# 2024 STATE OF DIGITAL TRUST REPORT

LEADERS

LAGGARDS

PKI

COMPLIANCE

OUTAGES

XX
SECURITY ALERT

DIGITAL TRUST FOR THE REAL WORLD

IoT

BEST PRACTICES

digicert®

# 2024 STATE OF DIGITAL TRUST REPORT

In 2022, DigiCert introduced our annual State of Digital Trust Survey. As digital transformation rolls out across every industry, digital trust is essential to ensuring that the people and devices we connect with are legitimate and that our interactions are safe.

Jennifer Glenn, Research Director for IDC, defined digital trust as "the foundation for securing the connected world, and necessary for organizations looking to ensure that their customers, employees, and partners can be confident that online business processes and interactions are secure."

DigiCert, the leading global provider of digital trust, enables individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. To serve our customers, we are committed to understanding how global organizations perceive digital trust and how they are progressing in their efforts to establish, manage, and extend digital trust.

## Building on trust insights

Our initial survey found that 100% of enterprises felt digital trust was important. Nearly all of them (99%) believed it possible that their customers would switch to a competitor if they lost trust in the enterprise. Most consumers agreed, with two-thirds (68%) saying digital trust is important.

In this latest read-out, we wanted to dive deeper to see what happened since the initial report. The DigiCert 2024 State of Digital Trust survey takes a closer look at specific digital trust functions and workflows to learn more about how enterprises are faring and how they can continue to optimize their digital trust efforts.

## Methodology

Dallas-based Eleven Research fielded the 2024 State of Digital Trust survey in Q4 2023, administering the survey by phone to 300 senior decision-makers in small to large enterprises in North America, EMEA, and APJ.

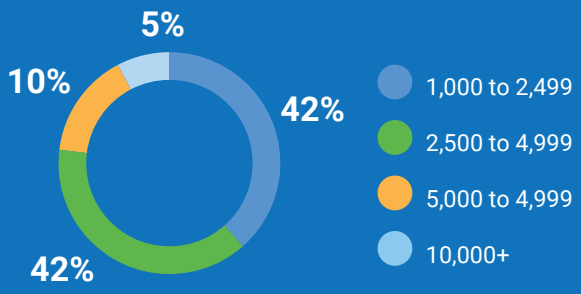
We spoke to participants from a variety of industries, including technology, manufacturing, and financial services. The companies ranged in size from 1,000 employees to more than 10,000.

To better understand specific digital trust efforts, Eleven Research focused on those responsible for four individual Digital Trust areas:

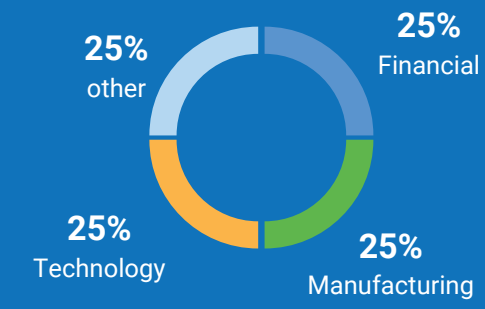
- Enterprise – securing communications, data, and access for employees, applications, and clouds
- IoT & Connected Device – protecting smart devices and services like glucose monitors
- Software – protecting software and apps from tampering and supply chain attacks
- eSignature – ensuring the authenticity and integrity of documents and content

## GEOGRAPHY

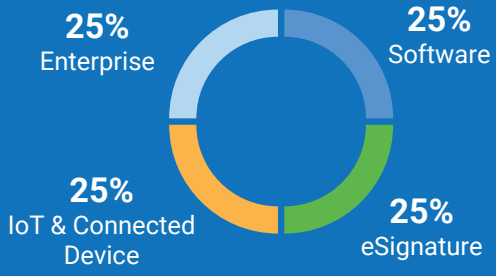

## COMPANY SIZE



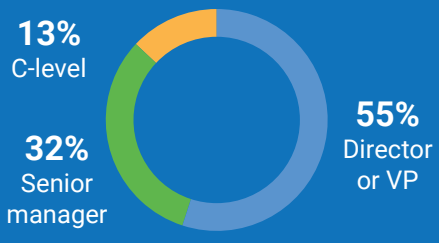

## INDUSTRY




## PERSONAS




## SENIORITY

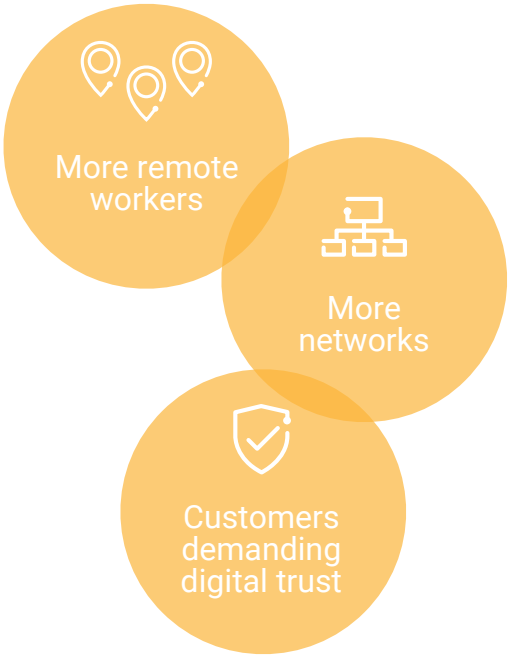


# ENTERPRISES REMAIN FOCUSED ON DIGITAL TRUST

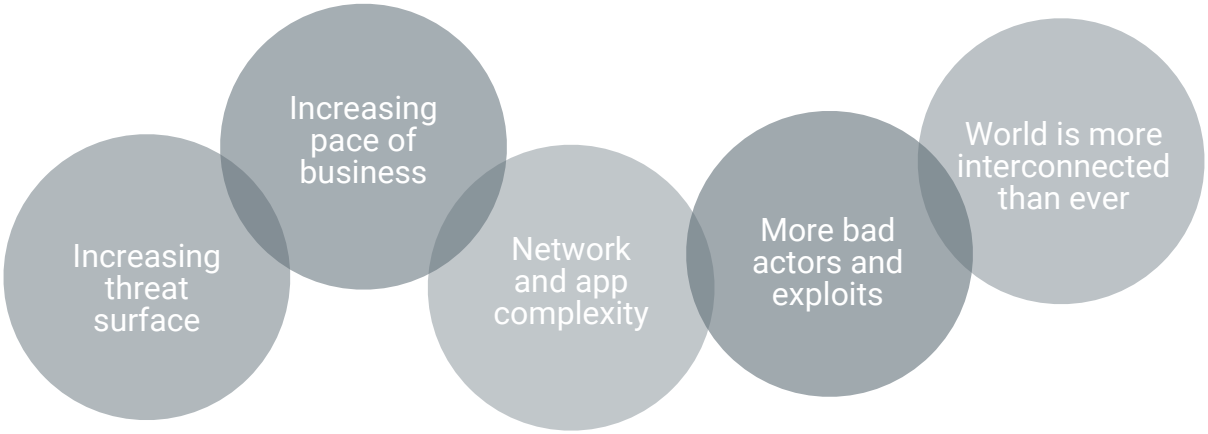
Given the overwhelming support shown in last year's survey, it's not surprising that enterprises are still laser-focused on digital trust. The three most important drivers of this interest are:

- There are more remote workers today than ever before
- There are also more networks (including at the edge and connecting to partners and customers)
- And, most importantly, customers are demanding digital trust from the enterprise

## TOP THREE REASONS



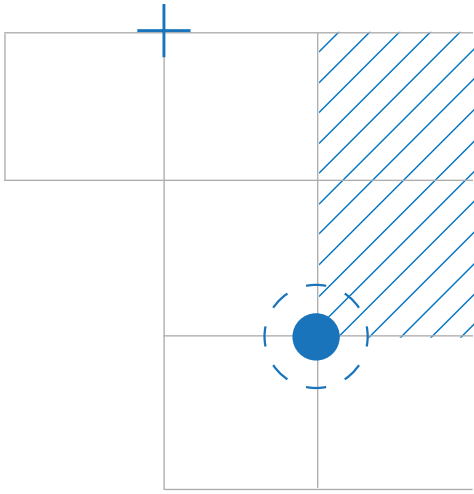

## OTHER REASONS



However, enterprises are finding that digital trust is not easy to establish, monitor, and manage. They struggle with five key challenges:

- **A lack of staff expertise.** Digital trust is still a relatively new discipline, and not all staff are up to speed on how to implement it in a centralized manner. Additionally, many private PKIs were established a decade ago and are perceived as brittle and prone to outages, further preventing teams from gaining much-needed expertise.
- **The growing complexity of networks and applications.** The enterprise technology fabric has become increasingly complex. On the network side, enterprises have moved beyond the traditional data center, remote offices, and cloud footing. Today's networks now include edge networks, thousands of remote workers, and multiple clouds.

  Furthermore, applications have moved from monolithic applications to highly distributed microservice architectures, where many services are not under the direct control of the enterprise. It is brutally difficult to achieve digital trust in such a complex environment.
- **The sheer scope of what enterprises need to secure.** As digital transformation efforts progress, more and more digital assets have become mission critical. As this happens, the scope of what enterprises need to protect grows exponentially.
- **A lack of management support.** As the economy has become more challenging due to the pandemic and inflation, management has been forced to make difficult decisions. For example, layoffs claimed more than 240,000 workers from the technology sector in 2023 alone.[1] It is not surprising to see management's commitment to digital trust waver in such a challenging environment.
- And, finally, the **rapid expansion of cryptographic assets is difficult to manage and time consuming.** Whether in public or private trust, digital certificates remain fundamental to establishing trust efforts. But digital certs are challenging to manage at the vast scale enterprises are now dealing with.



[1] Tech Crunch

# TRACKING PROGRESS ON ENSURING DIGITAL TRUST

How are enterprises doing at implementing digital trust? The full answer to this question is deep, complex, and nuanced. But the short answer is that enterprises are doing "good, but not great."

Their success varies depending on the specific areas of digital focus. We examined four specific digital trust areas to learn more about how enterprises are faring:

- Enterprise
- IoT & Connected Device
- Software
- eSignature

## Enterprise Trust Practices

Enterprise digital trust is most typically managed by IT. The types of digital trust most often managed within enterprise digital trust include:

- Certificate management
- Identity and access management
- Email security
- Endpoint security

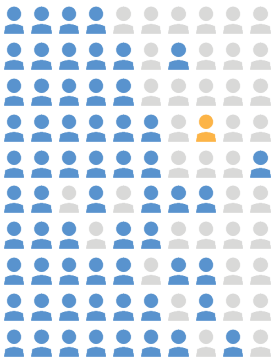
Even in Enterprise Digital Trust—the area we expect to be the most mature—digital trust efforts are still embryonic. Very few (just 1 in 100) enterprise trust managers say their practices are "extremely mature." In addition, 87% say their efforts are siloed.

Digital certificates provide the mechanism to authenticate and secure the communications of enterprise users and the machines they use like web servers and smartphones. As enterprise networks and use cases become larger and more complex, they require an ever-growing number of certificates.

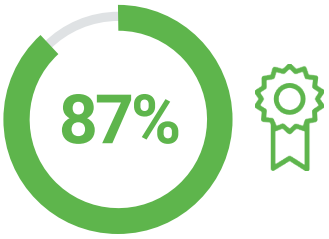
Roughly half (52%) of the enterprises we surveyed have IT manage their certificates, a third (37%) manage outside of IT, and one in nine (11%) are not managed.

Note that the typical enterprise has five or fewer departments that issue certificates, but most feel there should be more departments that do so.

Just **1 in 100** say their Digital Trust practices are extremely mature.



Most say just "somewhat" mature




say their Enterprise Trust efforts are siloed

Typical enterprise has 5 or fewer departments that issue certificates

Most say more departments should issue certificates

Where certificates are managed


IT


Managed outside of IT


Not managed

## Enterprise Trust Practices

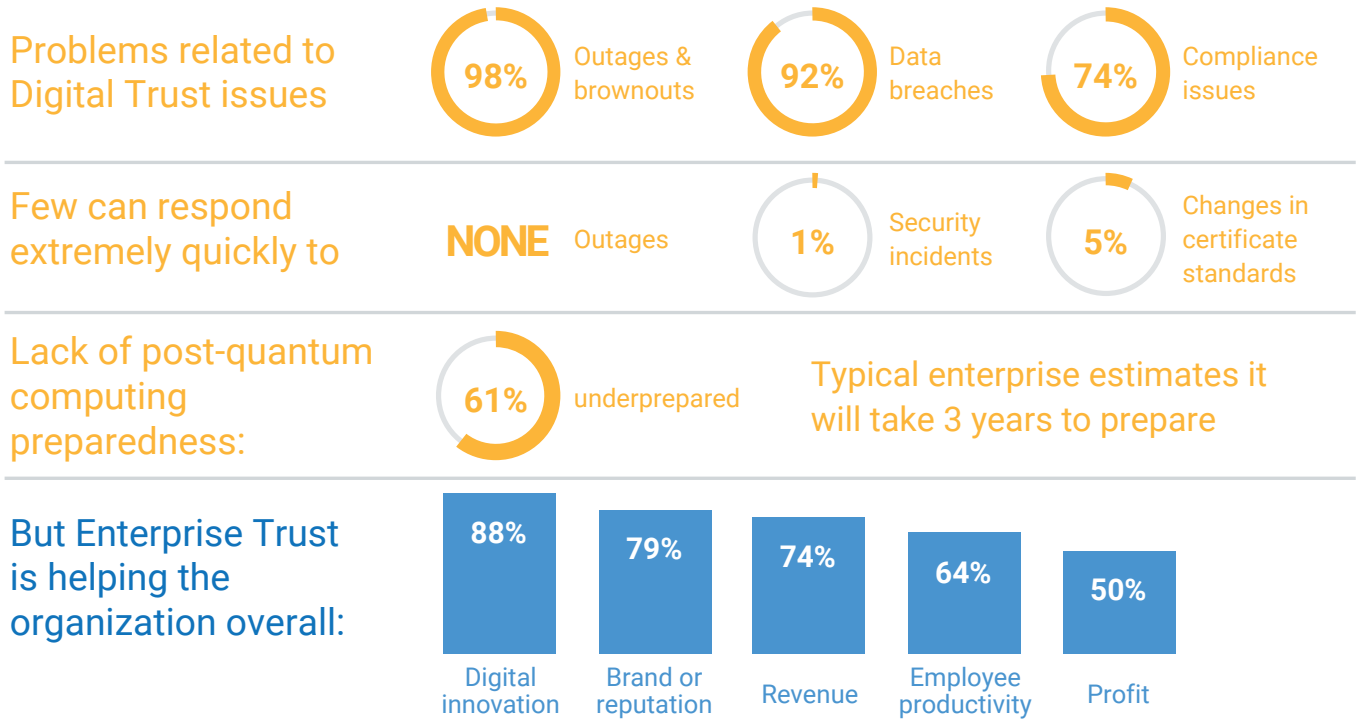
How are enterprises faring with their digital trust efforts? Not as well as they could, as it turns out. Respondents report the following issues related to digital trust mishaps:

- **Nearly all (98%)** report experiencing at least some outages & brownouts
- **Most (92%)** report experiencing data breaches
- And **quite a few (74%)** experienced compliance issues

We dug more deeply to measure their digital trust agility:

- **None** can respond extremely quickly to outages
- **Almost none** (1%) can respond extremely quickly to security incidents
- **Few (5%)** can respond extremely quickly to changes in certificate standards
- **Most (61%)** are under-prepared for a post-quantum world, with the typical enterprise estimating it will take three years to fully prepare

Despite these issues, enterprise digital trust managers say their efforts help the enterprise at a high level in areas ranging from digital innovation to brand to profit.



## IoT and Connected Device Trust Practices

Here, we focused on companies that manufactured and sold IoT devices or connected devices to customers (things like factory sensors, sports watches, and residential thermostats). We spoke with the people in the organization responsible for tasks such as:

- Working on authentication measures for IoT or connected devices
- Enabling encryption on IoT or connected devices
- Signing software or firmware updates to IoT or connected devices
- Using cryptography to protect IoT or connected devices

IoT & Connected Device digital trust managers report the same "good, not great" message. Just one in seven say their practices are extremely mature. Most indicated their practices were "somewhat" mature.

Astoundingly, **most (87%)** communicate PII coming from IoT or connected devices over unencrypted channels.

**Most firms (88%)** have a chief product security officer. They all use digital certificates to identify devices in the field and strong authentication for users.

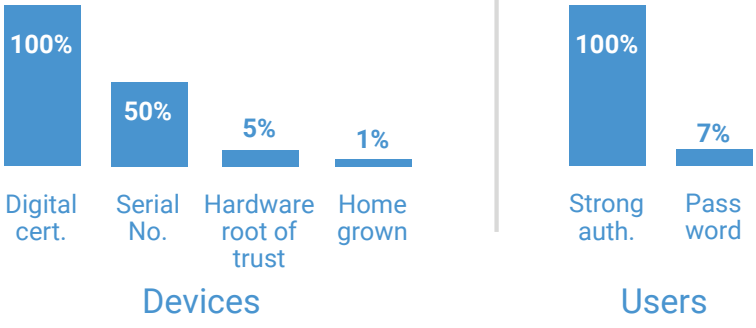
Just **1 in 7** say their Digital Trust practices are extremely mature.

Most say just "somewhat" mature


communicate PII coming from IoT or connected devices over unencrypted channels.


of organizations have a chief product security officer or centralized security practice that manages all IoT or connected devices.

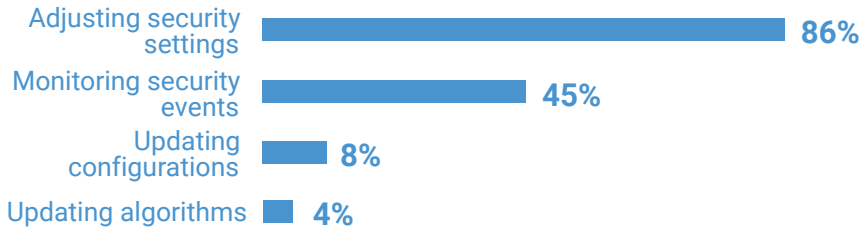
How they identify their devices and the users in the field:



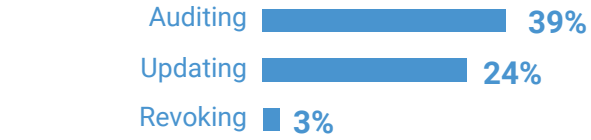
We asked respondents to rate their IoT & connected device capabilities in a variety of areas. Managing devices in the field was a mixed bag—they are great at managing security settings and okay at monitoring security events, but they're poor at updating devices.

They are also generally poor at managing device identities, especially revoking identities. One bright spot—they are primarily good at securing software, although they lag with secure delivery of software updates.

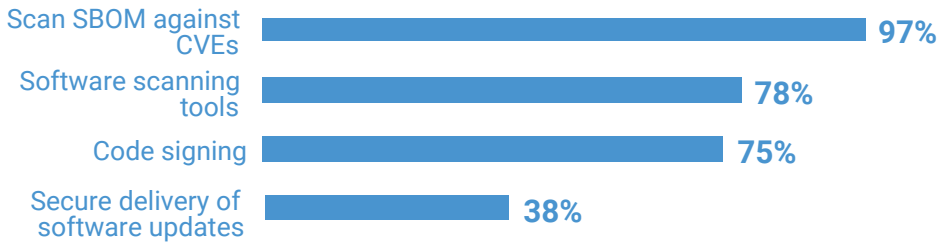
## Device capabilities in the field: Extremely capable of…




## Managing device identities:




## How enterprises secure software and firmware updates:



## IoT and Connected Device Trust Results

With these capabilities (and lack thereof), we found that the IoT and connected device manufacturers with whom we spoke were struggling somewhat:

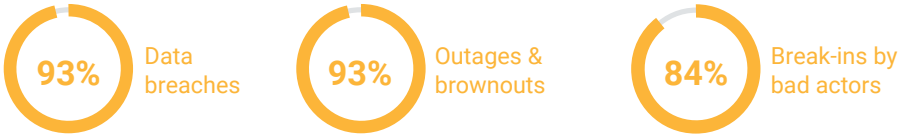
- **Most (93%)** had experienced data breaches. Many of these occurred because the device provided an easy back door to the network
- **Most (93%)** experienced both outages and brownouts
- And, related to our first point, **84%** had experienced break-ins by bad actors

IoT and Connected Device Trust practices did provide some benefits:

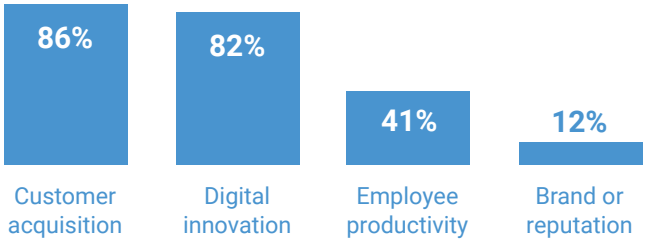
- **86%** reported they helped with customer acquisition
- **82%** say the practices helped with digital innovation

Nevertheless, it is clear that IoT and connected device manufacturers need to do better with their digital trust efforts.

### Problems related to Digital Trust issues




### But, IoT & Connected Device Trust is helping the organization overall:



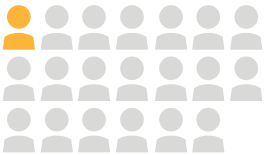
## Software Trust Practices

Software Trust ensures digital trust for the software enterprises sell (or simply distribute) to customers. Here again, the survey indicated "good, not great" progress. Just 1 in 20 (5%) say their software trust practices are extremely mature. What enterprises are code-signing also varies:

- **Nearly all (99%)** sign software source code
- **84%** report signing software binaries
- **62%** sign build scripts and infrastructure configuration
- **33%** report containers and serverless environments
- **Most (67%)** store code-signing private keys in FIPS-140-2 compliant devices

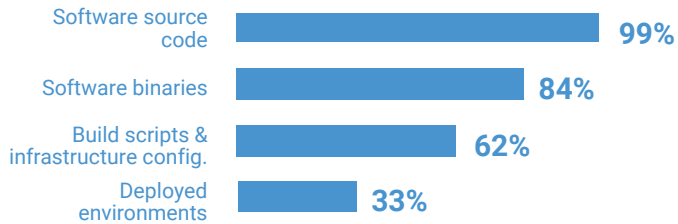
None of the enterprises we surveyed say they would be able to extremely quickly discover all applications associated with a specific code-signing private key if it were compromised.

Just **1 in 20** say their Digital Trust practices are extremely mature.

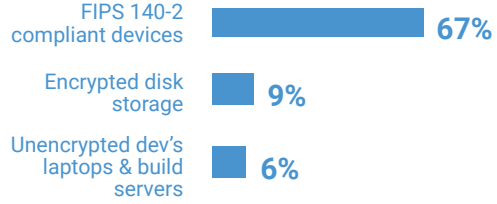


Most say just "somewhat" mature

### What enterprises are code-signing:




### What enterprises are storing code signing private keys:




If a code signing private key was compromised **NONE** would be able to quickly and easily discover all applications where it was used to sign.


Nearly everyone routinely generates Software Bill of Materials (SBOM) for the software they create.


Nearly everyone has risk, security, and legal requirements for third-party software.

## Software Trust Results

How are enterprises faring with software-related regulatory compliance? Only 1 in 8 are doing extremely well. They also report a host of issues related to software trust mishaps:

- **86%** reported data breaches
- **80%** reported breaches of software build infrastructure
- **79%** reported that software stopped working due to expired code signing certs
- **78%** delivered software that contained malware and other vulnerabilities
- **75%** missed release deadlines related to code signing or malware detection

Customers depend on the integrity of an enterprise's software, but securing all the keys needed for code signing can be daunting.

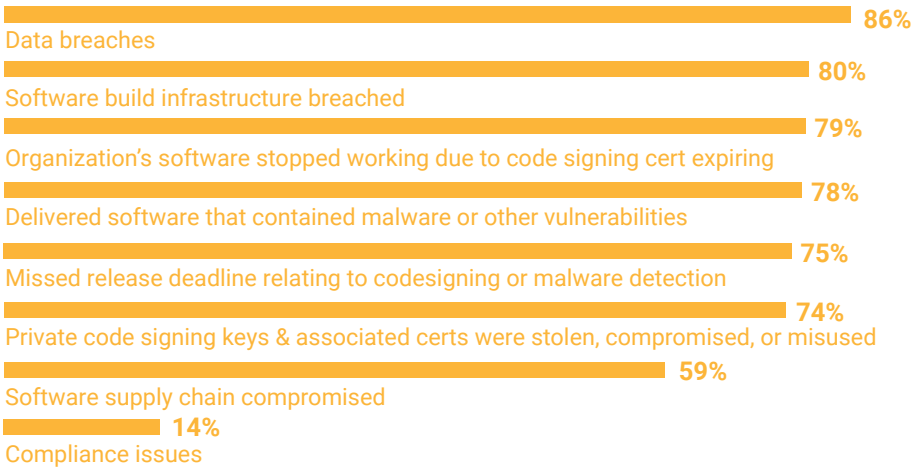
Few say they can easily generate a list of software components used in the software they produce.

All that said, software trust managers say their efforts are helping the enterprise in two high-level ways (digital innovation and employee productivity).


Are doing extremely well in terms of regulatory compliance as it relates to software.


Most are doing somewhat well.

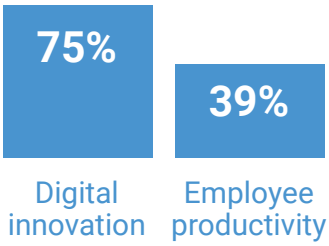
### Problems related to Digital Trust issues





Say it is extremely easy to generate list of software components and their configurations in software they produce

### But IoT & Connected Device Trust is helping the organization overall:



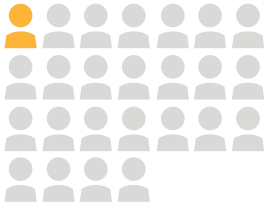
## eSignature Trust Practices

Document Signing certificates allow individuals, teams, and organizations to add an electronic, digital signature to a document in a variety of file formats to prove ownership, ensure documents stay unaltered, and protect sensitive information.

We asked respondents to rate the maturity of their eSignature trust, and 1 in 25 (4%) of enterprises say their eSignature trust practices are extremely mature—the lowest rating of our four areas. One characteristic of this segment is that eSignatures are administrated by businesspeople rather than IT (legal, HR, procurement, etc.), and only 1 in 8 have an understanding of the differences between basic and certificate-based eSignatures.

- **About half (48%)** use electronic seals for documents (legal, sales, procurement, etc.)
- **Most (86%)** use digital signatures with certificates issued by trusted third parties to verify signers

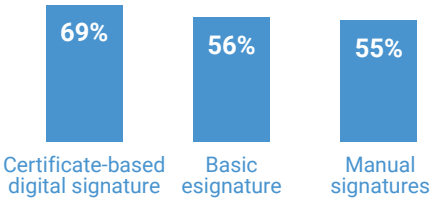
Just **1 in 25** say their Digital Trust practices are extremely mature.



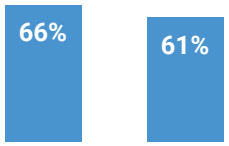
Most say just "somewhat" mature


Have a good understanding of the differences between basic e-signatures or certificate-based digital signatures

### Types of signatures being used:




### Types of signatures used by those using eSignatures:

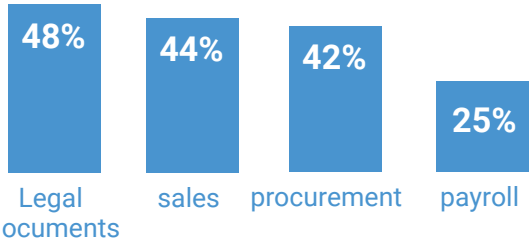




Use digital signatures with certificates issued by trusted third parties to verify signers.


Half use electronic seals for documents.

### Most common use cases:



## eSignature Trust Results

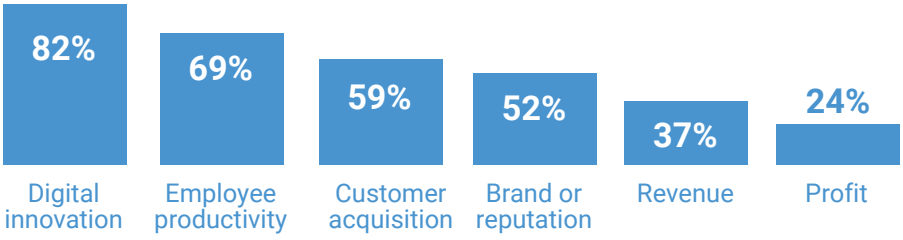
This group showed the highest incidents of issues associated with trust mishaps:

- **100%** report bad actor misrepresenting a document as coming from their organization
- **100%** report issues with paper-based contract processes
- **100%** report issues related to identity theft/ impersonation
- Nearly all **(99%)** report legal issues with cross-border contracts
- **96%** report compliance issues
- **87%** report organizations disputing that they signed an agreement

However, despite these issues, they say their efforts help the enterprise overall, with digital innovation, productivity, customer acquisition, and more.

### Problems related to Digital Trust issues


### But, Enterprise Trust is helping the organization overall:



# LESSONS FROM THE DIGITAL TRUST COGNOSCENTI

So far, we've discussed the results of all enterprises combined. But we noticed that within the group, some enterprises did better—and some did worse than average.

We were curious about these differences, so we tiered the results and compared them. To do this, we scored every question that measured results—questions like, "Have you seen breaches?" and "How quickly can you respond to incidents?" We gave positive points for good results and negative points for poor results, then tallied the points to give every respondent a total score.

We gave the title of "Digital Trust Leaders" to enterprises with scores in the top 33% of all categories. Those with scores in the bottom 33% are the "Digital Trust Laggards."

We dove in to understand the differences in outcomes and practices for these two cohorts in each of the four digital trust areas.

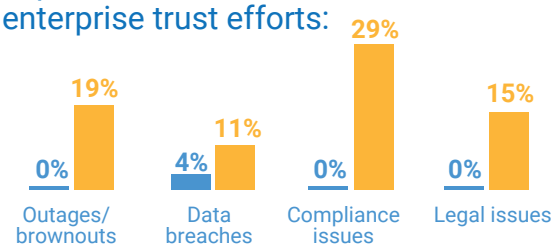
## Enterprise Trust

Starting with Enterprise Trust, we see the leaders are performing much better. They exhibit far fewer issues related to enterprise trust (no outages, few data breaches, and no compliance or legal issues).

**About three-quarters of the leaders (74%)** say they can respond extremely quickly to outages, compared to just 59% of laggards.

Leaders are nearly six times as likely to say they are prepared for post-quantum computing **(59% compared to 11% of laggards)**.

### Experienced fewer issues related to enterprise trust efforts:




### Respond quicker to outages


of leaders respond extremely quickly


of laggards respond extremely quickly

### More prepared for PQC

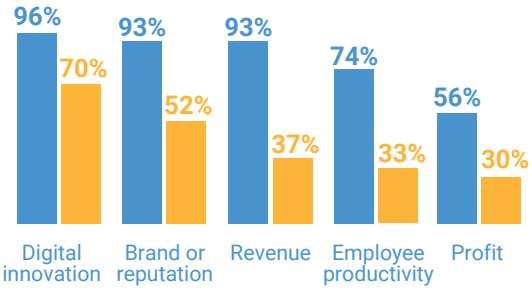

of leaders are prepared


of laggards are prepared

### Quicker to prepare for PQC

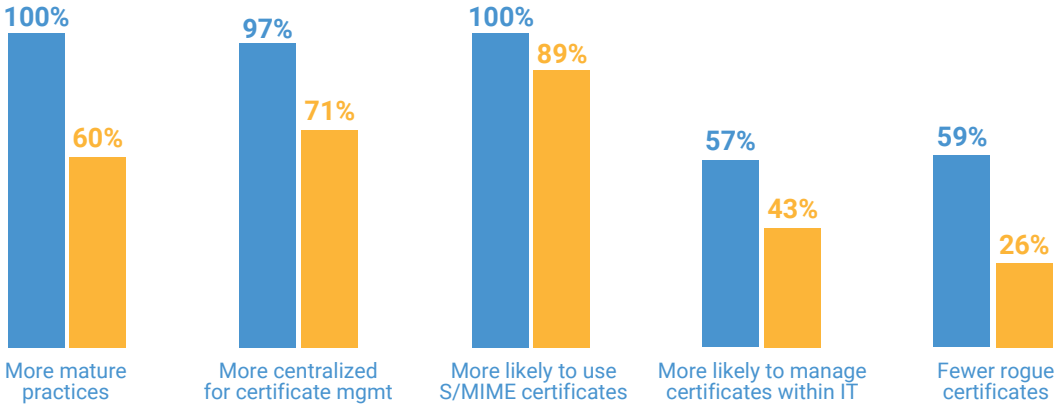

Leaders will take two years to prepare vs. three for laggards

### Enterprise Trust has significantly helped the organization in these ways:



### What are the leaders doing differently?

First, 100% of the Enterprise Trust leaders say they have extremely mature Enterprise Trust practices. They are more centralized, use S/MIME certificates to secure email communications, and manage certificates within IT. They also report fewer rogue certificates—as paradoxical as that seems.

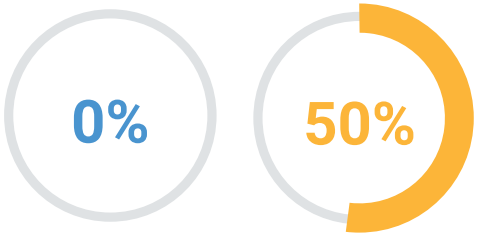



## IoT & Connected Device Trust

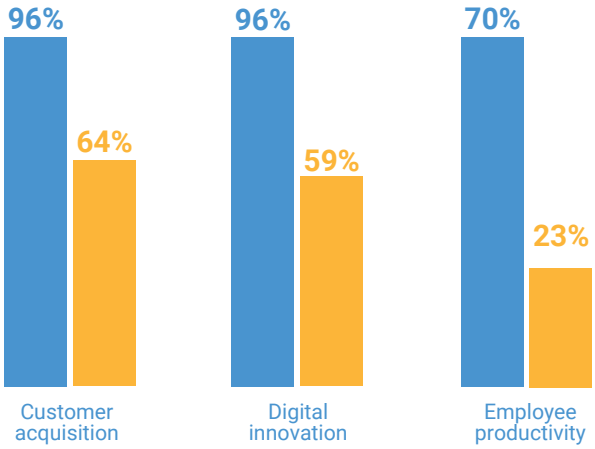
Next, we checked into IoT & Connected Device Trust professionals. Here again, leaders are significantly outperforming the laggards. The leaders experienced zero compliance issues due to IoT & Connected Device Trust, while half **(50%)** of the laggards did.

The leaders also felt their IoT & Connected Device Trust was helping the overall organization more, with nearly all (96%) saying it helped customer acquisition and digital innovation and most (70%) saying it helped employee productivity. This compares to just 64%, 59%, and 23%, respectively for the laggards.

### Experienced fewer compliance issues




### IoT Trust has significantly helped the organization in these ways:

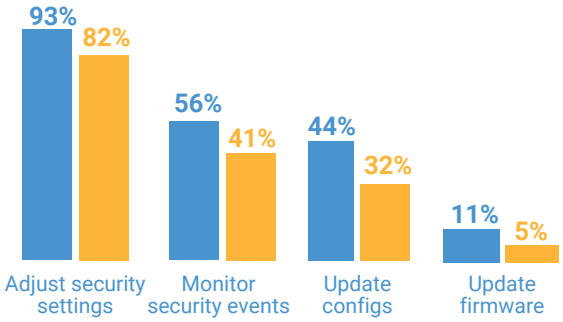


### What are the differences in practices?

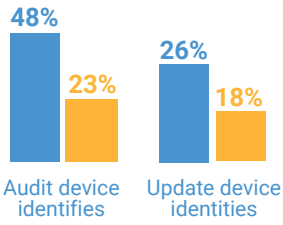
First, leaders are better able to make changes to and monitor devices in the field. They are also more capable of auditing and updating device identities.

Finally, while NONE of the laggards say they are extremely prepared for IoT trust issues, 19% of the leaders say they are.

## Better able to make changes to devices in the field:




## More capable in the following areas:




## More prepared for IoT trust issues

## Software Trust

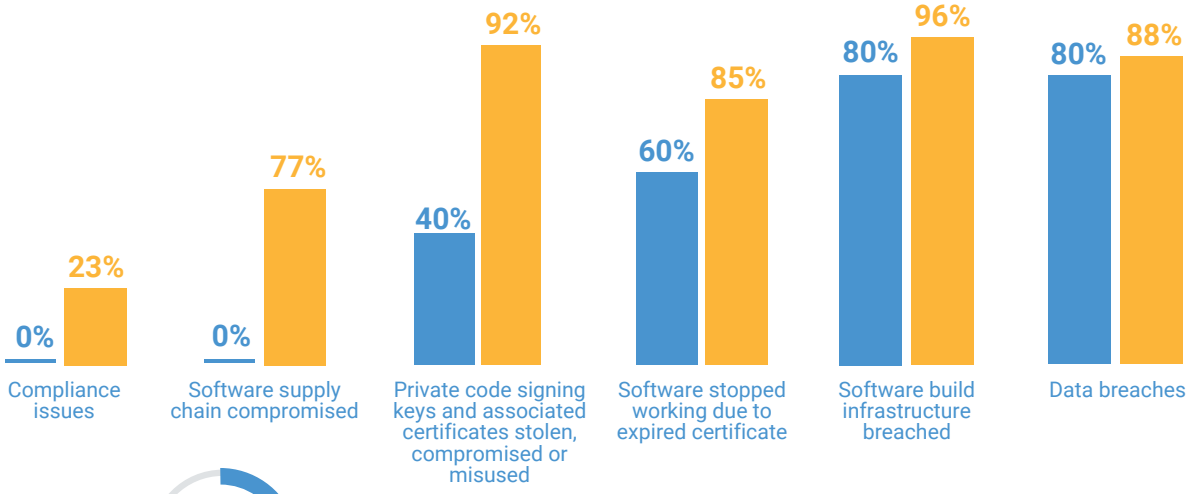
We then moved on to Software Trust professionals. Here, the leaders continue to do better than the laggards, with significantly fewer issues due to software trust mishaps. For example, none of the leaders experienced compliance issues or software supply chain compromises, compared to 23% and 77% of the laggards, respectively.

In addition, one in five **(20%)** say they have extremely mature trust practices versus none of the laggards.

Leaders also do much better in terms of regulatory compliance (60% compared to just 8% of laggards).

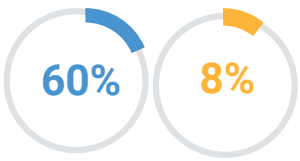
And leaders report their software trust efforts have had a more positive impact on the overall organization than the laggards, helping in areas like digital innovation, customer innovation, and employee productivity.

### Leaders experience fewer issues related to software trust mishaps:



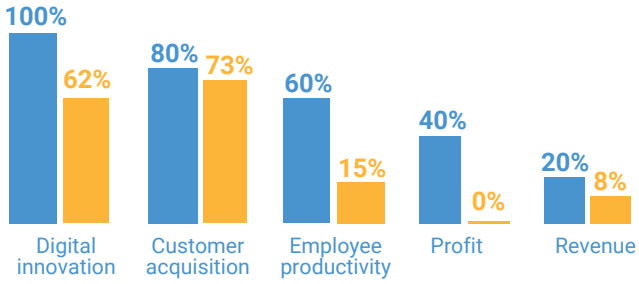


Leaders have extremely mature software trust practices versus NONE of the laggards




Leaders are doing extremely well in terms of regulatory compliance

### Software Trust has significantly helped the organization in these ways:



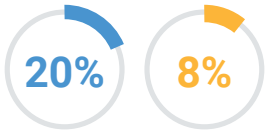
### What sets leaders apart?

Leaders are twice as likely to use a formal approval process to access cryptographic keys (80% compared to 38% of laggards).

Also, leaders were much more likely to say they find it extremely easy to generate a list of all software components and their configurations in the software that they produce (20% compared to just 8% of laggards).


More likely to use approval process to access any keys

Leaders find it extremely easy to generate a list of all software components and their configurations in the software that you produce



## eSignature Trust

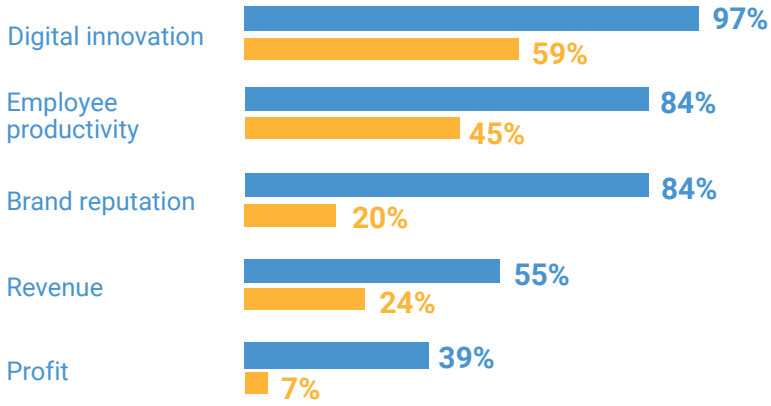
The final group we looked at was the eSignature trust professionals. eSignature trust is often managed by non-technical staff (managers from HR, legal, or sales, for example). Without IT's involvement, there is less technical depth to help manage the details of the eSignature trust efforts, and this shows in our results.

For example, more leaders say they employ extremely mature eSignature trust practices than the laggards, but the actual number (10%) is still small. Leaders also experience fewer eSignature trust issues, and report they are helping the organization more than the laggards.


of leaders are have extremely mature eSignature trust practices versus NONE of bottom

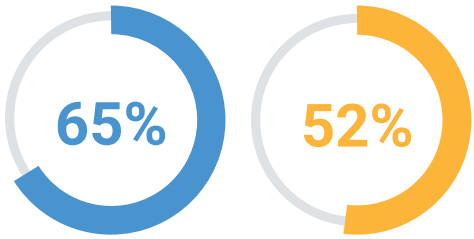
### Leaders experiencing fewer eSignature trust issues:


### eSignature Trust has significantly helped the organization in these ways:



### What is distinctive about the leaders?

These differences come down to one crucial quality. Leaders are more mature when it comes to understanding, implementing, and managing policies and governance for e-signature and eSeals.




Leaders are more mature when it comes to understanding, implementing and managing policies and governance for e-signature and eSeals

# DIGICERT'S TAKE

As the threat landscape broadens, so does the disparity between organizations at the forefront of digital trust and those lagging behind. While leaders and laggards are self-aware, the real risk lies with those in the middle who may harbor a false sense of security. If this gap widens due to ongoing complacency, the consequences could be severe.

What should organizations do to optimize their digital trust efforts overall and in specific areas such as Enterprise IT, software, device, and document trust?

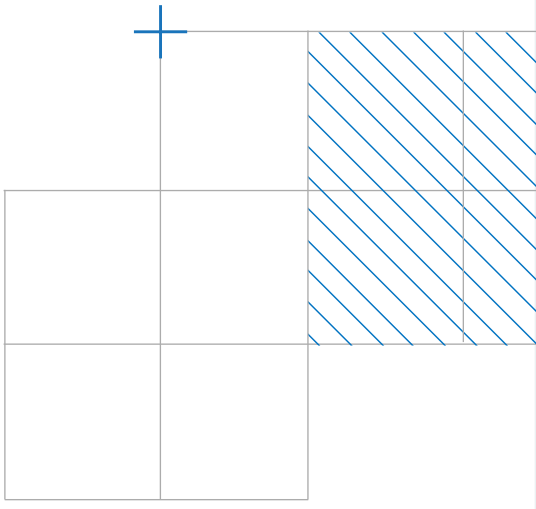
DigiCert is the leading global provider of digital trust, enabling individuals and businesses to engage online with the confidence that their digital footprint is secure. DigiCert has been involved in digital trust for more than 20 years, and our advice for companies wishing to emulate the success demonstrated by leaders is to:

## Take Inventory

The adage that you can't manage what you can't see applies to managing digital trust. Build a complete picture of how digital identities and cryptographic keys are created, protected, and used within your enterprise. You can do this through a manual effort of business process discovery or use technology to continuously scan your environment and ingest data from other sources like IT asset management systems.

## Define Policies

There are a host of policy considerations to aid your digital trust journey. Organizations should define policies for secure device and user authentication for remote and traditional workforces. Identify any policies required for regulatory compliance, especially for medical devices manufacturers and other heavily regulated industries. If your organization publishes business-critical software define policies for software supply chain security. Establish or evolve zero-trust initiatives especially for cloud-native workloads that process sensitive and regulated data. These examples are in addition to foundational polices to govern the use of cryptography and public key infrastructure within the organization.



## Centralize PKI Management

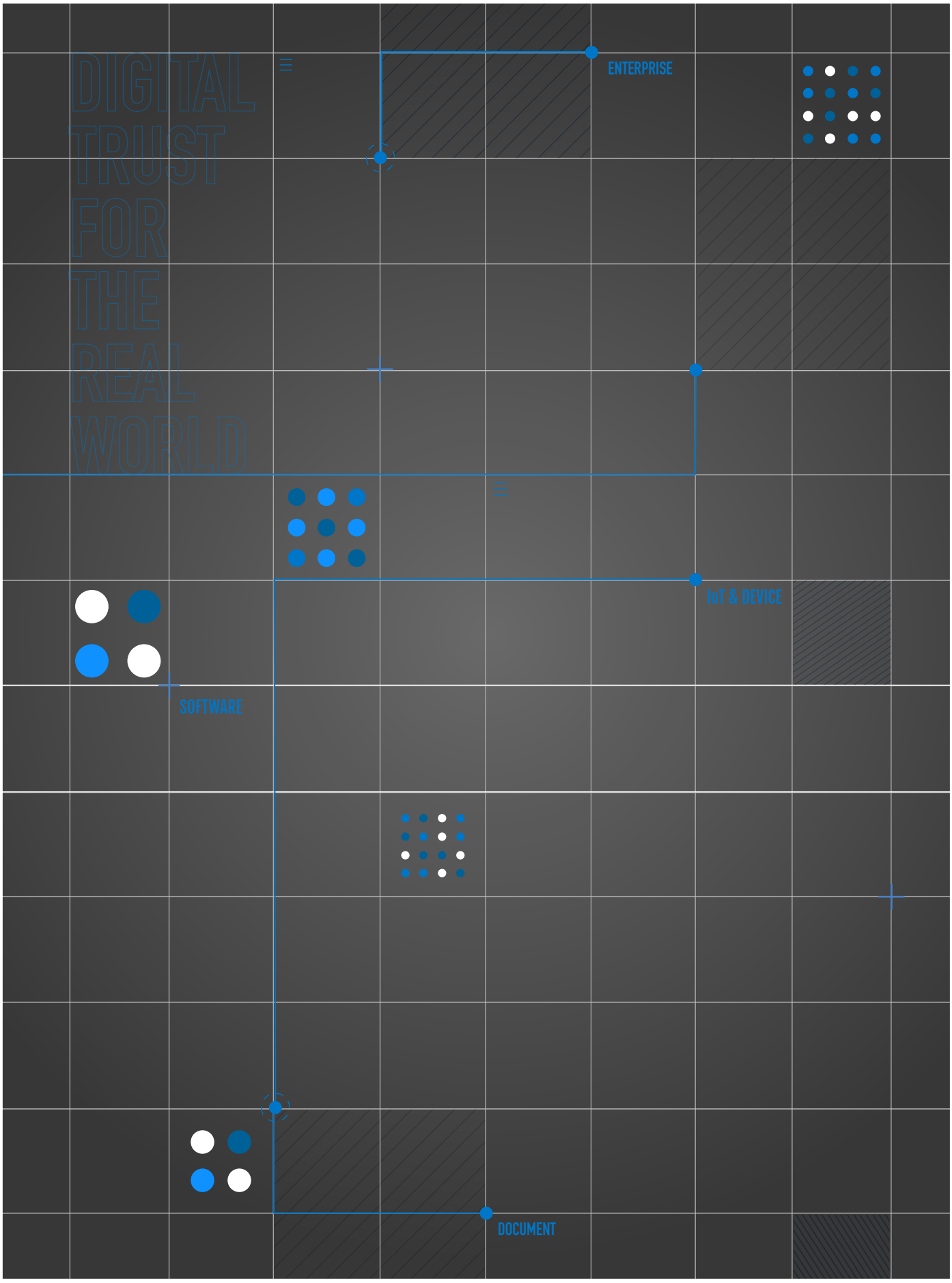
Organizations need some degree of "crypto-agility," or the ability to rapidly update and remediate cryptographic assets. To prevent future disruptions and minimize risk, deploy tools to centrally manage and automate digital certificates and PKI.  This approach offers several advantages, including enhanced security, improved efficiency, and simplified administration.

## Prioritize Based on Business Impact

Review your inventory to identify assets that relate to business-critical applications and processes. These are the areas you want to up-level first. Address any security vulnerabilities before moving to implement solutions to streamline the tasks that support digital trust. For example, allow users to automatically and easily enroll their devices for secure remote access without help from the IT team. Improve cloud security by quickly and securely issuing and installing server certificates to protect data and communications.

## Conclusion

Organizations prioritizing digital trust enjoy stronger brands, lower cybersecurity risks, and operational efficiencies. They instill confidence among customers, partners, and stakeholders through robust security measures and transparent governance. Establishing digital trust enables effective navigation of regulatory complexities, ensuring compliance and reducing legal and financial risks. This safeguards data, enhances resilience, and addresses emerging threats in today's digital landscape.


DIGITAL
TRUST
FOR
THE
REAL
WORLD
ENTERPRISE
IoT & DEVICE
SOFTWARE
DOCUMENT