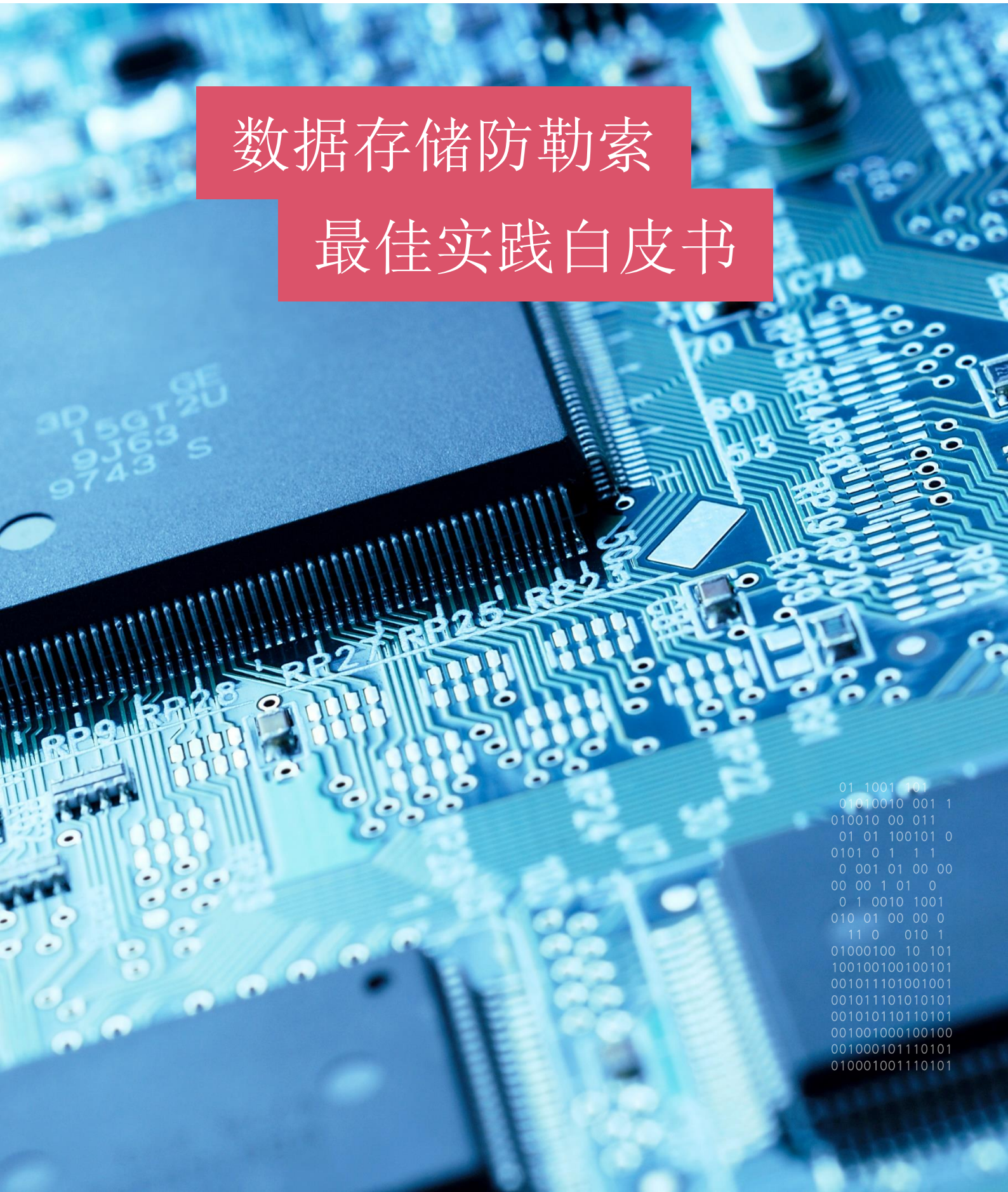
pwc 普华永道

HUAWEI

数据存储防勒索
最佳实践白皮书



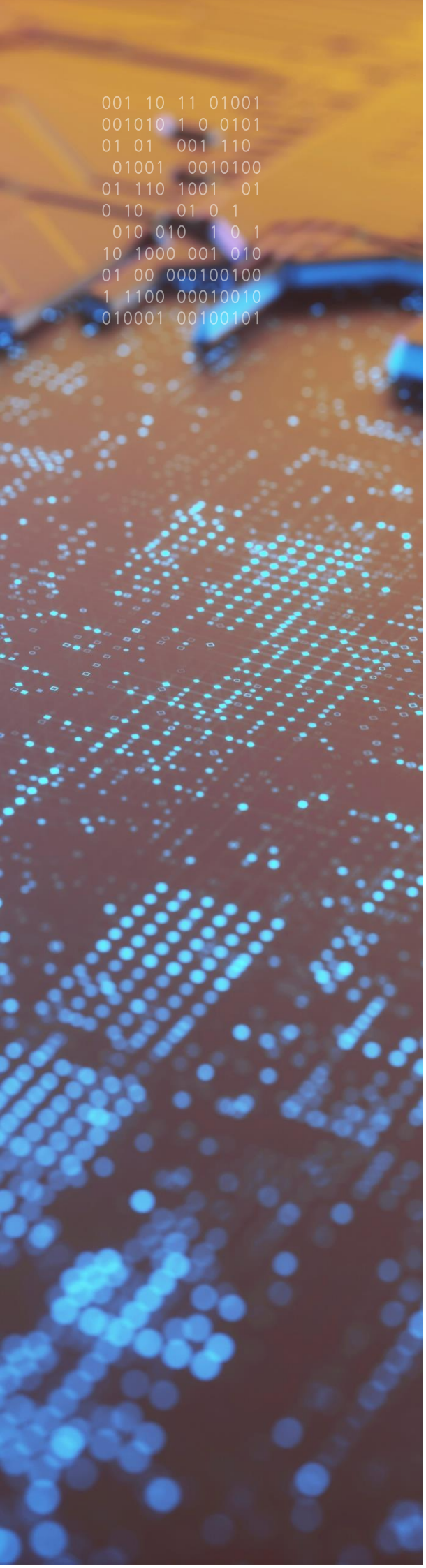
声明

未经普华永道咨询（深圳）有限公司（以下简称“普华永道中国”）和 /或香港华为国际有限公司（以下简称“华为”）的书面许可，任何机构和个人不得基于任何商业目的使用本白皮书中的信息(包含报告全部或部分内容) 。如果任何机构和个人因非商业、非盈利、非广告的目的需要引用本报告中内容，需要注明 “转载自普华永道咨询（深圳）有限公司和香港华为国际有限公司联合发布的《数据存储防勒索最佳实践白皮书2023》。

本白皮书仅提供一般性信息之目的，不应用于替代专业咨询者提供的咨询意见。由于每个客户的需求不尽相同，普华永道中国和 /或华为鼓励每个受监管的机构/企业可根据相关法律法规要求，以及其业务相关的其他适用法律法规，来获取适当的实施建议。在作出任何决定或采取任何行动之前，您应该咨询专业顾问，并向其提供与您特定情况相关的所有事实。

本白皮书的信息来源于本次调研所收集的数据以及公开的资料，普华永道中国和 /或华为对信息的完整性、准确性或及时性概不做出任何保证或担保，也不提供任何明示或暗示的担保，包括但不限于对业绩、适销性和适用于特定用途的担保，在不同时期可能会得出与本白皮书不一致的观点。

本白皮书仅供一般参考使用，不构成具体事项和咨询意见，普华永道中国和 /或华为不对本白皮书内容承担审慎责任，并且未就本白皮书内容做出任何明示或暗示保证。普华永道中国和 /或华为不就本白皮书内容向任何人士承担任何责任或义务，也不向任何人士承担因本白皮书所引起的或与本白皮书有关的任何责任或义务。读者不应依赖本白皮书内容做出投资或其他商业决定。如需具体意见，请咨询专业顾问。



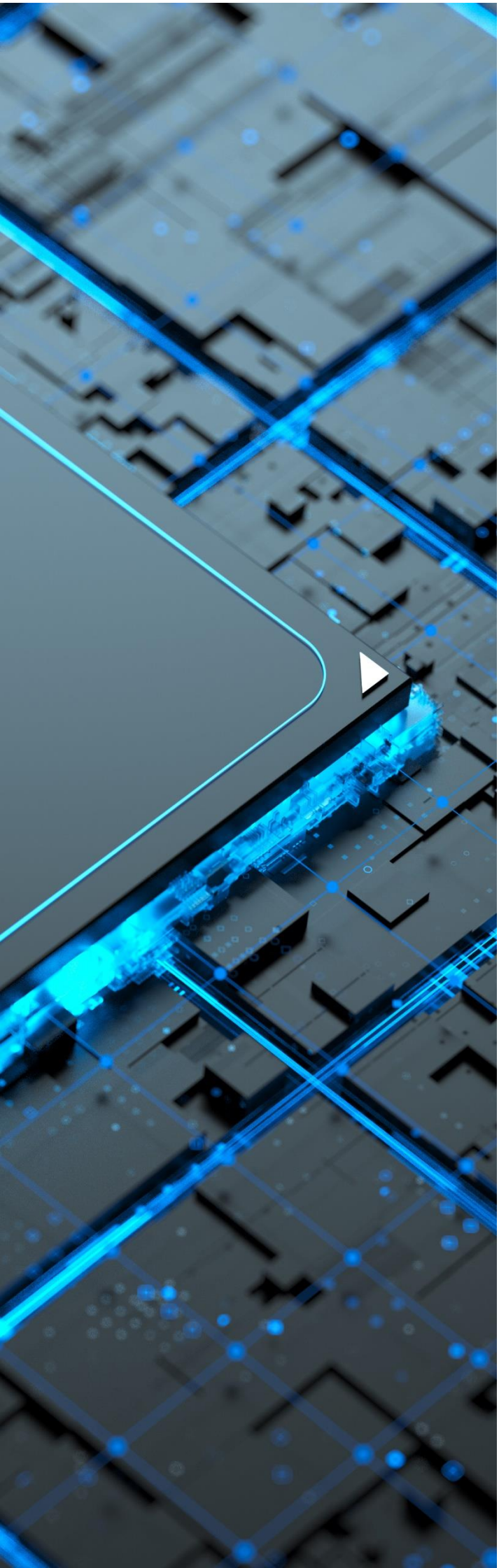
目录

前言

全球数字化革命正在以迅猛的速度重塑经济发展与生产生活方式，5G、人工智能、区块链、云计算、物联网等新兴技术得到了快速普及和广泛应用，近年来勒索软件作为最流行和最持久的恶意软件之一，在国内外的攻击态势日益严峻，近期发生的勒索事件已经对国内外政府、高校、医院和各行业领域核心企业造成了严重的影响。

加密数据勒索是勒索犯罪中最常采用的手段，勒索者往往通过加密企业核心系统内的重要数据，例如机密文文件数据等，胁迫企业支付赎金以恢复数据。目前攻击者已开始将攻击目标转向企业的内部备份和恢复系统，以提高勒索攻击的成功率。

因此，面对勒索软件的攻击，一方面，需要提高网络侧的防护能力，减少被攻破的可能性；另一方面，需要提升数据安全的韧性能力，当网络侧漏防时，应采取有效措施防止数据被加密，及时预警勒索软件的攻击行为，以及当生产数据遭到加密，甚至整个数据中心被“污染”后，保留一份完整、干净的数据副本，以备及时有效地恢复业务系统。



随着全球范围内针对政府机构和关键信息基础设施的网络攻击日益增多，多个国家及地区开始通过立法手段来促进提升企业及机构的网络安全预防能力。

- 2020年11月，美国众议院金融服务委员会资深共和党人Patrick McHenry提出了《Ransomware and Financial Stability Act》(勒索软件和金融稳定法案)，旨在加强对勒索软件的打击和防范，保护金融机构和个人用户的数据安全。

- 2021年8月，澳大利亚联邦的议会发布《Ransomware Payments Bill 2021》（勒索软件付款法案2021），该法案的目的是通过获取更准确地信息来了解勒索软件的威胁和产生的成本，以此加强澳大利亚的网络安全。

- 2021年4月，香港银行协会（HKAB）制定并发布了《Secure Tertiary Data Backup Guideline》（STDB）。该指南涵盖了8项高层次原则，分为治理、设计和数据恢复，被视为增强香港金融机构网络弹性和数据安全的有效措施。

本白皮书概述了我们对当今网络安全形势的观察和理解，包括对近年来勒索软件攻击的趋势和国内外相关案例的分析，并分享基于数据存储及备份系统的防勒索最佳实践及应用实例。

1

勒索软件最新趋势及案例分析

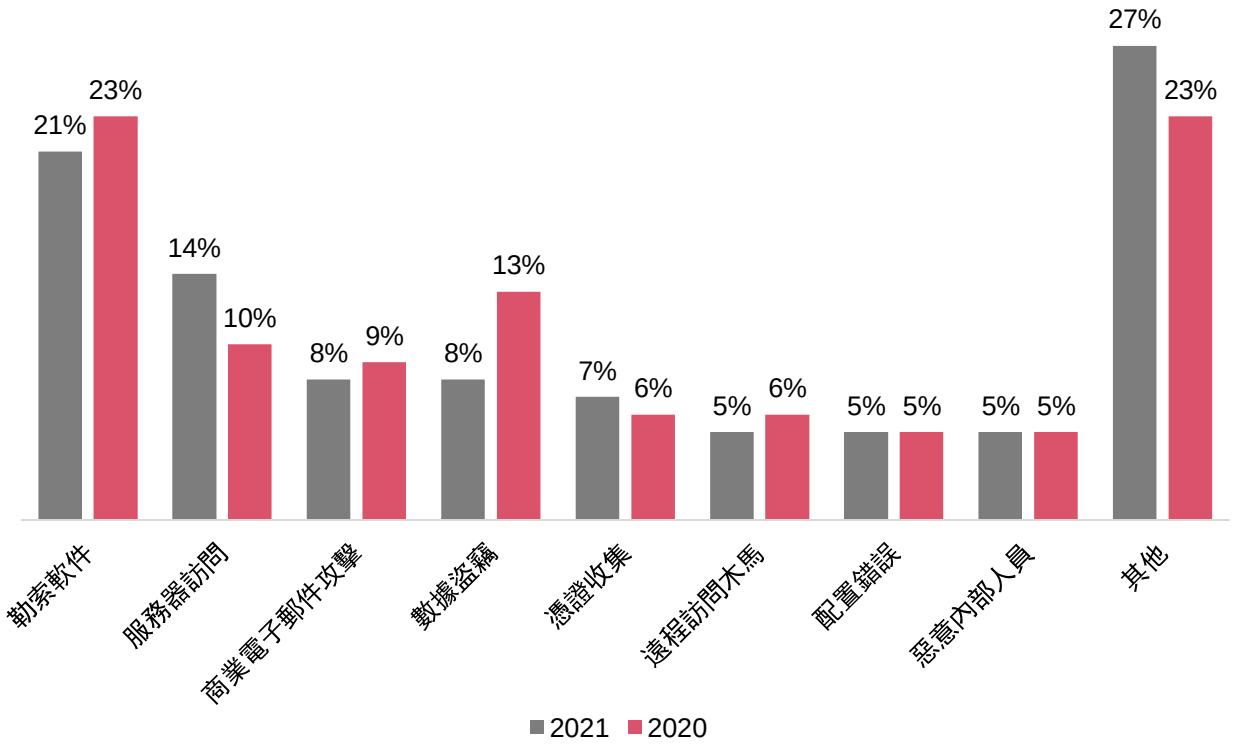
1.1 不断发展的网络安全格局

全球数字化革命正在以迅猛的速度重塑经济发展与生产生活方式，随着数字化转型成本的持续降低，企业数字化转型不再是一种奢侈品，而是企业保持竞争力和提升行业创新相关性的必要条件，与此同时，新技术的应用也伴随着新的网络安全风险。

新型冠状肺炎的流行加速了数字化转型步伐，远程办公的兴起促使企业拥抱云技术，传统的网络边界和范围变得模糊，威胁边界从机构内部办公场所扩充至与机构网络安全防护程度不同的普通公用、家用场所设备中，不断扩大的攻击面成为了网络罪犯攻击的新目标。

近年来，随着勒索软件即服务（RaaS）模式的日渐成熟，勒索攻击的技术门坎越来越低，由此导致了全球勒索软件攻击势头急剧上升，IBM《X-Force 威胁情报指数（2022）》[1]显示，目前勒索软件已成为大多数组织面临的首要网络威胁之一。

图表1：2021年与2020年的主要攻击类型对比[1]

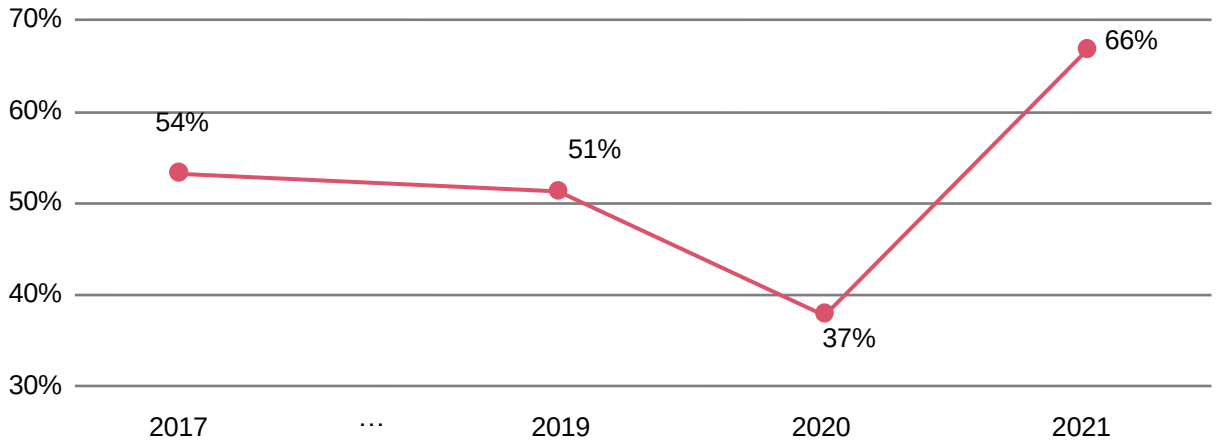


[1] IBM, '2002年度X-Force 威胁情报指数', IBM Security, February 2022

1.2 勒索软件的态势

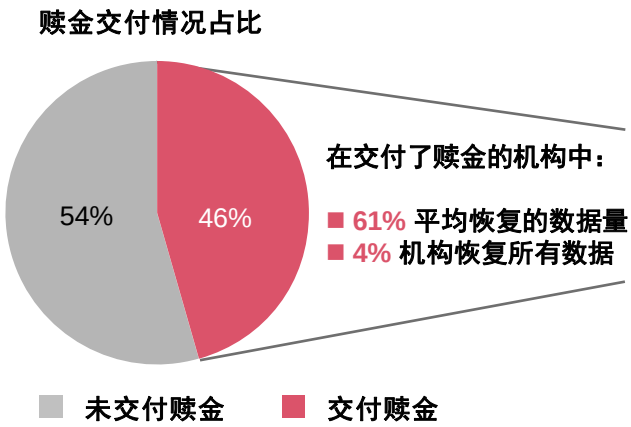
据全球网络安全最佳实践公司Sophos发布的年度勒索软件态势报告 ，在针对来自各规模机构的5000多位IT专业人士的调查中显示，2021年期间遭受过勒索软件攻击的机构比例高达66%，是近几年来的高峰。

图表2：受到勒索软件攻击的机构比例趋势[2, 3]



报告显示，2021年期间被勒索软件成功攻击的机构中，有73%的机构使用了备份数据来恢复数据，同时有46%的机构支付赎金来恢复数据，这反映了很多机构为了提高数据恢复的效率和效果，通常会采用多种数据恢复方式。但采用支付赎金的方式来恢复数据的机构，也并不能保证数据能恢复如初。调查显示，在支付了赎金的机构中，平均能恢复的数据量仅为61%，且极少机构能恢复所有数据（仅占支付赎金机构的4%）。由此可见，依靠支付赎金的方式来恢复所有数据的可能性是很渺茫的。

图表3：受到勒索软件攻击的机构的赎金交付与数据恢复情况[2]



[2] Sophos, 'The State of Ransomware 2022', Sophos Ltd., 20 April 2022, https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

[3] Sophos, 'The State of Ransomware 2021', Sophos Ltd., 19 April 2021, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

1.3 勒索软件案例分析

在国内外网络攻击态势日益严峻，勒索软件攻击范围涉及各种不同规模、地点和行业的企业，其中金融、能源和制造行业是勒索攻击的重点行业，且在近几年里，针对政府、教育、医院等各行业的勒索软件攻击事件也越来越多，由此可见，勒索攻击的目标范围正呈现逐步扩大的趋势。

1.3.1某国政府因勒索软件Conti攻击宣布进入“国家紧急状态”

2022年，某国政府遭受到了来自勒索软件组织Conti的恶意攻击，涉及范围多达27个政府部门，其中包括财政部的税务系统瘫痪，以及财政部的850多GB的数据被盗，在针对海关的攻击中，导致海关进出口控制流程崩溃。Conti加密了政府机构的计算器网络，并勒索政府支付多达2000万美金的“解锁费”，致使该国进入“国家紧急状态”，这也是历史上首例因勒索软件宣布进入紧急状态的国家。

勒索软件Conti于2019年首次被发现，主要因其能够快速加密目标系统而闻名，现已成为网络世界中最具威胁性的勒索软件之一。根据有关网络安全监控服务商的情报分析师表示，勒索软件组织Conti采取了双维度的勒索手段，对政府施加压力：第一，通过加密政府计算器系统对其运行能力造成障碍或瘫痪；第二，若不能按时收到勒索费用，则会泄露政府部门可造成全球性影响的高机密性文件。尽管政府表示不会向Conti支付勒索款，但第三方的网络安全顾问表示此次事件已经对其造成了不可计量的影响。

目前在各国都在加速推进数字化产业及产品的时代，各组织需加大对信息系统保护、数据恢复及勒索软件防范等的资源投入，并提升各层级人员的安全防范意识，以应对网络安全攻击可能造成的严重影响。

1.3.2 某国家银行遭勒索软件REvil攻击被迫关闭所有分行

2020年，南美洲某国国有银行，因内部网络感染REvil勒索软件，致使大部分的内部服务器和雇员工作站被加密而无法运行，其中受影响的计算器多达12,000台。

勒索软件REvil于2019年首次被发现。REvil的其中一种攻击形式，则是通过钓鱼邮件对目标安装木马程序，然后通过横向渗透感染以获取企业的域和服务器权限，从而登录到多台电脑主机后安装病毒。REvil勒索团队以攻击大型机构而闻名，主要通过加密计算器系统或环境，以及威胁泄露个人信息及机密文件而进行双重勒索。

据相关调查人员表示，银行内部网络感染病毒是由于内部员工收到并打开了一份被黑客设置了后门的恶意文档，导致黑客后续在公司内部网络安装了勒索软件。起初，银行尝试在不被发现的情况下恢复相关服务的运行，但由于病毒涉及的范围较大导致银行被迫关闭分支，甚至对其国家的支付和交易产生了影响。

为应对勒索软件，银行聘用了第三方网络安全专家，与警方的信息安全部门保持联系，并适当分割内部网络以限制病毒的再度扩张。据网上流传消息表示，该银行后续可能与勒索团伙进行了谈判。

1.3.3 某墨西哥工厂两年内两次遭遇勒索软件攻击

2020 年 11 月，DoppelPaymer勒索软件组织袭击了某电子制造巨头墨西哥奇瓦瓦州华雷斯城的工厂，在获取了未加密的机密文件后，攻击组织成功加密了超过1200台服务器，并要求支付3400万美元的赎金。随后，DoppelPaymer在其勒索软件数据泄漏站点上发布了窃取的部分文件。

据相关报道称，攻击组织获取了100GB的未加密文件，并删除了超过20TB的备份文件。该企业后续回应称，其内部网络安全团队已完成软件以及操作系统的安全性更新，同时提高了安全防护层级。

该企业两年内发生的第二次勒索软件袭击，是在墨西哥的另一个工厂，位于墨西哥西北边境城市蒂华纳市，该生产工厂在2022年5月下旬遭受了勒索软件的攻击，工厂的运营因勒索软件攻击而中断。该企业没有公布本次攻击期间数据是否被盗，但LockBit 勒索软件组织对外声称从该设施窃取了数据，并威胁如不支付赎金将泄露被盗取的数据。

该企业后续回应声称，本次的网络安全攻击对集团整体运营影响不大，其网络安全团队一直在执行相应的恢复计划。不难看出，经历了上一次勒索软件攻击后，该企业完善了恢复计划以支撑他们的业务维持在正常状态，也将本次攻击造成的影响降至更低。

1.3.4 日本某汽车制造商全球网络遭勒索攻击

据媒体报道，日本某汽车制造商在2020年6月7日发现遭遇勒索软件攻击，当时其美国公司的计算器网络突然中断，并导致工厂被迫停产。该企业被迫关闭其位于美国、土耳其、印度和南美等地的部分工厂以控制干扰，导致生产停顿、产量下降。随后，该企业在对外声明中表示，目前没有证据表明存在个人身份信息泄露，并且已经恢复了大部分工厂的生产，此次的网络攻击不会对其业务产生很大影响。

据该企业工作人员透露，其遭受的网络攻击所使用的攻击软件可能是Snake勒索软件。该勒索软件于 2020年1月首次出现，目前仍处于活跃状态。其主要的攻击目标是工业控制系统（ICS）环境，并且攻击范围针对整个网络环境。它能够停止与工业控制系统（ICS）操作相关的很多流程应用程序。

目前Snake勒索软件的攻击目标已经覆盖了能源、汽车制造、医疗设备经销等多个工业行业，打击工业控制系统已成为其重要目的。

1.3.5 某电力巨头集团多次遭遇网络攻击

2022年10月，某能源供货商集团的安全专家报告称服务器出现了部分问题。与此同时，Everest勒索团伙发布了有关的攻击声明，并声称可以访问该公司的所有服务器，并对其中部分服务器具有root访问权限，以此勒索20万美元。

事实上，这并不是该公司首次遭遇网络攻击了，早在2019年2月也曾遭遇过双重安全漏洞，包括一个包含客户信息的数据库和一台感染了Azorult信息窃取木马病毒的公司计算器，其数据库中的客户信息、经修改后的客户信用卡信息、电表信息等敏感数据均被泄露。经后续跟踪调查披露，被感染的原因竟是员工安装了伪装成游戏安装包的病毒软件。

随着政府、公共服务机构、关键信息基础设施成为勒索软件等恶意程序的攻击目标，其涉及的范围不再局限于个别企业，而是提升至国家安全层面的重要问题。在当前不断变化的国际趋势背景下，多个国家及地区开始通过立法手段来提升地区企业及机构的网络安全标准。

2

全球多国多地区加强网络安全立法

随着新兴信息技术的应用和日益更新，网络安全风险不断升级，在当前不断变化的网络安全局势下，多个国家及地区相继出台了多项网络安全和防勒索软件攻击的相关立法，以促进企业及机构提升网络安全防御能力。

美国

2021年美国相继发生SolarWinds事件、Microsoft Exchange事件和Colonial Pipeline事件等一连串的重大网络安全事件，其中SolarWinds事件更是直接威胁到美国联邦机构和美国各大公司的信息安全，这也直接促使了拜登政府在2021年5月12日签署了《Executive Order on Improving the Nation's Cybersecurity》（改善国家网络安全的行政命令），成为美国当前在网络安全方面最详细的行政命令之一。

2020年11月，美国众议院金融服务委员会资深共和党人Patrick McHenry提出了《Ransomware and Financial Stability Act》(勒索软件和金融稳定法案)，该法案旨在为金融机构提供勒索软件防御和响应指南。法案内容主要包括，当金融机构遭受勒索软件攻击时，应及时通知财政部金融犯罪执法网络（FinCEN），主动提供攻击事件及相关赎金的细节，并做好保密工作。同时，法案对高额赎金的支付规则作出了规定，即金融机构支付的赎金一旦超过10万美元，就需要获得财政部的特别授权。

澳大利亚

澳大利亚联邦的议会发布的《Ransomware Payments Bill 2021》（勒索软件付款法案2021）中要求受害实体必须在向黑客团伙支付赎金之前，通知澳大利亚网络安全中心（ACSC），且支付了勒索赎金的政府部门、企业等实体必须主动将勒索攻击及赎金等相关信息提供到指定执法部门，具体信息包括实体名称和联系方式、攻击者信息、勒索金额、支付类型以及已泄露的数据字段等。

欧盟

在全球数字化和互联程度不断提高的背景下，网络犯罪活动的数量不断增加，欧盟委员会通过的《关于在欧盟全境实现高度统一网络安全措施的指令》（NIS2指令）在2023年1月13日正式生效，其取代了2016年生效的《网络和信息系统安全规则》（NIS指令）。NIS2指令覆盖了更多的关键实体的部门和类型，并加强了企业需要遵守的网络安全监管要求。

中国内地

全球范围内针对关键信息基础设施的网络攻击破坏、窃密等日趋加剧，涉及众多行业领域。在此背景下国务院公布的《关键信息基础设施安全保护条例》，并在2021年9月1日正式生效。条例明确了关键信息基础设施的保护范围，以及对关键信息基础设施运营者在保障稳定运行和维护数据的完整性、保密性和可用性提出了相应的要求。

中国香港地区

金融机构及其客户受益于数字化技术的应用，但同时也带来了新的威胁和风险。为了应对不断升级的网络风险，香港银行协会（HKAB）制定并发布了《Secure Tertiary Data Backup Guideline》（三级安全数据备份指南）。该指南提出的安全原则将帮助银行等金融机构在面对已发生的破坏性网络攻击时及时恢复关键功能、服务和系统。

新加坡

新加坡政府早在2016年的《网络安全战略》中提出加强对关键信息基础设施的网络弹性，并以2018年通过的《Cybersecurity Act》（网络安全法）作为保护关键信息基础设施的立法框架。2021年10月，新加坡政府发布《网络安全战略2021》以应对网络安全的新威胁，其中在基础设施方面提出了加强数字基础设施以及政府系统的安全与弹性，并将保护范围扩大到除关键信息基础设施外的实体与系统。

阿拉伯联合酋长国(UAE)

鉴于快速发展的网络威胁，为应对挑战国家安全和危害关键信息资产的黑客活动，阿联酋电信和数字政府监管局于2020年3月发布了《UAE Information Assurance Regulation》（阿联酋信息保障条例）。该条例为实体建立、实施、维护和持续改进信息保障提供了管理和技术信息的安全控制要求。

随着全球各地区政府逐渐加强对网络安全领域的立法，对企业的运行安全能力也提出了更高的要求。企业应该根据相关指南建立一套适合的政策制度，并采取合理有效的技术手段，以确保遵守不断变化的网络安全标准和要求。

3

数据存储防勒索最佳实践

勒索软件突破企业网络边界防线后，下一个攻击目标即为企业内部存放数据的各种信息系统，生产及备份数据的存储系统就是其中的重点攻击对象，因此，除了网络层的安全防护措施外，数据存储及备份基础架构也需要具备防勒索软件的能力。

完善的数据存储及备份基础架构是企业数据安全的最后一道防线，即使在网络侧防护失效，勒索软件攻击到生产中心，造成整个生产中心被感染的极端情况下，保有一份可用于恢复的安全副本，则可帮助企业恢复业务数据。

3.1 数据存储防勒索最佳实践特性

企业的数据存储及备份基础架构应符合以下的九大特性，以具备足够的网络韧性和数据恢复能力，来应对破环性的网络风险。

防篡改能力

数据备份系统中的数据应保持与它们在存储流程时定义的内容及状态一致，且在保留期间不能被更改或删除。系统应具备数据和活动的完整性控制能力，以确保提取的文件类型和字段值是完整的，且它们的规范是根据源系统中的权威记录进行验证的。

可控性

应配置适当的工具和机制，保障导入数据存储系统的数据完整、准确且无恶意软件或计算器病毒，促进有效的数据导入和提取。

安全隔离区

数据存储系统的备份域应在逻辑或物理上与企业的其他网络、系统、基础设施和数据（包括现有的生产和灾难恢复站点）断开连接形成安全隔离区，以便它能够抵御针对性的网络攻击（如勒索软件或恶意内部人员的威胁），并能维护源数据的准确性。

可恢复性

数据备份系统应能够在不需要诸如备份设备和相关目录提供的中间功能的情况下进行恢复。系统的数据恢复也不应依赖于企业可能受到损害的任何基础设施。

高性能

备份系统的设计应配置大规模并行处理（MPP）和实时流数据的加载来提高运行效率。

安全性

应配备适当的预防性控制措施（如访问控制和管理）、检测性控制措施（如日志监控和实时警报）并制定相应流程，以确保数据的机密性、完整性和可用性。

可验证

应建立适当的控制措施和流程，以验证数据在整个生命周期中的状态，并检测篡改或其他形式的数据损坏。

保障性

应制定适当的控制措施和流程，以减少误报。例如，可能需要至少两个经过认证和授权的资源来启动恢复过程。

异构性

备份系统的设计应不同于企业生产环境的设计，以减少攻击者利用类似漏洞、设计缺陷或错误配置的可能性。

3.2 数据存储防勒索防治策略与技术

企业应在数据存储及备份基础架构中配置防勒索技术措施，包括加密技术、数据防篡改技术、检测分析等能力可保证存储内部数据免遭篡改或删除，并可同样通过建立隔离区保证数据安全，以便我们在遭受勒索攻击的时候能快速恢复安全数据，确保企业的正常运营。

我们根据行业针对勒索软件的相关研究报告[4]，以及关于勒索软件防范措施的介绍，在此总结分享了勒索软件攻击的全路径，以及各路径节点下的防治策略与技术参考。

图表4：勒索软件的攻击路径解析[4]

[4] McAfee, 'Understanding Ransomware and Strategies to Defeat it', McAfee Labs, March 2016

入侵阶段：

建立“人为防火墙”：

员工的安全意识是预防勒索软件攻击最薄弱的环节，企业应定期对员工进行针对性防勒索攻击的培训。

阻止勒索软件到达端点：

端点是指可以接收信号的任何设备，包括台式机、笔记本、路由器和打印机等，以及企业的其他物联网设备。保护网络免受勒索软件攻击的最积极的方法是首先防止勒索软件到达端点，应确保所有设备都具有安全配置，不存在安全漏洞。

系统更新和安全补丁：

勒索软件利用操作系统或应用程序中的漏洞感染端点，因此及时更新操作系统和应用程序安全补丁可以将攻击面降至最低。

垃圾邮件过滤和网络网关过滤：

垃圾邮件过滤和网络网关过滤是阻止试图通过恶意IP、URL和垃圾电子邮件到达端点的勒索软件的好方法。

应用白名单：

白名单决定了哪些程序可以在终端上运行，从而可以阻止服务器、公司台式机和固定功能设备上未经授权程序的执行，大大减少大多数勒索软件的攻击面。

侦测分析技术[5]：

在面对勒索软件攻击时，侦测分析技术可有效拦截已知勒索软件的加密行为，当未知勒索软件对数据进行加密时，能够在第一时间发现异常，及时告警。常见的勒索软件侦测技术包括，通用文件扩展名侦测、静态文件分析、蜜罐文件、批处理文件操作的动态监控等。但由于勒索软件的变种不断地出现，攻击者也会使用各种迷惑性的战术让勒索软件逃避侦测，企业需要充分了解每种侦测方法的优缺点，并使用多种侦测技术才能更好地将勒索软件进行拦截。

[5] 华为, '华为存储防勒索解决方案技术白皮书',华为技术有限公司, 30 October 2022

感染阶段：

谨慎启用宏：

通常在通过电子邮件接收的文文件中不应启用宏。Office宏是勒索软件感染计算器的一种流行方式，因此如果打开未知文档的时候“要求”启用宏时请谨慎选择。

阻止“未经批准”的进程更改文件：

通过主机入侵防御系统或编写访问保护规则来阻止这些进程。

访问控制技术[6]：

访问控制可以用于防止勒索软件攻击。当一个恶意程序尝试访问系统时，它需要在访问之前通过访问控制进行身份验证。安全的访问控制措施与策略可以确保只有授权的用户或组才能访问特定的资源，从而防止未经授权的访问和攻击。常见的访问控制措施有基于角色权限管理（RBAC）和多因素身份验证（MFA）。

基于角色权限管理（RBAC）是一种有效的访问控制措施，可以根据不同的角色定义不同的访问权限，企业也应针对数据备份业务设置少数人员以控制数据备份的关键操作在可控范围内。

多因素身份验证（MFA）是一种更复杂、更安全的身份验证机制，是一种通过呈现多条信息或对象对用户进行身份验证的系统，可以使未经授权的攻击者更加难以访问关键系统或网络。

[6] IDC,'IDC Huawei White Paper - Developing Ransomware Resilience', International Data Corporation, February 2023, https://e.huawei.com/en/material/enterprise/10708d681d05414d9391a4ff2cb8df5a

华为, ' Ransomware Protection Storage Solution',华为技术有限公司,

扩散阶段：

防火墙可以阻止已知的恶意域：

编写规则阻止恶意域是网络防火墙的标准功能。

代理/网关流量扫描：

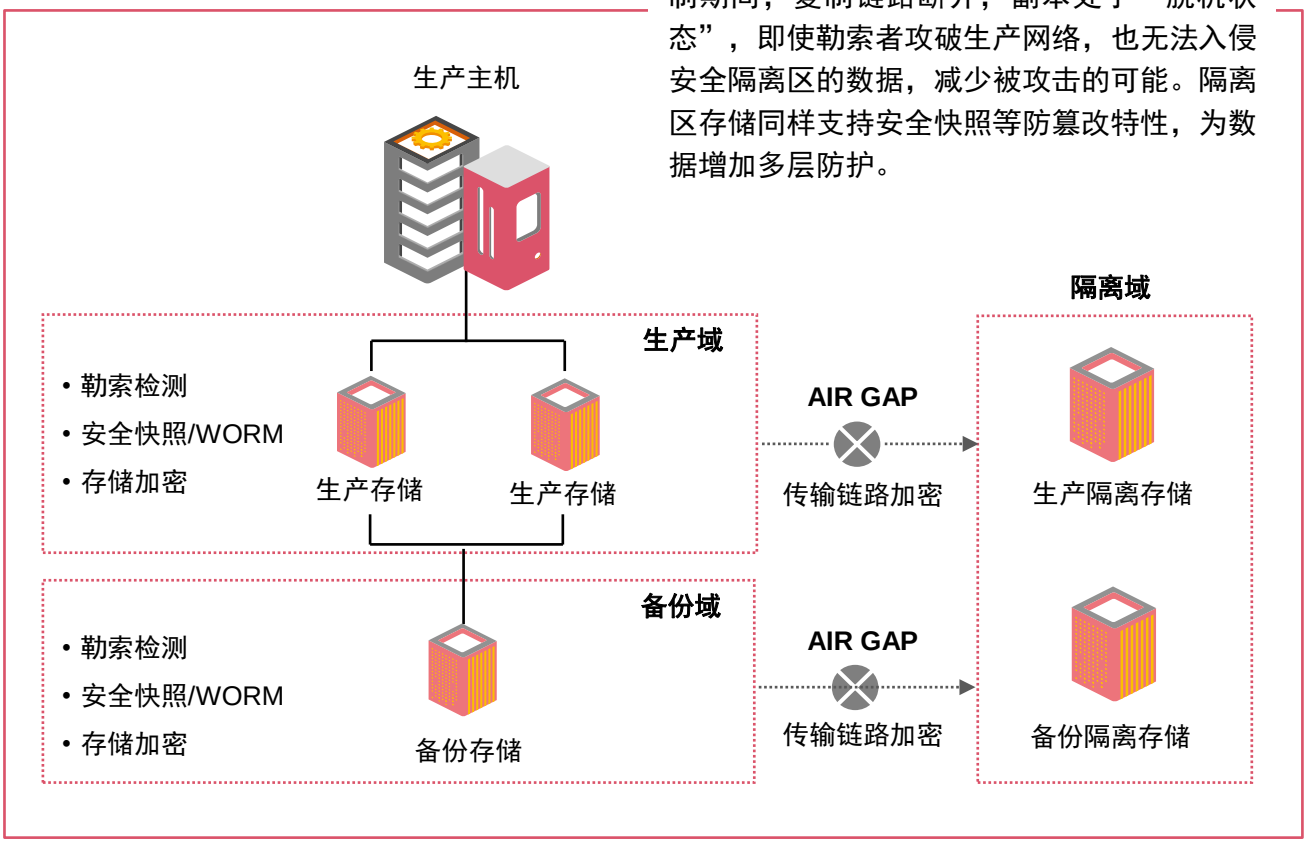
可以使用代理和网关设备的扫描功能来检索已知勒索软件所控制的服务器的流量，这可以阻止部分依赖公共加密秘钥来进行对称加密的勒索软件，使其无法继续攻击。

零信任原则：

零信任安全原则默认任何人、设备、系统的访问都视为潜在威胁，并在身份验证前不予信任，从而确保身份可信、设备可信、应用可信和链路可信。

气隙隔离技术（AIR GAP）[7]：

气隙隔离（AIR GAP）指通过实施系统网络孤立，将气隙隔离的设备与其他连接的设备隔开，从而避免在线访问，以此创造安全隔离区。将生产存储与备份存储的数据复制到隔离区。若生产存储和备份存储均被勒索软件攻破，可使用隔离区的副本进行数据恢复。非复制期间，复制链路断开，副本处于“脱机状态”，即使勒索者攻破生产网络，也无法入侵安全隔离区的数据，减少被攻击的可能。隔离区存储同样支持安全快照等防篡改特性，为数据增加多层防护。



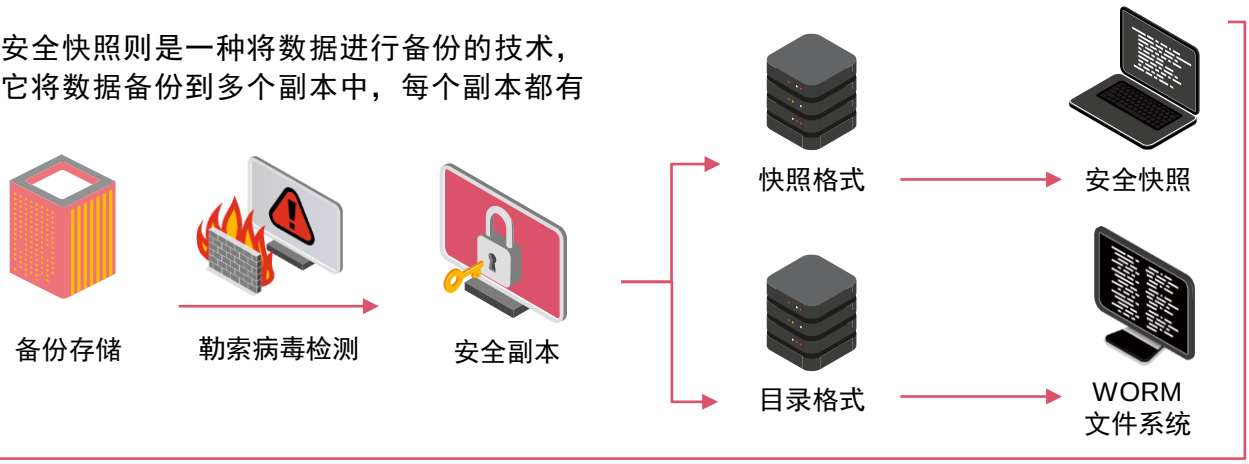
[7] 华为, ' Ransomware Protection Storage Solution',华为技术有限公司, https://e.huawei.com/en/solutions/storage/oceanprotect/ransomware

加密阶段：

数据防篡改技术[5]：

WORM文件存储和安全快照都是用于数据防篡改的技术。WORM是一种写一次读多次的文件存储方式，本质上是一次写入技术，即文件被写入完成后即可通过设置使其进入保护状态，在该状态下文件只能被读取，无法被删除、修改或重命名。

安全快照则是一种将数据进行备份的技术，它将数据备份到多个副本中，每个副本都有独立的数据块，同时可设置安全快照保留周期。在保留周期内，该快照以及所依赖的文件系统不能够被恶意删除，从而保证其中数据防篡改，实现当原数据被黑客或内部人员恶意破坏或篡改后，可借助安全快照恢复到被篡改前快照时间点。



数据加密技术：

使用加密技术对数据传输链路、数据复制链路进行加密可防止数据在传输中遭到窃取、泄露和篡改，除此以外还需具备存储加密能力以保障存储磁盘被窃取后数据不被泄露。

静态数据加密是一种对存储数据进行加密以防止未经授权访问的网络安全实践。静态加密技术将明文数据转换为密文数据，使得非法用户无法直接解读原始数据，只能通过解密密文后才能获取其中的信息。静态加密技术可以有效地保护数据的安全性和隐私性，避免了未经授权的用户对数据的访问和篡改。常见的静态加密技术包括透明加密和轮换密钥加密。

传输加密是指对传输中的数据进行加密，考虑到数据泄密频发多数都集中在数据传输阶段，而数据传输加密是保障数据传输安全的主要手段。数据传输加密可以帮助数据在不可信或安全性较低的网络中传输，尤其是跨广域网传输，能够有效防止数据遭到窃取、泄露和篡改。

数据完整性校验技术：

数据完整性校验是指在数据传输或存储过程中，对数据的正确性、有效性和一致性进行检查和验证的过程。数据完整性校验的目的是确保数据在传输或存储过程中不会出现错误、遗漏或不一致的情况，从而保证数据的准确性、可靠性和完整性。常见的数据完整性校验方法有哈希校验、序列号校验、数字签名校验、时间戳校验、随机数校验等。

[5]华为, '华为存储防勒索解决方案技术白皮书',华为技术有限公司, 30 October 2022

勒索阶段：

数据安全备份：

在勒索软件突破防火墙对系统数据、文件进行加密后，数据备份成为了企业能否恢复数据的关键。

大规模并行处理架构（MPP）：

大规模并行处理（MPP）是一种采用大量处理单元对问题进行求解的并行处理技术，具有并行性、灵活性和扩展性三个优势。可以提供更好的并行性能和更高的计算效率，从而更快地完成数据备份和恢复。

- 并行性：大规模并行处理通过将问题分解为若干个子问题，并将这些子问题分配到不同的处理单元中进行求解，从而实现并行处理。由于处理单元（PE）之间的通信和协作是并行的，因此可以获得更高的计算效率和更好的性能。
- 扩展性：大规模并行处理支持集群节点的扩容，可以在不增加硬件成本的情况下实现规模扩展。
- 灵活性：大规模并行处理采用共享内存和互联机制，可以实现任务的分布式存储和计算，从而实现横向扩展。这使得MPP可以适应各种不同的应用场景，包括高性能计算、分布式系统、实时控制等。

随着数字化技术的不断发展和应用，创新技术正在深刻地改变着人们的生产方式、生活方式和社会结构。与此同时，网络安全威胁也呈现越来越普遍化、复杂化、隐蔽化和技术化的趋势，对企业造成的影响也越来越严重。由于网络安全问题的影响范围广泛，已经成为企业面临的一项重大挑战，给企业的正常运营和发展带来困扰。网络安全漏洞导致的勒索软件攻击事件频繁发生，给企业带来严重的经济损失，甚至可能导致业务中断。企业应该及时依照相关行业经验或法律法规，不断更新调整自身针对防勒索软件的防治策略，加强预防措施和能力。

4

关于普华永道中国

普华永道秉承“解决重要问题，营造社会诚信”的企业使命。全球各成员机构组成的网络遍及152个国家和地区，有将近32.8万名员工，致力于在审计、咨询及税务领域提供高质量的服务。其中，普华永道中国内地、香港地区及澳门地区成员机构根据各地适用的法律协作运营，员工总数超过28,000人，其中包括逾1,117名合伙人。

无论客户身在何处，普华永道均能提供所需的专业意见。我们实务经验丰富、高素质的专业团队能聆听各种意见， 帮助客户解决业务问题，发掘并把握机遇，我们的行业专业化有助于就客户关注的领域共创解决方案。

5

关于华为

华为创立于1987年，是全球领先的ICT（信息与通信）基础设施和智能终端提供商，致力于把数字世界带入每个人、每个家庭、每个组织，构建万物互联的智能世界。目前华为约有19.7万员工，业务遍及170多个国家及地区，服务全球30多亿人口。

华为凭借领先的创新技术与能力积累，智能云网、智简全光网、数据中心、数据存储、5GtoB、可信赖服务等产品和最佳实践的竞争力获得业界广泛认可。自2011年成立以来，华为企业业务保持稳健增长，赢得了越来越多的客户和伙伴的信任。截至 2021年底，全球700多个城市、267家世界500强企业选择华为作为数字化转型的合作伙伴。华为从场景、模式和生态三个方面探索行业数字化转型前景与未来，2021年面向政府、交通、金融、能源以及制造等重点行业，发布11大场景化最佳实践。截至2021年底，华为共打造了覆盖10余个行业的 100 多个场景化最佳实践。

面向未来，华为将持续围绕伙伴盈利、政策简化、伙伴能力提升、数字化工具和装备打造以及健康生态构建等五个方面，加大对伙伴的投入，深耕伙伴的拓展与运营，构筑长期生存、高速发展基石。

英文缩略语

缩略语	英文全称	中文全称
STDB	Secure Tertiary Data Backup Guideline	三级安全数据备份指南
HKAB	The Hong Kong Association of Banks	传输控制协议/互联网络协议
HKMA	Hong Kong Monetary Authority	香港金融管理局
ACSC	The Australian Cyber Security Centre	澳大利亚网络安全中心
GB	Gigabyte	十亿字节
TB	Terabyte	太字节
Root	Root	超级用户权限
RaaS	Ransomware as a Service	勒索软件即服务
IP	Internet Protocol	网际互连协议
URL	Uniform Resource Locator	统一资源定位系统
ICS	Industrial Control Systems	工业控制系统
WORM	Write Once Read Many	一次写入,多次读取
AIR GAP	AIR GAP	气隙隔离
NIS	The Network and Information Security (NIS) Directive	《网络和信息系统安全规则》
NIS2	The NIS2 Directive A high common level of cybersecurity in the EU	《关于在欧盟全境实现高度统一网络安全措施的指令》
MPP	Massive Parallel Processor	大规模并行处理计算器
DR	Disaster Recovery	灾难恢复
IT	Internet Technology	互联网技术
RBAC	Role-Based Access Control	基于角色的访问控制
MFA	Multi-Factor Authentication	多因子认证
PE	Processing Element	处理单元
ICT	Information and Communications Technology	信息与通信技术
UAE	United Arab Emirates	阿拉伯联合酋长国

附录

参考引用：

[1] IBM, ‘2002年度X-Force 威胁情报指数’, IBM Security, February 2022

[2] Sophos, ‘The State of Ransomware 2022’, Sophos Ltd., 20 April 2022, https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

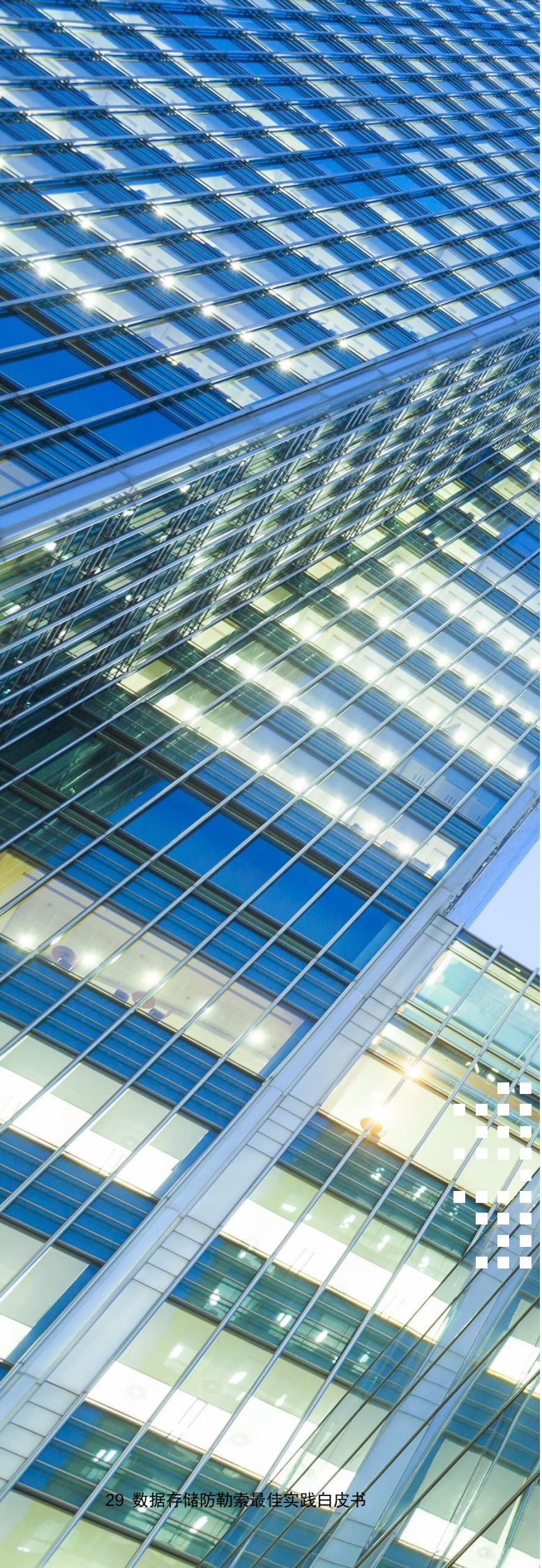
[3] Sophos, ‘The State of Ransomware 2021’, Sophos Ltd., 19 April 2021, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

[4] McAfee, ‘Understanding Ransomware and Strategies to Defeat it’, McAfee Labs, March 2016

[5] 华为, '华为存储防勒索解决方案技术白皮书',华为技术有限公司, 30 October 2022

[6] IDC,'IDC Huawei White Paper - Developing Ransomware Resilience', International Data Corporation, February 2023, https://e.huawei.com/en/material/enterprise/10708d681d05414d9391a4ff2cb8df5a

[7] 华为, ' Ransomware Protection Storage Solution',华为技术有限公司, https://e.huawei.com/en/solutions/storage/oceanprotect/ransomware



联系我们

普华永道中国

翁泽鸿

普华永道中国网络安全和隐私服务合伙人

电话：+86 (20) 3819 2629

邮箱：danny.weng@cn.pwc.com

马东诚

普华永道香港地区网络安全和隐私服务合伙人

电话：+[852] 2289 1843

邮箱：aaron.ts.ma@hk.pwc.com

丁力旻

普华永道香港地区网络安全和隐私服务高级经理

电话：+[852] 2289 8512

邮箱：duncan.lm.ding@hk.pwc.com

黄琳倩

普华永道中国网络安全和隐私服务经理

电话：+86 (20) 3819 2958

邮箱：lynn.lq.huang@cn.pwc.com

华为

Joe Yip
华为国际有限公司数据中心解决方案总监

Michelle Cheung
华为国际有限公司解决方案高级经理

Xiao Hui Cao
华为国际有限公司技术专家

Si Yuan Sun
华为国际有限公司首席工程师

Sui Ying Chen
华为国际有限公司数据存储专家

www.pwccn.com