

STATE OF DIGITAL TRUST

AUTOMATION
433.6°
24567.76°

IoT
ENTERPRISES
EMPLOYEES
CUSTOMERS
6578.854°
6785.77°

PILLARS OF TRUST

C- LEVEL, DIRECTOR,
MANAGER INSIGHTS

DIGITAL TRUST READINESS
SCORE

1245.56°
753234.72°

IDENTITY

THREATS

ID 7021.4

ZERO TRUST

GLOBAL STUDY

NOVEMBER 2022

digicert®

2022年度 数字信任调查报告

我们正迅速从一个人们面对面的世界过渡到一个始终在线的、以数字化方式互联的世界。数字化转型正在推动这一进程。新冠疫情也已为此进程助力。然而，我们如何在这一新世界中建立信任？ 我们如何：

- 确保我们所连接的人（与设备）的合法性？
- 了解我们所消费的数据的安全性？
- 确保我们不会遭受安全漏洞或拒绝服务攻击？
- 确保我们运行的应用程序和服务未遭受攻击？

这并非易事。这一新世界极大地扩展了威胁面，因此安全方面的失误所造成的代价也随之激增。特别是除了您考虑的法律、监管和补救成本之外，最大的代价可能是客户忠诚度和公司品牌的损失。一份Forbes Insights报告显示，近一半（46%）的组织都经历过因第三方安全漏洞而造成声誉和品牌损害¹。

这将数字信任问题推向了前台。IDC研究总监Jennifer Glenn表示，数字信任是保护互联世界的基础，对于希望确保其客户、员工和合作伙伴信任线上业务流程与交互安全性的组织来说，数字信任必不可少。

从本质上讲，数字信任提供了充分参与数字世界的自由。

DigiCert是全球领先的数字信任提供商，它能让个人与企业在参与线上活动时确信，他们在数字世界的足迹是安全的，而且它有责任更好地了解全球组织如何看待数字信任，以及他们在数字信任工作中的进展。

DigiCert 2022年度数字信任状况调查报告探讨了世界各地的企业、员工和消费者采纳数字信任的相关情况。

¹IT风险的声誉影响——Forbes Insights

什么是数字信任？

IDC研究总监Jennifer Glenn表示，数字信任是保护互联世界的基础，对于希望确保其客户、员工和合作伙伴信任线上业务流程与交互安全性的组织来说，数字信任必不可少。

数字信任的基础取决于四大基石：

1. 标准——为某一既定技术或行业定义信任要求。
2. 合规与运营——生成或验证建立信任（通过身份、完整性与加密）的数字证书，并确保这些证书符合标准机构规定的要求。

3. 信任管理——确保企业妥善管理证书生命周期，并能集中了解和管控证书使用。
4. 互联信任——将信任扩展到更复杂的供应链（如软件、设备和内容）。

数字信任来源于这四大基石。企业可能依靠第三方开展上述部分或全部工作，也可能自行开展管理。

“数字信任是保护互联世界的基石。”

—Jennifer Glenn,



数字信任至关重要

对数字信任的需求引起了受访者的共鸣，100%的受访企业表示数字信任是重要的，绝大多数（90%）的受访企业表示数字信任极为重要。事实上，如此重要的是，近三分之二的受访企业在失去对供应商的信任后对供应商进行了更换。而且几乎所有（99%）的受访企业都认为，如果其客户对企业失去信任，就可能会选择企业的竞争对手。近一半（47%）的受访企业认为这一结果是可能的。

企业员工也全都非常重视数字信任，100%的受访员工认为数字信任是重要的，而且86%的受访员工认为数字信任极为重要。就受访员工在企业中的职责而言，99%的受访员工表示如果对供应商失去信任就会考虑更换供应商，大约一半（51%）的受访员工表示“可能”会更换供应商。

最后，三分之二（68%）的受访消费者表示数字信任是重要的，三分之一（36%）的受访消费者表示数字信任极为重要。事实上，一半（47%）的受访者已经停止与其不再信任的企业开展业务。展望未来，84%的受访者会考虑更换合作企业，57%的受访者表示可能会更换合作企业。值得注意的是，消费者越富有，他们就越认可数字信任的重要性（58%的收入高于平均水平的消费者认为数字信任是重要的）。

方法论

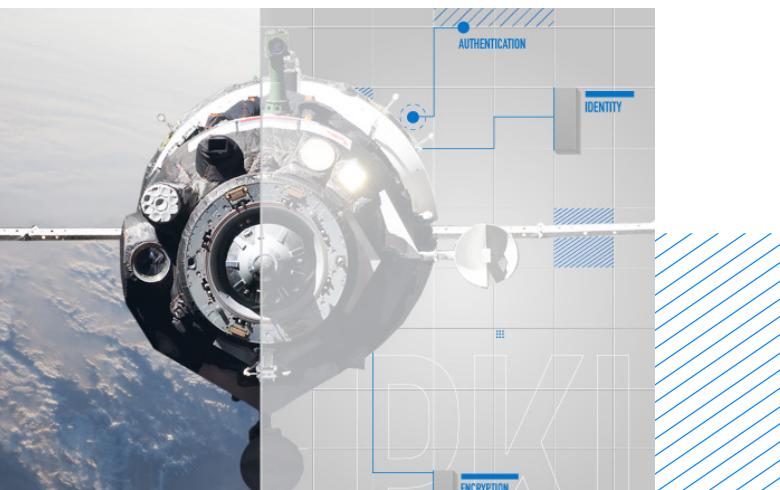
总部位于达拉斯的Eleven Research于2022年9月进行了2022年度数字信任状况调查。本次调查通过向全球400家企业和400名消费者致电或发送电子邮件的方式进行。

企业

400位IT、信息安全和DevOps高级管理人员和企业最高层管理人员接受了调查，他们来自拥有1000名或以上员工的企业。本次调查的回复来自全球各地：图A（见第5页）

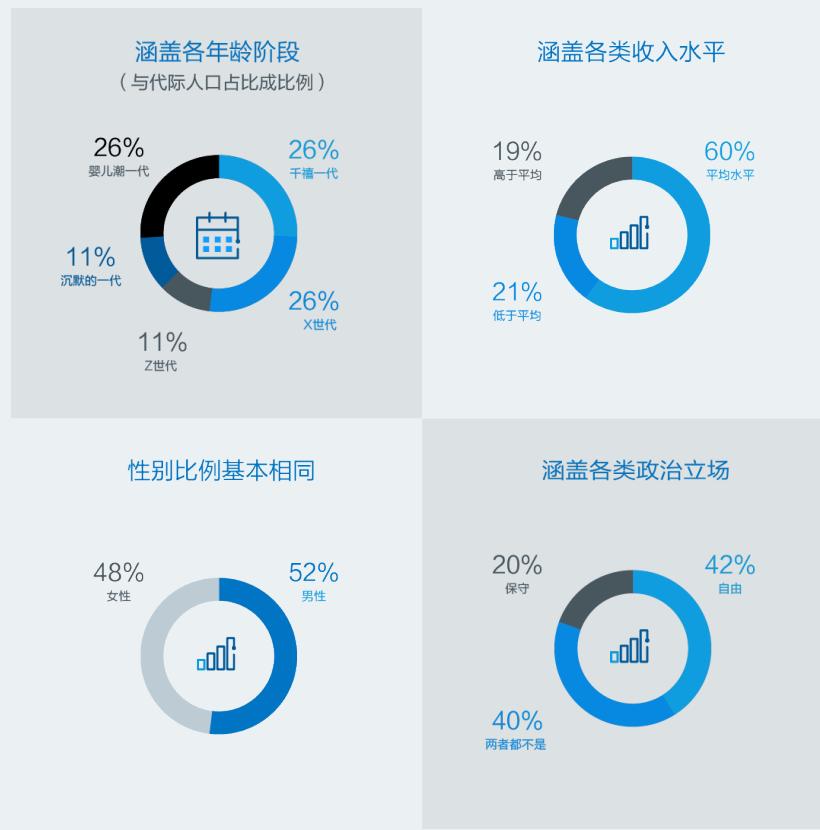
消费者

我们调查了全球400位消费者，（同一地区）涵盖各年龄段、性别、政治取向和经济地位：图B（见第5页）





图A.

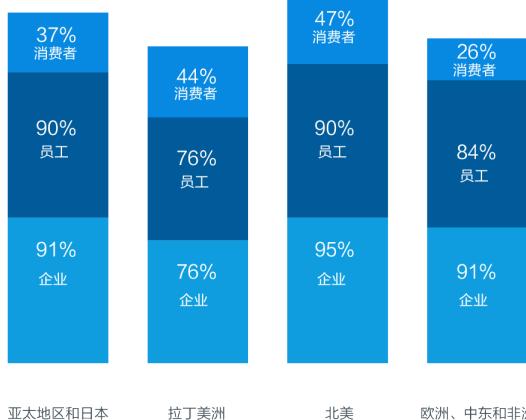


图B.

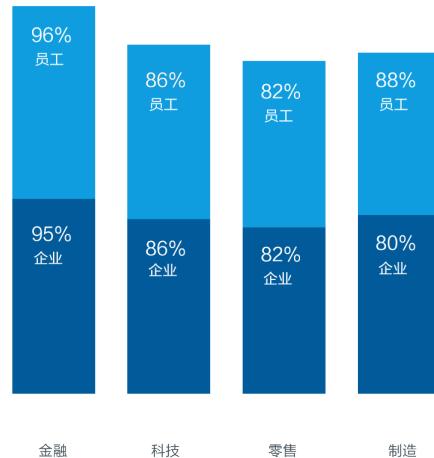
数字信任的重要程度不同

企业、员工和消费者都认为数字信任是重要的，但其重要程度取决于多种属性。

认为数字信任极为重要——按地区



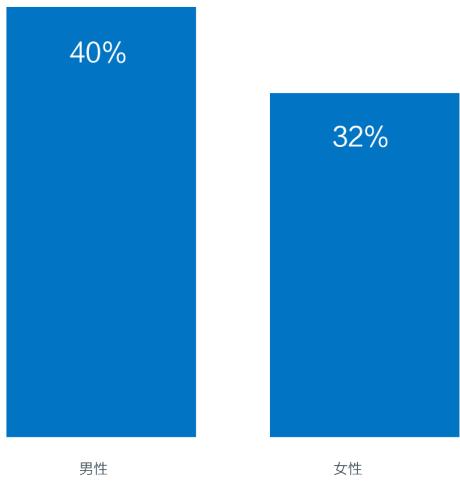
认为数字信任极为重要——按行业



拉丁美洲的受访企业和员工感到数字信任极为重要的比例低于其他地区。亚太地区和日本以及欧洲、中东和非洲的消费者感到数字信任极为重要的比例低于其他地区。鉴于2018年颁布了严格的欧盟GDPR法规，因此仅有26%的欧洲、中东和非洲消费者表示数字信任极为重要这一情况令人惊讶。

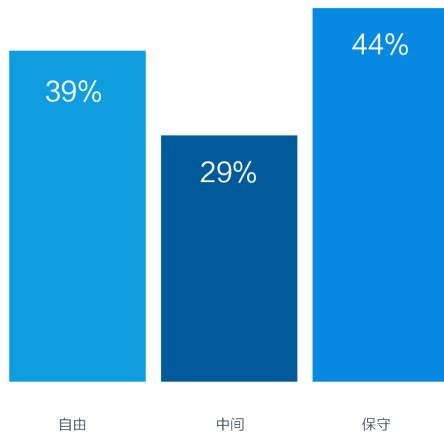
不足为奇的是，金融公司最有可能表示数字信任极为重要。

认为数字信任极为重要——按性别（消费者）



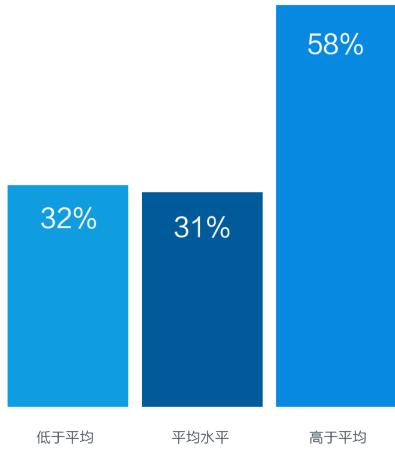
对于消费者来说，相比女性，数字信任对男性更重要。

认为数字信任极为重要——按政治立场（消费者）



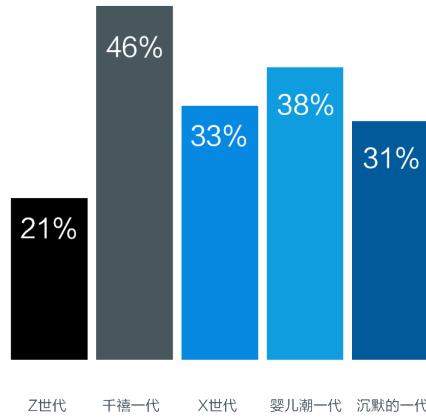
最终，自由派和保守派可以就数字信任的重要性达成共识！两者都更有可能表示数字信任极为重要。

认为数字信任极为重要——按收入（消费者）



此外，对于收入高于平均水平的消费者来说，数字信任的重要性要高得多。

认为数字信任极为重要——按代际（消费者）



有意思的是，最年轻的两代人（也是唯一的数字原生民）中一代最不可能表示数字信任极为重要，一代最有可能表示数字信任极为重要。

是什么推动了对数字信任的兴趣？

人们普遍对数字信任感兴趣，但这是为什么？是什么推动了这种兴趣？我们发现了多种因素。

数据的重要性与日俱增。受访者称，这是最主要的推动因素。为什么？因为数据在以23%的复合增速增长²。换句话说，截至2021年底，全世界用了70年的时间收集了97泽字节（ZB）的数据。到2025年，仅仅四年后，世界的数据量就将近乎翻番（174ZB）。这相当于到2025年地球上人均数据量将超过20000GB！

然而，这不仅在于数据的数量，还在于这些数据的重要性。数据包含大量的个人身份信息，比如我们购买的东西、访问的网站、病历、社交媒体、照片等许多内容。

扩大的威胁面。企业已将其相对静态的数据中心、办公室和远程站点网络转变为更复杂的混合网络。这些新型网络连接数据中心、办公室和远程站点，同时增加数千个居家办公站点、多个云端、数字设备、边缘网络和物联网（IoT）设备。

在这一全新的无边界网络中，攻击点呈现数量级的增加。

客户的期望。正如我们在上一节中看到的，100%的企业和68%的消费者认为数字信任是重要的。如果他们对某家企业失去信任，就都可能会选择该企业的竞争对手。数字信任已经成为一种存在的资产。

恶意分子的增加。恶意分子的数量逐年增长。他们包括：

- 黑帽子黑客
- 网络犯罪分子
- 网络恐怖分子
- 激进黑客
- 内部恶意分子
- 民族国家激进分子
- 寻求刺激者和恶意挑衅者

2021年IC3收到的投诉数量创下历史记录，证明了恶意分子的增加：847,376宗投诉，比2020年增长7%³。



²大数据的大幅增长预测——IDC

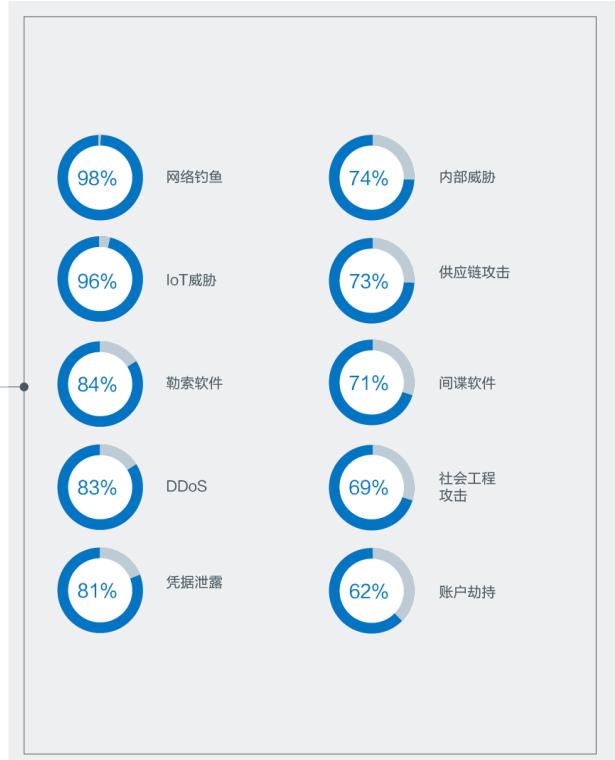
³FBI网络犯罪投诉中心（IC3）

什么处于危险之中？

企业在保护什么？100%的企业受访者认为客户忠诚度是重要的。若您考虑如果客户对某家企业失去信任，他们有多大可能会转而选择企业的竞争对手时，这是有意义的。

受访者告诉我们，他们最害怕的攻击类型是（按顺序排列）：

对于企业……

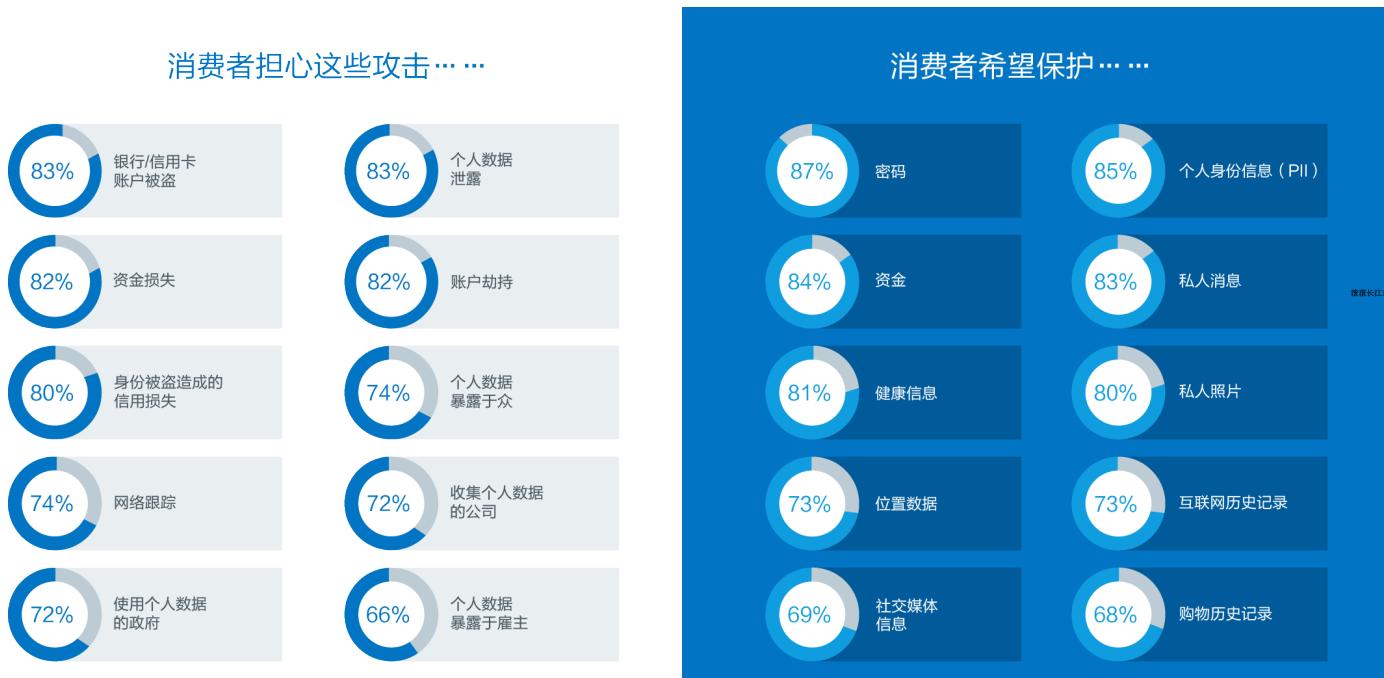


企业员工有不同的关注点：他们的个人信息。

对于员工……

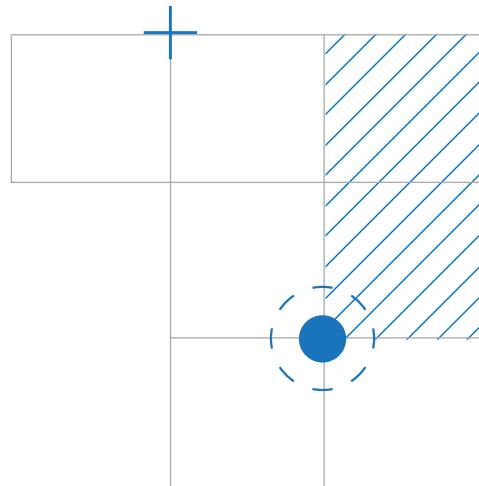


最后，消费者的关注点更为广泛：



我们想知道，在帮助保护对消费者而言最重要的事项（密码、个人身份信息（PII）等）方面，企业是否与消费者站在同一立场。几乎所有危害消费者数据的攻击都始于电子邮件攻击⁴。然而，尽管企业为保护消费者做了各项工作，但他们将其在防范网络钓鱼方面的表现评为倒数第二。此外，他们将网络钓鱼评为其最担心的攻击。

因此，尽管企业专注于对消费者而言最重要的事项，但他们必须始终达到消费者希望看到的安全级别。

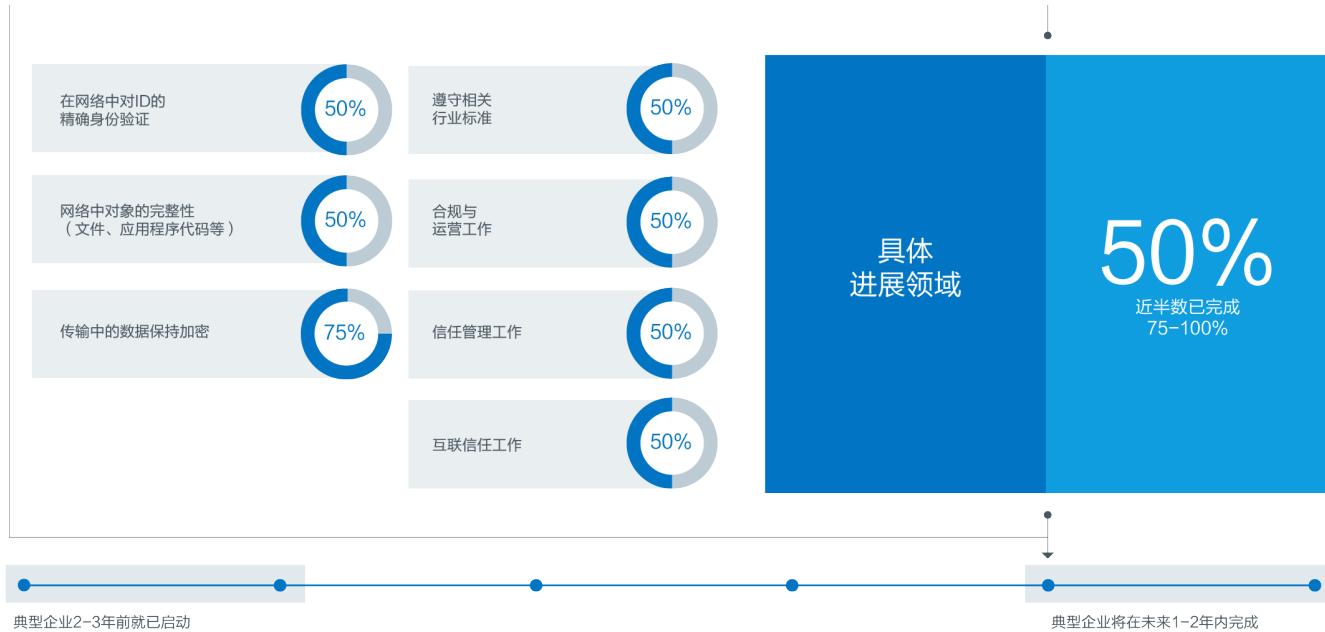


⁴为什么您的企业需要更好的电子邮件安全性——Guardian Digital

企业如何优化数字信任？

企业正在参与数字信任。典型的组织已经在两到三年前就开始了与数字信任相关的工作，并且到目前为止已经完成了75%（或更多）的目标。典型的组织将在未来一到两年内完成其数字信任之旅。

数字信任有很多方面。我们来进一步深入了解企业将在哪些方面走得更远。



数字信任目标：企业明确表示，数字信任的首要目标是客户忠诚度。100%的受访企业认为这一目标很重要，使其成为企业的首要目标。但还有其他目标。



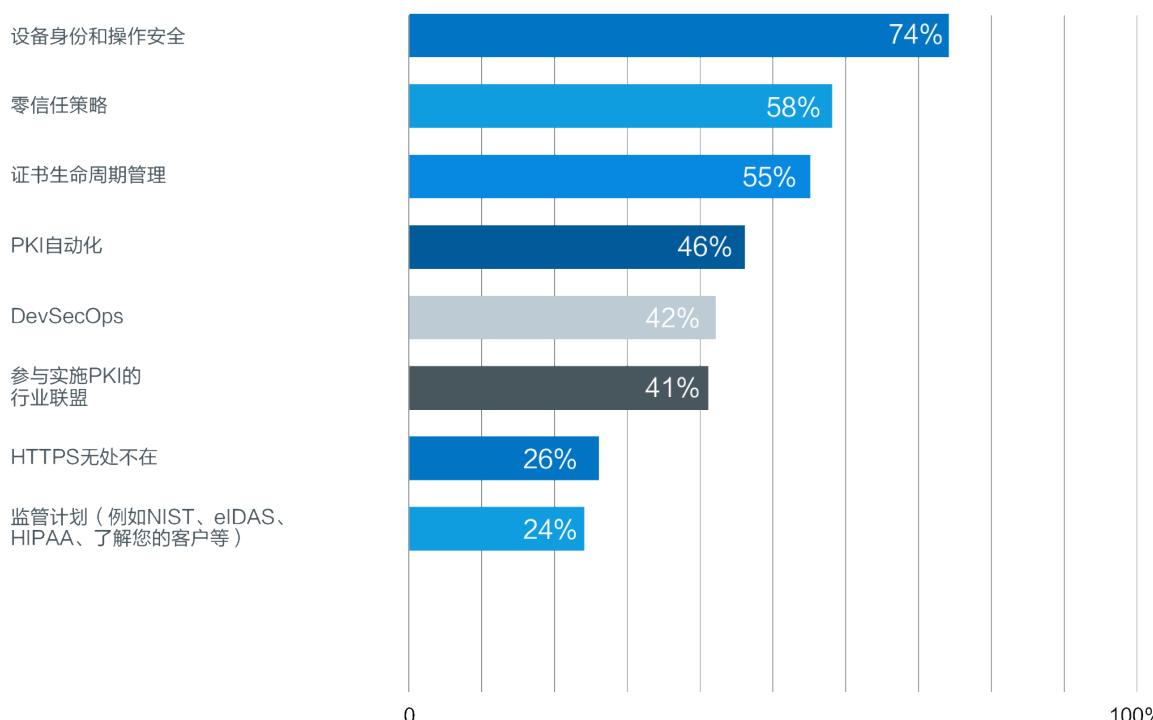
数字信任挑战：企业在其数字信任之旅中进展顺利，但这并非易事。IT部门提到的头号挑战是管理数字证书，100%的受访企业认为管理数字证书是重要的。遵守法规以及处理他们所保护的大量内容紧随其后，达到99%。挑战还包括复杂性——保护一个复杂、动态的多供应商网络——以及员工专业知识的缺乏。



数字信任实践：多种新方案都会影响企业的数字信任。大多数企业至少在一定程度上参与了这些方案，然而，真正有帮助的是要看看企业已经全面实施了哪些方案。

最重要的是设备身份和操作安全性，目前已被74%的企业全面实施。零信任策略排名第二，但仅被58%的企业完全实施。被超过一半的企业（55%）实施的唯一一个其他方案是证书生命周期管理。具体信息列示如下：

**问题22：贵组织对以下数字信任实践的参与程度如何？
(已实施)**

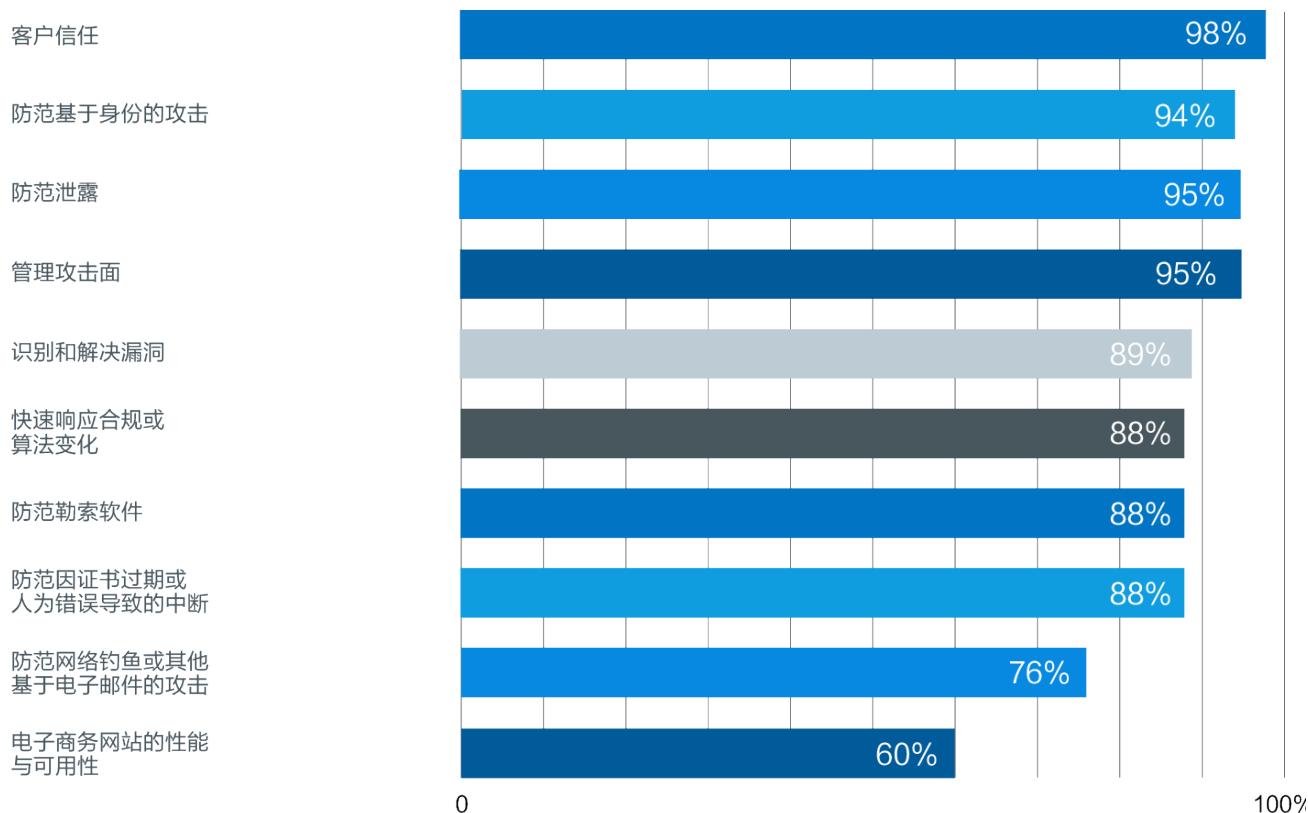


企业在数字信任指标方面表现如何？

企业在多种数字信任目标指标方面表现良好。以其首要目标（客户信任）为例。98%的受访企业在这个目标方面表现出色（61%的受访企业表现极好）。他们在防范漏洞（95%，51%表现极好）和基于身份的攻击（94%，50%表现极好）方面也有出色表现。

事实上，对于我们研究的十个指标中的八个指标，八家受访企业中至少有七家企业表示他们表现出色。落后的两个指标只有防范网络钓鱼或其他基于电子邮件的攻击，以及电子商务网站性能与可用性（分别为76%和60%）。

**问题23：贵组织在以下每个数字信任指标方面的表现如何？
(比较好/极好)**



客户正在看到改进

所有（100%）的受访企业都表示数字信任对其客户是重要的，其中91%的企业表示其客户认为数字信任极为重要。

因此，有必要评估客户对数字信任的看法。从企业的角度来看，这是一个好消息，99%的受访企业表示，相比过去，现在他们的客户对企业的数字信任更有信心。近四分之三（73%）的受访企业表示，客户信心提高幅度很大。

那么，企业的感受如何？他们也这么乐观吗？事实上，数字几乎相同。当被问及企业对与其交互的其他企业的信心时，98%的受访企业表示相比过去，现在他们更有信心，而且76%的受访企业则表示信心提高幅度很大。

但这是B2B交互的情况。B2C的情况怎么样？这里的数字没有B2B那么乐观。不到一半的受访者表示，他们对与之打交道的组织的数字信任度高于过去，同时54%的受访者表示还有改进的空间。

“91%的客户认为数字信任极为重要。”



北美地区的结果

北美地区（美国和加拿大）的受访者认为数字信任极为重要的比例全球领先。企业、员工和消费者都是如此。

值得注意的是，相比除亚太地区之外的世界其他地区的消费者，北美消费者最担心网络威胁（例如银行账户或信用卡被访问及资金被盗）。（91%的亚太地区消费者对这些威胁表示担忧对比北美地区的85%，欧洲、中东和非洲的77%，以及拉丁美洲的78%。）

消费者给北美企业的高分显示了这一点。就数字信任是否成功而言，31%的北美消费者表示，他们对与其有业务往来的企业的信任度明显提高。亚太地区消费者如此认为的比例居中，为19%。相比之下，拉丁美洲消费者如此认为的比例为24%，亚太地区消费者的比例如为19%，欧洲、中东和非洲消费者的比例如为15%。

亚太地区的结果

总体而言，亚太地区认为数字信任极为重要。相比除北美之外的任何其他地区，他们更注重数字信任。

其部分原因是，亚太地区的消费者比世界其他地区的消费者更担心网络威胁（例如银行账户或信用卡被访问及资金被盗）。（91%的亚太地区消费者对这些威胁表示担忧，对比北美地区的85%，欧洲、中东和非洲的77%，以及拉丁美洲的78%。）

就数字信任是否成功而言，19%的亚太消费者表示，他们对与其有业务往来的企业的信任度明显提高，这一比例居中。北美地区和拉丁美洲消费者的比例如是31%和24%，而欧洲、中东和非洲消费者的比例如为15%。

拉丁美洲的结果

总体而言，拉丁美洲认为数字信任极为重要的比例落后于世界。

其部分原因是，拉丁美洲的消费者比大多数消费者更不担心网络威胁（例如银行账户或信用卡被访问及资金被盗）。（仅有78%的拉丁美洲消费者担心这些威胁，对比91%的亚太地区消费者、85%的北美消费者和77%的欧洲、中东和非洲消费者。）

就数字信任是否成功而言，24%的拉丁美洲消费者表示，他们对与其有业务往来的企业的信任度明显提高，这一比例相对较高。相比之下，北美消费者的比例如为31%，亚太地区消费者的比例如为19%和15%。

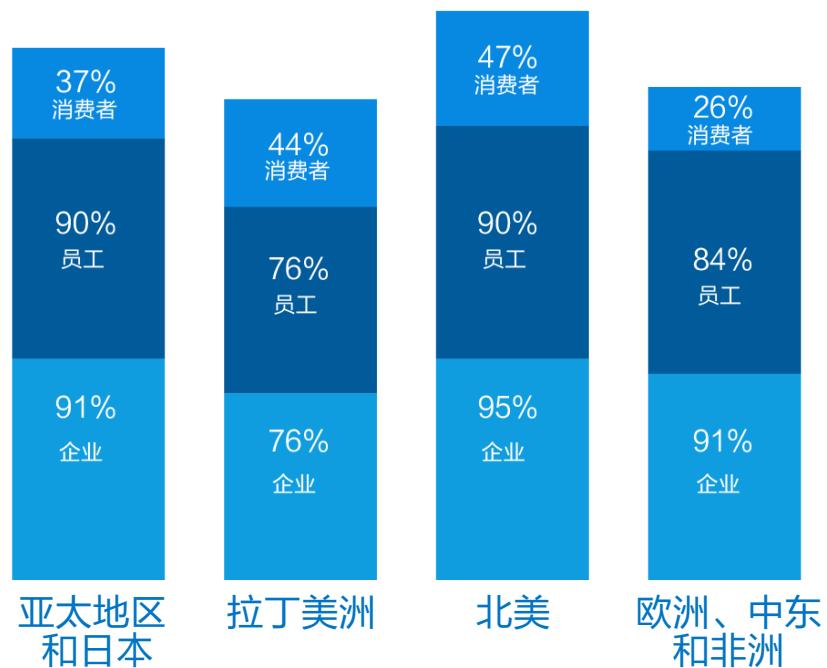
欧洲、中东和非洲的结果

对于这个实施了一些最严格的隐私法规（GDPR）的地区来说，欧洲、中东和非洲消费者对数字信任的淡漠让人惊讶。总体而言，欧洲、中东和非洲在评价数字信任的重要性方面排名第三。然而，如果您深入研究数据就会发现，欧洲、中东和非洲在企业层面对此关注程度较强，在员工层面对此关注程度居中。在消费者层面，我们看到有关数字信任重要性的比例几乎只有北美地区的一半。

这与对网络威胁的担忧有关。欧洲、中东和非洲消费者对银行账户或信用卡被访问及资金被盗等网络威胁的担忧程度最低。仅有77%的欧洲、中东和非洲消费者担心这些威胁，相比之下，拉丁美洲消费者的比率为78%，北美消费者的比率为85%，亚太消费者的比率为91%。

这也与以下相对较低的比例相关：仅有15%的欧洲、中东和非洲消费者表示近年来他们对与其有业务往来的企业的信任度有所提高。这落后于亚太地区（19%）、拉丁美洲（24%）和北美地区（31%）。

认为数字信任极为重要——按地区



数字信任专家的榜样

如上一节所示，企业似乎在数字信任方面表现出色。我们想看看这是否是普遍现象，还是有一部分企业的表现明显好于或差于平均水平。

为了探究这一点，我们对受访者给指标问题的答案进行了评分：

评分指南

| | |
|--------|----|
| 极差 | -2 |
| 较差 | -1 |
| 既不差也不好 | 0 |
| 较好 | +1 |
| 极好 | +2 |

然后，我们将三个单独的分数相加，为每个受访者创建一个总分。我们将受访者分为三个层级：

企业数字信任层级

顶层（得分在所有受访者中排前三分之一）

中层（中三分之一）

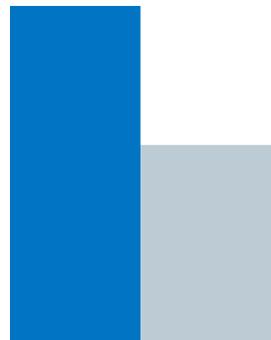
底层（后三分之一）

这种分层展现了最好的企业（顶层）和最差的企业（底层）之间的一些显著差异。

更出色的程度如何

顶层企业在数字信任指标方面表现更出色是显而易见的，因为我们就是使用这种方法将受访者分为几个层级。然而有意思的是，顶层企业比底层企业的表现出色多少。例如，在电子商务网站的性能与可用性方面表现出色的顶层企业数量是底层企业的三倍，表示在防范网络钓鱼或其他基于电子邮件的攻击方面表现出色的顶层企业数量是底层企业的2.9倍。对于每一个指标，顶层企业的出色程度都要高10%到300%不等：

1.7倍



相比底层组织，
顶层组织的客户
信任组织的可能性要高得多。

²大数据的大幅增长预测——IDC

³FBI网络犯罪投诉中心 (IC3)

在数字信任方面，最好的企业比最差的企业要好得多



为什么顶层企业表现这么出色？

顶层企业和底层企业之间存在着各种显著的差异，正是这些差异造成了数字信任结果的巨大差异：

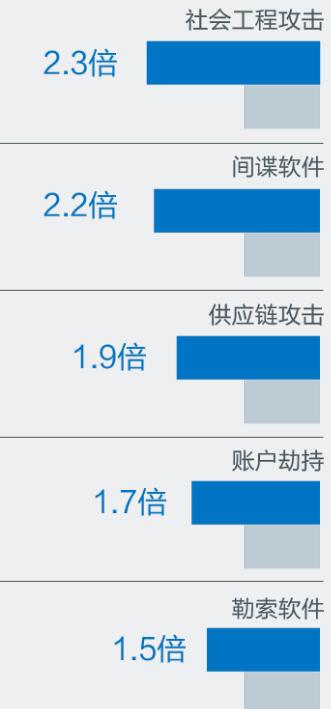
- **态度：**顶层企业认为失去客户信任将导致该客户流失的可能性是底层企业的4.5倍。他们也更可能认为数字信任会影响其品牌、销售和利润。此外，顶层企业表示如果对合作伙伴失去信任就会更换合作伙伴的可能性是底层企业的5.6倍。
- **提前启动：**领先企业在其数字信任之旅中走得更远，而且将比落后企业更早地完成其数字信任之旅。

- **更关注网络威胁：**领先企业更重视网络威胁。顶层企业关注网络威胁的可能性是底层企业的1.5至2.3倍。
- **更多地采用常见的网络安全措施：**顶层企业采用重要网络安全措施的可能性是底层企业的三倍。

顶层企业参与以下事项的可能性要高多少：



顶层企业更关注一些重要的网络威胁：



数字信任应该由谁负责管理？

确定数字信任在企业组织中应该由谁负责管理是一项重要决策。在这个问题上，顶层企业和底层企业之间存在着明显的意见分歧。

绝大多数顶层企业表示，首席信息官应该在IT组织中管理数字信任，而底层企业则持不同意见，认为安全运营部门应该对数字信任进行管理。

这并不是对安全运营部门及其职责的轻视，安全运营部门及其职责对于组织而言至关重要。这应该被视为确认首席信息官了解其组织更广泛的技术足迹，以及数字信任对技术驱动型组织的成功有多重要。这一发现反映了顶级企业对数字信任的战略考量。

DIGICERT的见解

DigiCert是全球领先的数字信任提供商，它能让个人与企业在参与线上活动时确信，他们在数字世界的足迹是安全的，DigiCert从最初期就参与了数字信任工作。对于希望效仿顶层的“数字信任专家”所展示的出色表现的企业，我们的建议是考虑开展以下五项工作：



让数字信任成为战略要务。这是顶层企业与其他企业的明显区别之一，顶层企业认识到了数字信任会影响品牌、客户忠诚度、收入和利润等重要业务成果。



在贵组织的技术口建立数字信任办公室，明确指定一位领导，并为该领导授予决策权。



认识到贵企业的用户（包括消费者）对数字信任的意识正在提高，而且您在业务上的成功和声誉与您确保高水平数字信任的能力直接相关。

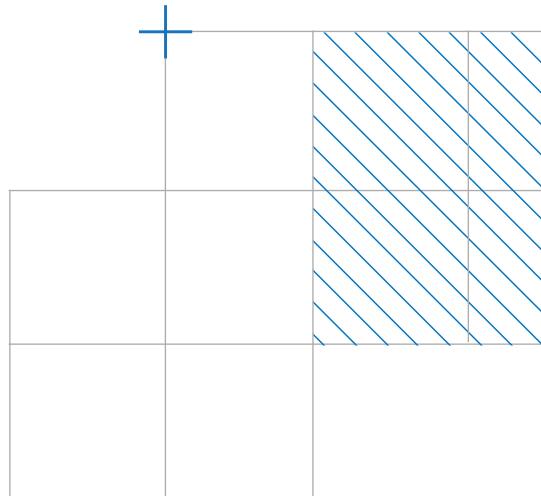


在您寻求数字信任的过程中寻求专家帮助。企业提到的数字信任挑战之一就是缺乏员工专业知识。确保您选择的合作伙伴拥有覆盖数字信任各大基石的全面产品组合，并能够为您的整个组织提供统一的信任管理解决方案。



请牢记——您的客户关注数字信任。与他们建立清晰的数字信任沟通渠道，不仅介绍贵公司对数字信任的承诺，还介绍贵公司在这方面的进展。

这与贝恩公司的一项著名研究一致⁵，该研究发现，客户保留率提高5%，利润将提高25%至95%。鉴于客户失去对企业的信任后其远离企业的可能性之大，最大程度实现数字信任应该是一项必须要开展的工作。



⁵削减成本的方法——贝恩公司

