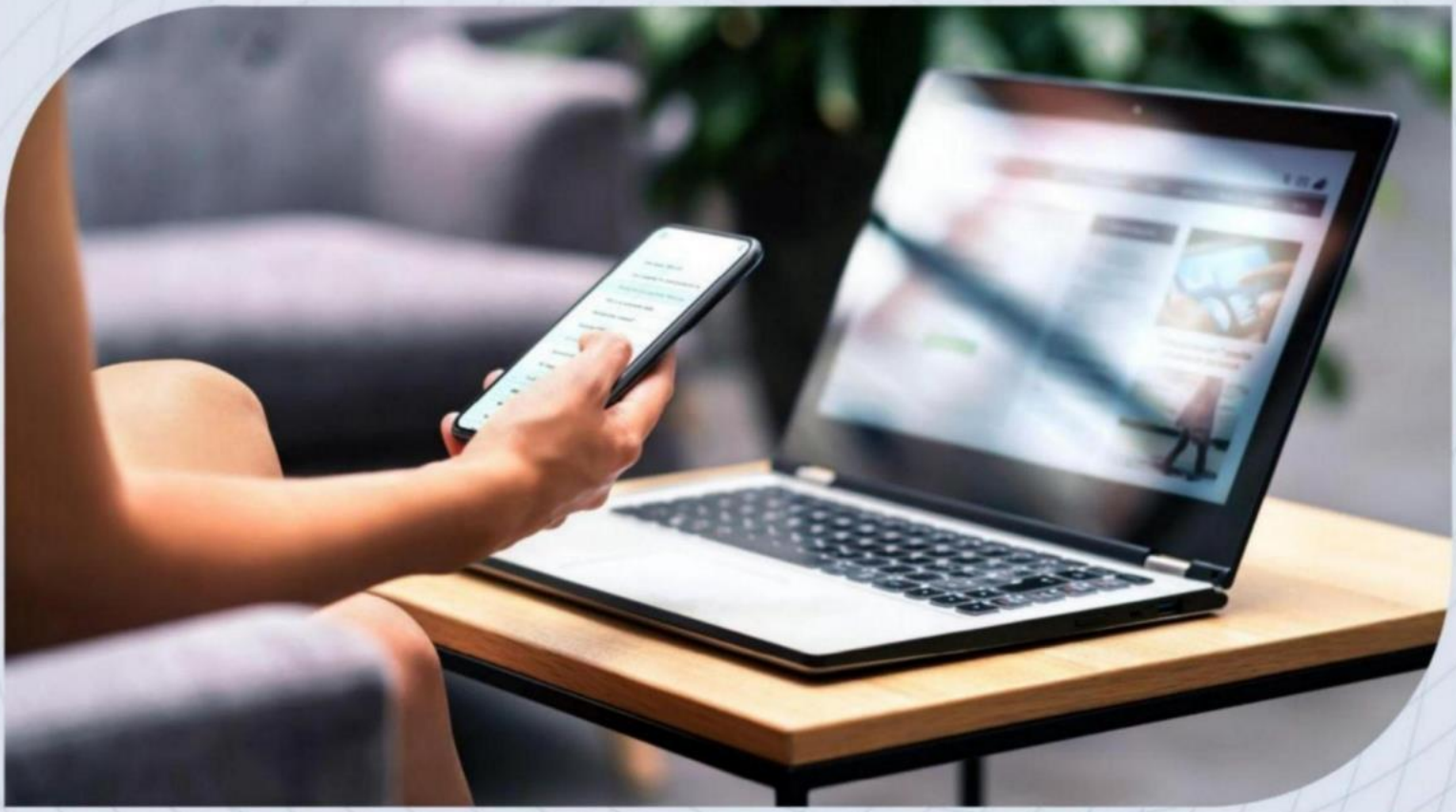
面向IAM的零信任原则与指南



Release Candidate

CSA GCR GREATER CHINA REGION cloud security alliance®

CSA cloud security alliance®

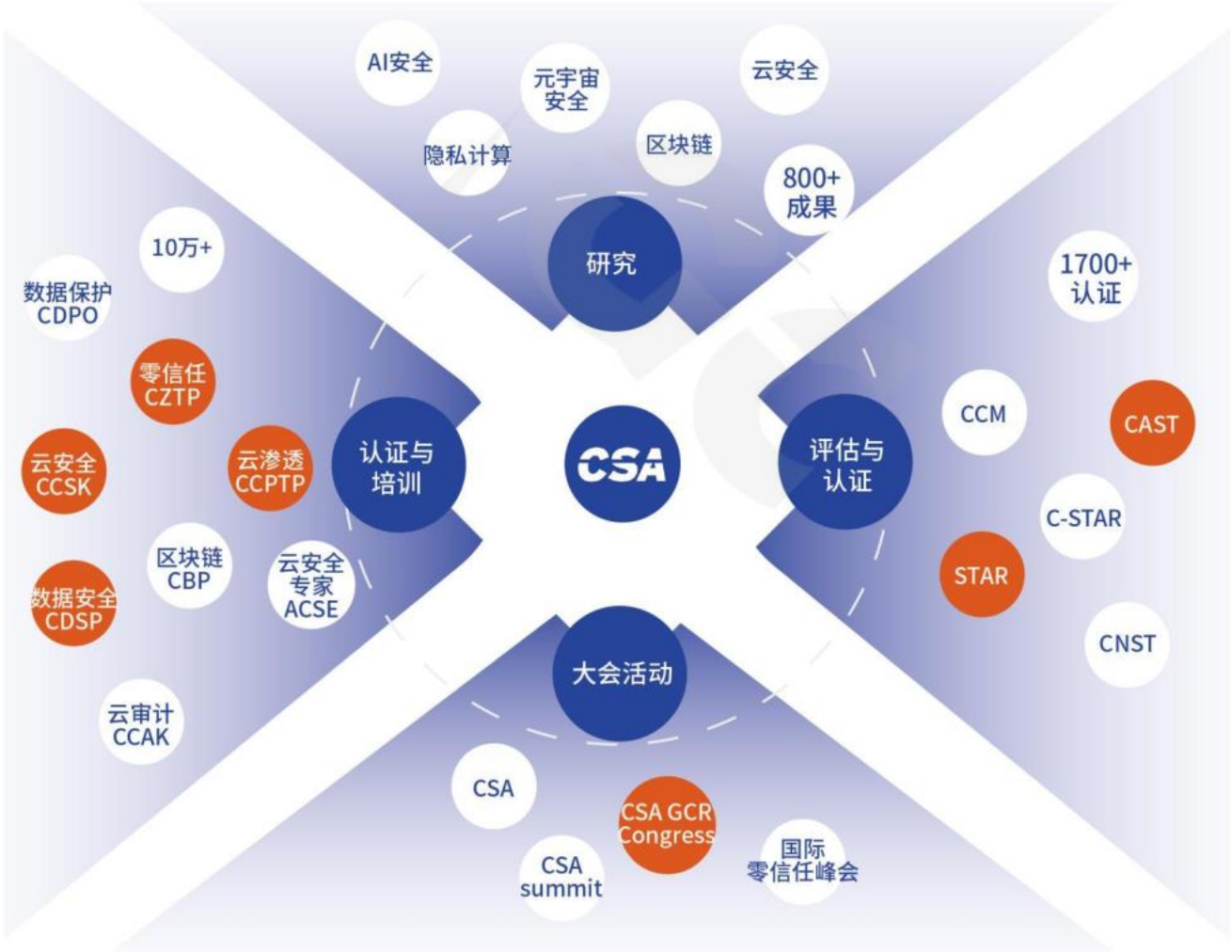
联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息



加入我们

CSA大中华区官网
（https://c-csa.cn）

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

报告中文版支持单位

上海派拉软件股份有限公司成立于2008年，是国内最早从事身份安全研发的原厂商，致力于为企业和机构提供以“数字身份”为核心的数字化能力底座与安全基石，覆盖身份安全、应用安全、数据安全，在上海、北京、广州、武汉、成都、长春、深圳、济南、厦门、合肥、杭州、西安等地设有研发中心和服务机构，拥有600+行业专家和资深团队，服务能力遍布全国。派拉软件已成功为全球范围内的金融、制造、医疗、教育、零售、政府、地产、科研院所等多行业2000余家企业和机构提供极致体验的“全域数字身份统一安全管控”专业服务，覆盖五百强客户300余家。

派拉软件是CSA会员单位，支持该报告内容的翻译，但不影响 CSA研究内容的开发权和编辑权。

主要贡献专家：

茆正华徐安哲王育恒王磊

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR秘书处给予改正！联系邮箱research@c-csa.cn ；国际云安全联盟CSA公众号

©2024云安全联盟大中华区版权所有

英文版本编写专家

主要作者：

Hani Raouda

Jonathan Flack

Kevin Dillaway

Paul Simmonds

Rohini Sulatycki

Shruti Kulkarni

Clement Betacorne

Irshad Javid

John Yeoh

Paul Simmonds

审校者：

Anna Pasupathy

CSA全球员工：

Erik Johnson

Ryan Gifford

Stephen Lumpe

©2024云安全联盟大中华区版权所有

目录

©2024云安全联盟大中华区版权所有

摘要

身份及身份相关的属性，以及其他零信任（ZT）标识（零信任中关于身份的其他属性）是零信任架构的关键原则之一。零信任方法旨在通过基于风险的访问控制来减少网络攻击和数据泄露的几率。也就是说，在授予对资源（数据、系统）的访问权限之前，必须进行身份验证和授权。

为了满足这一要求，重要的是要通过零信任的视角来审视现存和新的身份、访问管理和云解决方案。

零信任是一个技术无关的指导性框架，将访问控制措施更加靠近受保护资产（保护面）。从身份、访问管理的角度来看，它提供了基于风险的决策授权能力，而不是仅基于单一访问控制方法的二元信任来进行授权访问。

目标受众

主要：零信任（ZT）实施和架构的技术经理
次要：CISO / ISO /信息安全、IAM供应商

零信任的背景和推动因素

多年来，有各种论文谈论信任作为人类和社会现象，其中一些使用了“零信任”这个术语。2001年，开源安全测试方法手册（OSSTMM）开始解决信息技术中的信任问题，并在其第三版（2007年）中将“信任”标记为漏洞，并专门撰写了一整章来讨论这个主题。

Sun Microsystems在 1990年代引入了“Chewy Center”①（智能糖果或 M&M糖果模型②）的概念。在 2005-2007年期间，Jericho Forum(visioning paper and Jericho Forum® Commandments)和 OpenGroup为零信任做了一些基础工作，讨论了

©2024云安全联盟大中华区版权所有

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/136042030111010111

传统网络边界安全模型的失败以及去边界化的必要性，这是 Open Group零信任安全准则的灵感来源。

零信任网络（ZTN）概念是在 21世纪初由美国国防部（DoD）提出的，当时正在定义全球信息网（GIG）网络运营黑核网络路由技术和路由寻址架构，这是 DoD的网络中心服务战略的一部分。随着时间的推移演变为 ZTN架构（ZTNA）和软件定义的边界（SDP）框架，并被 DoD、CSA和 NIST所采纳和进一步推广。

在经过两年的研究，Forrester Research的 John Kindervag于 2010年正式将这些概念整合成我们现在所知道的零信任实践领域。John的工作独特之处在于他正式确定了成功实施这些架构所需的组件，并提供了一种可理解的实施零信任的方法，包括利用 Kipling方法开发有效的零信任策略，以及启用扩展授权控制，例如基于上下文的访问控制。

2019年左右，美国国防部（DoD）在与国家安全局（NSA）进行情报磋商后开始拥抱零信任，美国国防部认为当时的安全方法不再有效，且需要调整其安全战略，以更好地抵御日益复杂的网络攻击。

2020年 8月，NIST发布了 SP 800-207零信任架构。2021年 5月，美国总统拜登签署行政命令（EO）14028，特别提到了零信任安全实践，要求联邦机构加强网络安全，为政府采用零信任提供了第一个重要的法规。虽然全球都对零信任的兴趣在最近几年不断增加，由于受到美国政府法规的影响，美国目前在零信任应用和相关指导方面处于领先地位。

无论是来自 NIST、DoD、CISA还是像 CSA、Forrester Research或英国 NCSC这样的组织的专家贡献，其中相关的指导原则都基于相同的基本原则（最初在 John Kindervag的基础研究中描述），其中许多是已经确立为信息安全概念（例如“最小特权”，“拒绝所有，例外允许”）。

©2024云安全联盟大中华区版权所有