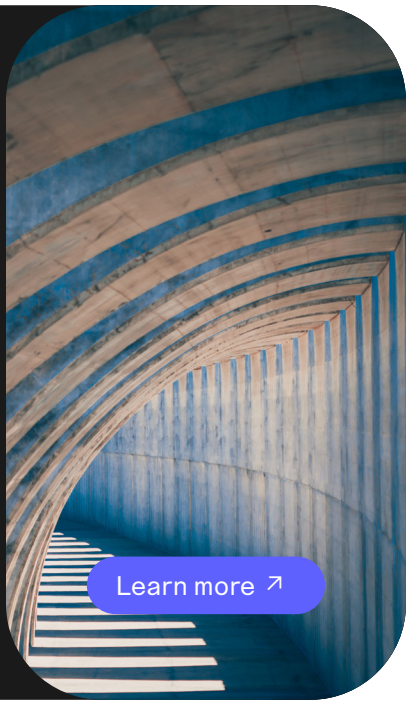
While automotive and healthcare technologies are focused on end-user digital trust, the same principles apply in business-to-business transactions, such as manufacturing. Companies need to safeguard their internal operations, but in the new connected economy they also need to trust electronic transactions between themselves, their vendors and their corporate customers.

Implementing PKI certificates allows every interaction to be verified, whether it's inside a company's network or involves a third party – a supplier, a customer or an employee.

4. Financial services

Banks and financial services firms rely on the electronic authentication of transactions – especially large institutions that may handle millions of transactions per day. For many of these companies, their PKI infrastructure evolved over time, without the policies and procedures in place to ensure consistent application.

Financial services are just as affected by rapid technological innovation as other industries. Establishing a standardized, system-wide process for issuing, updating and revoking certificates is essential to developing digital trust between the firm and all its myriad customers.



Think of the possibilities

Digital trust is quickly becoming both the framework and backbone of modern technological integrations and inventions. With digital trust, companies can build long-term relationships in the connected world in innovative ways that simply wouldn't work without it. That is because a foundation of digital trust provides the starting point that every new digital service or product must have.

There are many good examples of this, including everything from Facebook's rapid rise to the success of Amazon's online marketplace. Streaming services that people can use to watch their favorite shows or movies on any device is yet another example of a technology that once seemed impossible, now quickly becoming commonplace.

And what is the one thing that all of those examples, and so many others in the technology realm, have in common? None of them could exist without digital trust. In every case, the unifying factor is that digital trust is so integrated into the technology that customers don't even really think about it.

For example, someone who wants to watch the new Top Gun movie on their laptop, television, or phone simply goes to the streaming service that hosts it and either logs in if they are a member or pays a one-time fee to access the film. They don't worry about the safety of their credit card details, or if their personal information is going to be protected. Digital trust takes what is actually a fairly complex backend process and simplifies it to the point where it becomes an impulse purchase. Customers simply point and click, and suddenly Tom Cruise is soaring through the skies again.

Digital trust means that customers never have to worry about the layers of trust embedded throughout the process of using technology. That leads to increased usage and sales. In fact, an October 2022 survey by McKinsey estimated that organizations that foster digital trust will see growth rates of at least 10 percent in both gross sales and net profits across the board. No matter what new idea or service a company wants to create or support, having digital trust will either outright enable its success, or will make it much more profitable and popular.

Conclusion

Digital trust is becoming the bedrock of today's online world, even though it has not yet been achieved everywhere that it is needed. But it's rapidly expanding, driven by the needs and requirements of both businesses and the customers they serve.

On the business side, companies are seeing that a large part of their overall prosperity will now depend on customers having complete faith in the safety and privacy of their transactions. And that will require digital trust to protect data both at rest and in transit during those interactions. They also are seeing businesses that fully support digital trust reap measurable and increased profits versus those which have not yet achieved that milestone.

Consumers also are starting to expect digital trust. They value the speed and convenience of digital transactions, and have seen first-hand how convenient digital services can be for everything from ordering dinner to collaborating with colleagues online. But that only works if those services can be trusted, which is why consumers are also starting to take digital trust seriously, and why companies that foster digital trust are seeing increased popularity and profits.

Digital trust is not easy to achieve, and once obtained, it will take a lot of work on the part of all concerned to maintain it. But the roadmap is there. The actions needed to attain digital trust are well known at this point. They include better security, transparency of incident responses, better identity management, and more. And working on improving those elements is possible for almost any company or organization regardless of their size.

If organizations prioritize digital trust in both their own operations and customer interactions, the opportunities to build a new digital ecosystem filled with innovative products and services, and to earn healthy profits from those endeavors, are only limited by one's imagination of what a world based on a foundation of digital trust might look like, and what that world can achieve.

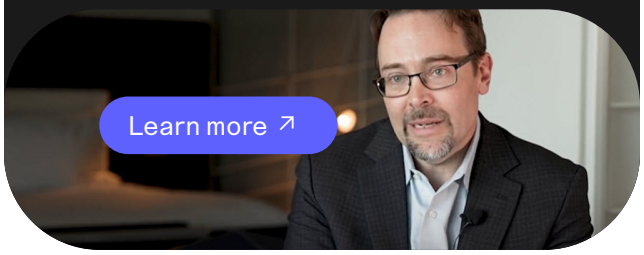
Additional resources:

eBook

Cybersecurity labor shortage

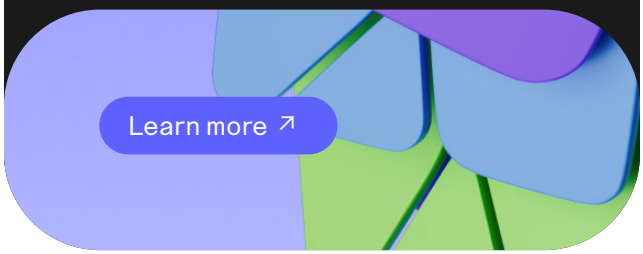
Video

What does digital trust mean to you?



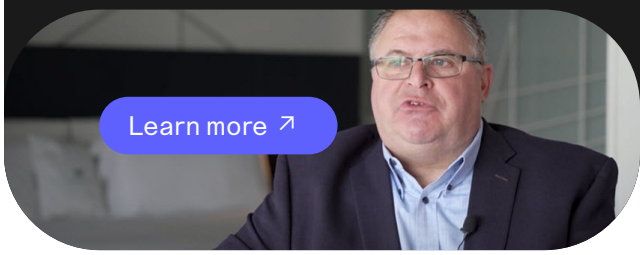
Industry report:

2023 State of Machine Identity Management Report



Video:

What is PKI complexity?



KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2946 (North America)
- +46 8 735 61 01 (Europe)