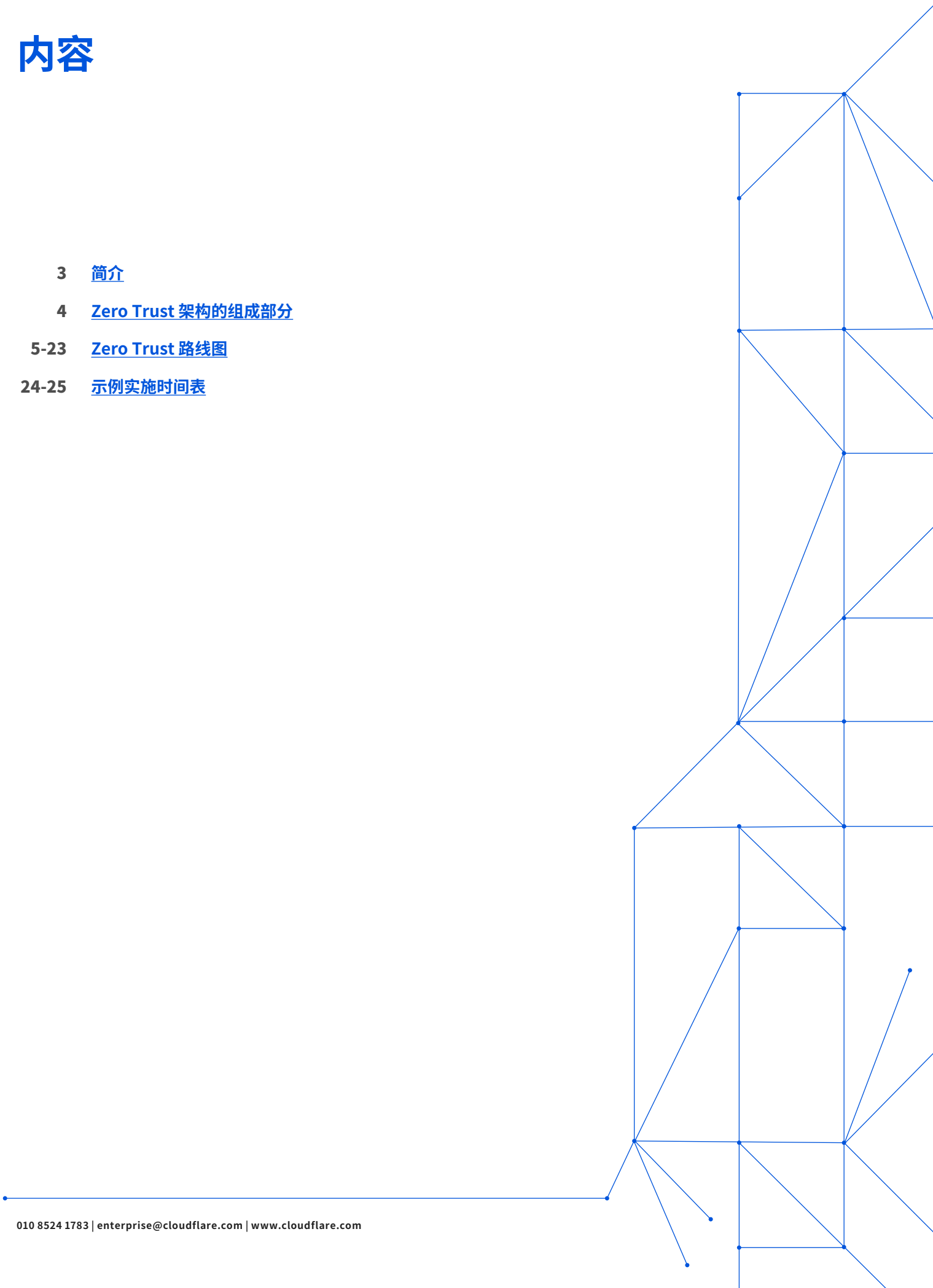
CLOUDFLARE

白皮书

Zero Trust 架构路线图

了解实现网络转型和安全现代化所需的步骤、工具和团队

内容



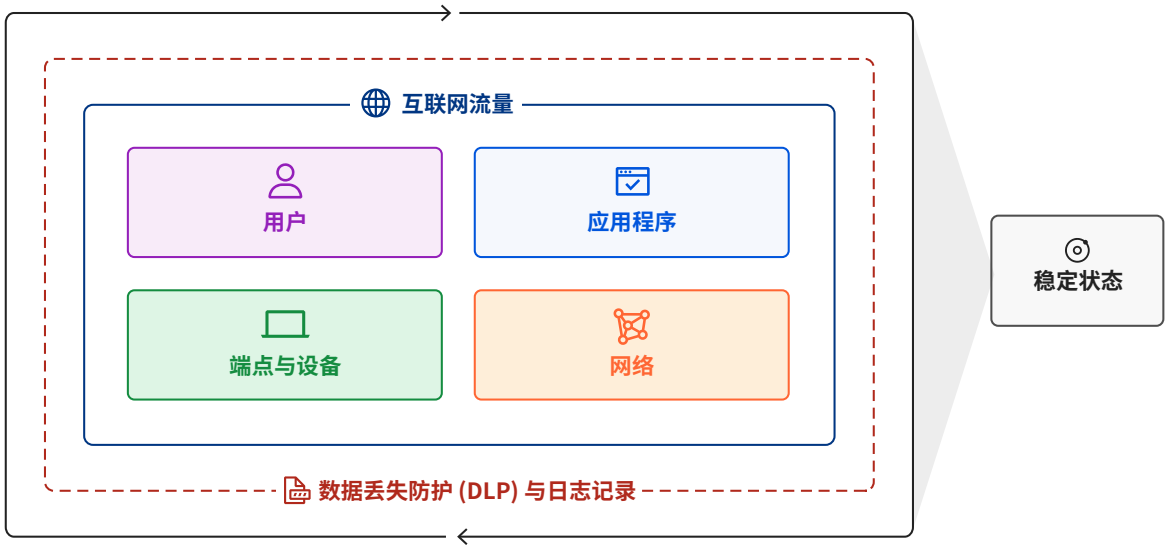
简介

传统网络架构建立在边界网络的概念之上，即一旦某人处于网络之中，即享有一种隐含的信任。向云托管、远程办公和其他现代化转型给传统边界网络架构带来了挑战。

这些挑战可以通过实施 Zero Trust 架构来解决，该架构可以确保所有进出企业的流量都经过验证和授权。可在不影响员工生产力和连接性的情况下分步实施 Zero Trust 架构。

本指南由安全专家编制，旨在提供一个与供应商无关的 Zero Trust 架构和示例实施时间表。该时间表假设组织从零开始其 Zero Trust 旅程，但对所有组织都是有用的。

实施全面的 Zero Trust 架构时，需要考虑组织安全的七个主要组成部分。您的实施顺序不需要与如下所列的组成部分和参考架构一致。



Zero Trust 架构的组成部分

	组成部分	目标	努力级别	页面
第一阶段	互联网流量	部署全球 DNS 过滤	▮	9
	应用程序	监控入站电子邮件并过滤网络钓鱼企图	▮	13
	DLP 与日志	识别 SaaS 工具中的错误配置和公开分享数据	▮	20
第二阶段	用户	建立企业身份	▮▮	5
	用户	对所有应用启用基本 MFA	▮	6
	应用程序	启用 HTTPS 和 DNSSEC	▮	17
	互联网流量	在 SSL 之后阻止或隔离威胁	▮▮	9-10
	应用程序	对公开可寻址应用执行 Zero Trust 策略	▮	14-16
	应用程序	保护应用以防第 7 层攻击	▮	16
	网络	为应用交付关闭所有对互联网开放的入站端口	▮	12
第三阶段	应用程序	盘点所有企业应用	▮▮	13-14
	应用程序	对 SaaS 应用执行 Zero Trust 策略	▮▮	14-16
	网络	隔离用户网络访问	▮▮▮	11
	应用程序	针对关键私有可寻址应用的 ZTNA	▮	14-16
	设备	实施 MDM/UEM 以管控企业设备	▮▮	7
	DLP 与日志	定义敏感数据及其所在位置	▮▮	18-19
	用户	发出基于硬件的身份验证令牌	▮▮	6
	DLP 与日志	掌握已知威胁行为者的最新状况	▮	21
第四阶段	用户	实施基于硬件的 MFA	▮▮	6
	应用程序	对所有应用实施 Zero Trust 策略和网络访问	▮▮▮	14-16
	DLP 与日志	创建安全运营中心 (SOC)，用于日志检查、策略更新和缓解	▮▮	20
	设备	实施端点保护	▮▮	7
	设备	清点所有企业设备、API 和服务	▮	8
	网络	用宽带互联网实现分支机构之间的连接	▮▮▮	11-12
	DLP 与日志	记录和审查敏感应用上的员工活动	▮▮	18
	DLP 与日志	防止敏感数据离开应用	▮▮▮	19
	稳定状态	用于新资源策略执行的 DevOps 方法	▮▮	22
	稳定状态	实施针对接入资源的自动扩展	▮▮▮	22-23

有关每一步所需努力程度的定义如下：

- ▮ - **低：**可由个人或小团队完成
- ▮▮ - **中：**需要一个团队和预先准备
- ▮▮▮ - **高：**需要多个团队和项目计划

Zero Trust 路线图

用户

用户包括员工、承包商和客户。要实施 Zero Trust，组织必须首先准确地知道谁应该被信任，以及被信任的依据——即身份。然后，组织必须建立一种安全地验证用户身份的方法。

建立企业身份

努力程度	**- 中**
涉及团队	• 负责身份提供商的团队（通常是安全或 IT） • 管理员工和合作伙伴所用的内部应用的管理员
产品	Microsoft Azure AD， Okta， Ping Identity PingOne， OneLogin
摘要	需要统一的企业身份，以准确地验证和授权对企业应用的访问。一致的企业身份将使应用的细粒度策略执行更无缝流畅。 **需要考虑的其他问题：** • 您的公司是否积极进行并购活动？您将如何整合身份库？ • 您是否正在使用任何非基于 Web 的身份认证协议（例如：活动目录，ntlm，kerberos）
步骤	1. 将所有企业用户添加到身份提供商 a. 这些数据常常可从 HR 系统（例如 Workday，ADP 等）同步过来 2. 验证每个用户的信息均正确无误 3. 向新用户发送注册信息，以设置登录凭据

对所有应用启用多因素身份验证

努力程度	- **低**（如果应用基本 MFA） - **中**（如果使用硬件密钥）
涉及团队	• 负责身份提供商的团队（通常是安全或 IT） • 员工和合作伙伴所用内部应用的管理员
产品	**身份提供商：** Microsoft Azure AD， Okta，Ping Identity PingOne，OneLogin **应用反向代理：** Microsoft Azure AD App Proxy，Akamai EAA，Cloudflare Access，Netskope Private Access，Zscaler Private Access (ZPA) **硬件密钥：** Yubico
摘要	多因素身份验证 (MFA) 是防御利用网络钓鱼或数据泄露盗取用户凭据的最佳保护措施。大多数 MFA 可在身份提供商中直接启用。 对于未与身份提供商直接集成的应用，考虑在应用前使用应用反向代理 (Application Reverse Proxy) 来实施 MFA。
步骤	1. 通知内部用户即将启用 MFA。提供通过短信或身份验证应用注册的选项 2. 在身份提供商中启用 MFA 3. 在未与身份提供商集成的应用前启用应用反向代理 4. （更进一步）通过邮件或亲自向员工分发硬件密钥 5. （更进一步）对最敏感的应用实施仅限硬件密钥的 MFA

端点与设备

端点和设备包括组织内或能够访问组织数据的任何设备、API 或软件服务。组织必须首先了解其完整的设备、API 和服务。然后即可根据设备、API 和服务的上下文来实施 Zero Trust 策略。

实施移动设备管理

努力程度	**- 中**
涉及团队	• IT 团队
产品	**Mac：** Jamf，Kandji **Windows:** Microsoft Intune
摘要	大多数 Zero Trust 架构要求在至少一部分用户机器上安装软件。移动设备管理 (MDM) 是大多数组织针对用户设备库管理软件和配置的方式。
步骤	查看 MDM 供应商站点以了解详情。

实施端点保护

努力程度	**- 中**
涉及团队	• 安全团队 • IT 团队
产品	VMWare Carbon Black，Crowdstrike，SentinelOne，Windows Defender
摘要	端点保护软件安装在用户的机器上，扫描影响设备的已知威胁。端点保护软件也可以用来强制安装操作系统补丁和更新。来自端点保护软件的信号可以并且应当用于应用访问控制策略。
步骤	1. 使用 MDM 在用户机器上安装端点保护软件 2. 在端点保护软件中启用威胁保护和合规控制

盘点设备、API 和服务

努力程度	- **低**
涉及团队	• 安全团队 • IT 团队
产品	**设备盘点：**VMWare Carbon Black，Crowdstrike，SentinelOne，Windows Defender，Oomnitza **API/服务盘点：**Cloudflare 应用连接器，Zscaler Private Access (ZPA)
摘要	端点保护软件和资产管理软件可用于跟踪已分发给用户的所有设备。应当维护准确的设备列表，以跟踪哪些设备是有效的，并应该具备对特定应用的访问权限。 也应当对 API 和服务进行盘点并通过库存列表维护。可利用网络扫描，以识别能通过内部或外部网络通信的新 API 和软件。
步骤	1. 使用 MDM 在用户机器上安装端点保护软件 2. 在网络内安装 API/服务扫描工具

互联网流量

互联网流量是指到组织控制之外网站的所有用户流量。其中可包括业务相关任务和个人网站使用。所有出站流量都容易受到恶意软件和恶意站点的影响。组织必须就前往互联网的用户流量建立可见性和管控。

阻止对已知威胁或有风险目的地的 DNS 请求。

努力程度	**- 低**
涉及团队	• 可访问路由器或机器配置的 IT 团队 • 安全团队
产品	**DNS 过滤：** Cisco Umbrella DNS，Cloudflare Gateway，DNSFilter，Zscaler Shift
摘要	DNS 过滤可通过路由器配置或直接在用户机器上应用。这是保护用户免受已知恶意网站攻击的最快方法之一。
步骤	**DNS 过滤：**更新办公室 Wifi 上的 DNS 解析配置，以指向适当的 DNS 解析服务。这可以用来阻止已知的恶意网站。

阻止或隔离 SSL/TLS 后的威胁

努力程度	**- 中**
涉及团队	• 可访问路由器或机器配置的 IT 团队 • 安全团队
产品	**TLS 解密：** Cloudflare Gateway，Netskope Next Gen SWG，Zscaler Internet Access (ZIA) **浏览器隔离：** Cloudflare Browser Isolation，Zscaler Cloud Browser Isolation

阻止或隔离 SSL/TLS 后的威胁（续）

摘要	一些威胁隐藏在 SSL 后，无法通过纯 HTTPS 检查来阻止。应当利用 TLS 解密来进一步保护用户免受 SSL 后的威胁。
步骤	**TLS 解密：** 1. 确保在用户机器上安装了正确的客户端软件 a. 检查是否有任何 VPN 或其他软件会干扰设备上的出站 Web 流量 2. 在设备上配置用于 TLS 解密的根证书 3. 启用何时避免解密用户流量的策略 a. 应对使用证书锁定的站点进行这一操作 b. 一些公司也绕过对用户个人流量（例如银行、社交媒体等）的解密 **浏览器隔离：** 1. 浏览器隔离可通过设备客户端软件或通过隔离链接部署。两种方式均应考虑。

网络

网络包括组织内的所有公共、私有和虚拟网络。组织必须首先了解其现有的全部网络，并进行隔离以防止横向移动。然后，组织可创建 Zero Trust 策略，以细粒度的方式控制用户、端点和设备可以访问网络的哪些部分。

隔离用户网络访问

努力程度	**- 高**
涉及团队	• 安全团队 • IT 团队
产品	**Zero Trust 网络访问 (ZTNA)：**Cloudflare Zero Trust（Access 和 Gateway 可一起使用），Netskope Private Access，Zscaler Private Access (ZPA)
摘要	一般情况下，用户可通过 VPN 或在办公室网络中访问整个私有网络。Zero Trust 规定，用户仅有权访问完成特定任务所需的特定网络部分。Zero Trust 网络解决方案允许用户远程访问某个本地网络，但采用基于用户、设备和其他因素的细粒度策略。
步骤	1. 使私有网络可用于 ZTNA a. 通常是应用连接器、GRE 或 IPSec Tunnel。 2. 使用 MDM 在用户机器上安装 ZTNA 客户端 3. 通过配置策略来隔离用户在私有网络中的访问

用宽带互联网实现分支机构之间的连接

努力程度	**- 高**
涉及团队	• 网络工程团队 • IT 团队
产品	Cloudflare Magic WAN，Cato Networks，Aryaka FlexCore

对分支机构之间的连接启用宽带互联网（续）

摘要	私有网络地点（例如数据中心和分支机构）之间的连接通常使用多协议标签交换 (MPLS) 线路或电信供应商提供的其他专用链路建立。这些 MPLS 链路通常费用昂贵。随着互联网连接的质量提高，组织可通过安全隧道在互联网上路由流量来提供同样级别的安全访问，但成本大幅降低。
步骤	1. 选择两个以 MPLS 连接的地点作为开始。这些地点将需要某种形式的互联网连接。 2. 通过互联网电路建立一对冗余 Anycast GRE 或 IPsec 隧道，连接到云 WAN 提供商的边缘网络。 3. 验证隧道之间的健康状况和连接性。以尽可能接近生产流量的流量负载来测试性能（吞吐量、延迟、丢包率、抖动）。 4. 更改路由策略，将生产流量从 MPLS 迁移到互联网隧道 5. 在下一个以 MPLS 连接的地点重复该步骤 6. 退役 MPLS 电路

为应用交付关闭所有对互联网开放的入站端口

努力程度	**- 低**
涉及团队	• 网络工程团队
产品	**Zero Trust 反向代理：**Akamai EAA，Cloudflare Access，Netskope，Zscaler Private Access (ZPA)
摘要	使用扫描技术发现可发现开放的入站网络端口，这是一种常见的攻击手段。Zero Trust 反向代理允许您安全地公开一个 Web 应用，而无需打开任何入站端口。应用的 DNS 记录是应用唯一公开可见的记录。该 DNS 记录受到 Zero Trust 策略保护。为进一步增强安全性，内部/私有 DNS 可使用一种 Zero Trust 网络访问服务来利用（详见下文）。
步骤	1. 安装反向代理应用连接器——通常是同一网络中的后台程序或虚拟机 2. 将反向代理应用连接到应用连接器 3. 用防火墙规则关闭专用网络上的所有入站端口

应用

应用包括存在组织数据或执行业务流程的任何资源。组织必须首先了解现有的应用程序，然后为每个应用建立 Zero Trust 策略，或者在某些情况下阻止未经批准的应用。

监控电子邮件应用并过滤网络钓鱼企图

努力程度	- 低
涉及团队	• 负责电子邮件供应商配置的团队（通常是 IT）
产品	**云电子邮件安全：** Cloudflare Area 1 Email Security， Mimecast，TitanHQ **浏览器隔离：** Cloudflare Browser Isolation，Zscaler Cloud Browser Isolation
摘要	电子邮件是攻击者能不受限制地接触员工的少数几个渠道之一。部署安全电子邮件网关是确保恶意或不受信任的电子邮件远离员工的关键步骤。此外，对于可疑程度不足以完全阻止的链接，安全团队应当考虑在隔离浏览器中打开链接的选项。
步骤	1. 配置域的 MX 记录，使其指向安全电子邮件网关服务 2. 在最初几周监控误报 3. （更进一步）对于临界的可疑电子邮件链接，实施基于链接的浏览器隔离方法。

盘点所有企业应用

努力程度	- 中
涉及团队	• 安全团队
产品	**安全 Web 网关和 CASB（含影子 IT 发现功能）：** Cloudflare Gateway，Microsoft Defender for Cloud Apps，Netskope Next Gen SWG，Zscaler Internet Access (ZIA)

清点所有企业应用（续）

摘要	对安全团队而言，了解企业使用的全部应用至关重要。安全团队常常会发现企业使用了未经批准或未知的应用，这常被称为“影子 IT”。配备 TLS 解密的安全 Web 网关可用于识别应用。安全 Web 网关也可用于阻止未经批准的应用或应用租户（例如个人 Dropbox 帐号）。
步骤	1. 在安全 Web 网关中启用影子 IT 扫描 2. 确保用户设备上已安装安全 Web 网关客户端 3. 允许 2-3 周的用户流量通过 4. 查看已识别的应用列表 5. 对于任何未经批准的应用，应当使用安全 Web 网关策略加以阻止 6. 对于已批准的应用，应当使用 Zero Trust 策略加以保护

为应用实施 Zero Trust 策略

努力程度	- **低**（对于大部分关键应用） - **高**（对于所有应用）
涉及团队	• 安全团队 • 应用开发团队 • IT 团队
产品	**Zero Trust 反向代理：** Azure App Proxy，Cloudflare Access，Netskope Private Access，Zscaler Private Access (ZPA) **Zero Trust 网络访问 (ZTNA)：** Cloudflare Access，Netskope Private Access，Zscaler Internet Access (ZIA) **CASB：** Cloudflare CASB，Netskope CASB，Zscaler CASB **远程浏览器隔离：** Cloudflare Browser Isolation，Zscaler Cloud Browser Isolation

为应用实施 Zero Trust 策略（续）

摘要	应用必须使用 Zero Trust 策略进行保护，这种策略基于用户身份、设备和网络上下文对访问进行身份验证和授权。应当对应用实施授予最小特权的细粒度策略，尤其是包含敏感数据的应用。有三种主要的应用类型，Zero Trust 安全模型因类型而异。主要的应用类型是： 1. 私有自托管应用（仅在企业网络上可寻址） 2. 公共自托管应用（在互联网上可寻址） 3. SaaS 应用程序 **注：**如果设备上下文或合规状态是要求的安全策略，则通常要求在设备上安装客户端软件。
步骤	**私有自托管应用** 1. 在应用和 Zero Trust 策略层之间建立一条加密隧道。通常这将是“应用连接器”，GRE 或 IPsec 隧道 2. 使私有 DNS 解析器对 ZTNA 设备客户端的用户可用 3. 构建基于用户、设备和网络上下文的策略，以确定谁能访问该应用 **公共自托管应用** 1. 将权威 DNS 或 CNAME 记录移动到应用反向代理 2. 确保关闭应用网络的所有入站端口 3. 构建基于用户、设备和网络上下文的策略，以确定谁能访问该应用 **SaaS 应用程序** 关于为 SaaS 应用实施 Zero Trust 策略，有几个不同的选项 **身份代理** Cloudflare、Netskope 和 Zscaler 提供身份代理，它允许与反向代理自托管应用程序相同的策略执行。这要求将身份代理设置成 SaaS 应用的 SSO 提供商。 1. 移除 SaaS 应用的现有 SSO 集成（如有） 2. 将身份代理与 SaaS 应用集成 3. 确保发送正确的 SAML 属性用于用户创建和更新 4. 创建基于用户、设备和网络上下文的策略

为应用实施 Zero Trust 策略（续）

步骤	**安全 Web 网关和单点登录** 另一种方法是使用现有的单点登录 (SSO) 提供商来控制哪些用户可以或不可以访问 SaaS 应用。然后，通过具有专用 IP 地址的安全 Web 网关，确保仅来自受管设备且通过流量检查的用户能访问 SaaS 应用。 1. 将 SaaS 应用加入到 SSO 提供商 2. 创建策略以确定哪些用户获得授权 3. 将安全 Web 网关实例的 IP 地址加入到 SaaS 应用的 IP 允许列表（大多数 SaaS 应用在其基本安全设置中支持 IP 允许列表） 4. 创建安全 Web 网关策略，以控制哪些用户能访问 SaaS 应用

保护应用以防第 7 层攻击（DDoS、注入、机器人等）

努力程度	- 低
涉及团队	• 安全团队 • 应用开发团队
产品	Akamai，AWS，Azure，Cloudflare，GCP
摘要	任何自托管的应用都容易受到第 7 层攻击，包括 DDoS、代码注入、机器人等。安全团队应该在所有自托管应用（无论是私有还是公共可寻址应用）前部署 Web 应用程序防火墙和 DDoS 保护。
步骤	1. 添加任何公共应用的权威 DNS 记录 2. 启用 Web 应用程序防火墙和 DDoS 保护

启用 HTTPS 和 DNSSEC

努力程度	**- 低**
涉及团队	• 安全团队 • 应用开发团队
产品	Akamai，AWS，Azure，Cloudflare，GCP
摘要	任何自托管的 Web 应用都应该利用 HTTPS 和 DNSSEC。这可以预防任何潜在的数据包嗅探或域劫持。
步骤	1. 添加任何公共应用的权威 DNS 记录 2. 设置 HTTPS 为严格并启用 DNSSEC

数据丢失防护与日志记录

到目前为止，您已经为自己的架构建立了所有 Zero Trust 元素，并将在网络内部运行时产生大量数据。此时应当实施数据丢失防护 (DLP) 和日志记录。这一套流程和工具专注于使敏感数据留在企业内部，并标记任何潜在的数据泄露机会。组织必须首先了解其敏感数据存在于何处。然后，组织可实施 Zero Trust 控制，以阻止敏感数据被访问和窃取。

建立记录和检查敏感应用流量的流程

努力程度	**- 中**
涉及团队	• 安全团队
产品	**安全 Web 网关 (SWG)：** Cisco Umbrella，Cloudflare Gateway，Netskope Next Gen SWG，Zscaler Internet Access (ZIA) **安全信息与事件管理 (SIEM)：** DataDog，Splunk，SolarWinds
摘要	安全 Web 网关解决方案具备将用户流量日志推送至 SIEM 工具的功能。安全团队应该定期检查敏感应用的流量日志。可在 SIEM 中设置针对异常或恶意流量的特定警报，并随时间推移进行调优。
步骤	1. 确保所有发送到敏感应用的用户流量都通过 SWG 进行代理 2. 启用 SWG 和 SIEM 之间的日志推送或拉取功能 3. 设定安全团队查看流量日志的特定间隔 4. 根据随时间推移而取得的发现，在 SIEM 中配置警报

定义敏感数据及其所在位置

努力程度	**- 中**
涉及团队	• 安全团队 • 合规/法律团队
产品	**安全信息与事件管理 (SIEM)：** DataDog，Splunk，SolarWinds

定义敏感数据及其所在位置（续）

摘要	敏感数据因行业而差异巨大。科技公司关心如何保护源代码，而医疗服务机构高度专注于《健康保险可携性和责任法案》(HIPAA) 合规。要点是确定哪些是公司的敏感数据，以及这些数据所在的位置。 敏感数据的准确定义和清单将为实施数据丢失防护工具提供依据。
步骤	1. 在 SIEM 工具或直接在安全 Web 网关查看流量日志，以识别目标应用和数据存储 2. 清点现有敏感数据

预防敏感数据离开应用

努力程度	**- 高**
涉及团队	• 安全团队 • IT 团队 • 合规/法律团队
产品	**内联数据丢失防护 (DLP)：**Cisco Umbrella，Cloudflare Gateway，Netskope Next Gen SWG，Zscaler Internet Access (ZIA)
摘要	内联 DLP 解决方案检查用户流量和文件上传/下载的敏感数据。敏感数据以众所周知的预定义列表提供（例如个人身份信息、社会保险号码、信用卡信息等），也可由管理员手动配置。应对敏感应用启用 DLP 控制，并可扩展到所有用户流量。
步骤	1. 安装来自 DLP 提供商的客户端软件 2. 确保没有会破坏连接性的现有 VPN 或其他工具 3. 确保启用 TLS 解密，且每台用户机器上都存在根证书 4. 启用 DLP 控制 5. 监控 DLP 阻止事件，验证其有效或是否为误报

识别 SaaS 工具中的错误配置和公开分享的数据

努力程度	**- 低**
涉及团队	• 安全团队
产品	**基于 API 的云访问安全代理 (CASB)：** Cloudflare CASB，DoControl，Netskope，Zscaler CSPM
摘要	CASB 通过 API 与主要 SaaS 应用集成。随后，CASB 将扫描 SaaS 应用，检测是否存在已知的安全错误配置和已被公开分享的数据。安全团队应定期查看 CASB 发现。
步骤	1. 根据提供商的 API 集成指引连接每一个 SaaS 应用 2. 对每个 SaaS 应用运行扫描 3. 检查扫描结果，并按需在每个 SaaS 应用程序中开始修复

创建安全运营中心 (SOC)，用于日志检查、策略更新和缓解

努力程度	**- 中**
涉及团队	• 安全团队
产品	**无**
摘要	对 Zero Trust 框架中的安全团队而言，SOC 是一个关键功能。它应该专注于审查日志信息和安全警报，调整所有核心安全产品的 Zero Trust 策略。
步骤	1. 在 SIEM 或直接在安全产品中查看日志 2. 识别任何警报或异常活动 3. 基于检查结果更新每个工具的 Zero Trust 策略

掌握已知威胁行为者的最新状况

努力程度	**- 低**
涉及团队	• 安全团队
产品	**威胁情报提供商：**Cloudflare Radar，CISA，OWASP
摘要	多家提供商专注于编制已知威胁行为者和恶意网站的列表。这些威胁情报源可自动加载到安全 Web 网关中，用于保护用户免受攻击。
步骤	1. 将威胁情报源连接到安全 Web 网关 2. 在 DNS 和 HTTP 过滤中启用威胁防御

稳定状态

一旦为组织的所有其他元素构建了 Zero Trust 架构，就可以采取一系列行动将组织转移到 Zero Trust 稳定状态，确保未来与该架构保持一致。

采用 DevOps 方法来确保对所有新资源执行一致的策略

努力程度	**- 高**
涉及团队	• 安全团队 • 应用开发团队
产品	**基础设施自动化：** Ansible，Puppet，Terraform
摘要	利用基础设施自动化工具，开发人员可将 Zero Trust 安全性作为其应用开发管道的一部分自动部署。建立要求 Zero Trust 反向代理保护的内部测试流程，在部署某个应用时触发。
步骤	1. 定义新应用的标准策略 2. 在应用部署过程中增加要求 Zero Trust 反向代理保护的测试

实施针对接入资源的自动扩展

努力程度	**- 高**
涉及团队	• 安全团队 • 应用开发团队
产品	**负载平衡器：** Akamai，Cloudflare **基础设施自动化：** Ansible，Puppet，Terraform

实施针对接入资源的自动扩展（续）

摘要	负载平衡器是确保个别应用程序基础设施永不过载的有效工具。同时在应用服务开始发生故障时提供一定程度的冗余。 在超过特定流量阈值时，可使用基础设施自动化工具启动新资源。
步骤	1. 在 Zero Trust 反向代理应用连接器前面配置负载平衡器 2. 启用基于用户流量和/或地理位置的负载均衡规则 3. 实现基础设施自动化策略：在特定应用程序集合的流量达到阈值时，配置新的虚拟机

示例实施时间表

每个 Zero Trust 架构部署都是独一无二的，但大多数项目都遵循一组通用的步骤。这个推荐的时间表适用于开始实施 Zero Trust 架构的企业。

时间表		目标	相关产品
第一阶段	☐	部署全球 DNS 过滤	Cisco Umbrella DNS，Cloudflare Gateway，DNSFilter，Zscaler Shift
	☐	监控入站电子邮件并过滤网络钓鱼企图	云电子邮件安全：Cloudflare Area 1 Email Security，Mimecast，TitanHQ 浏览器隔离：Cloudflare Browser Isolation，Zscaler Cloud Browser Isolation
	☐	识别 SaaS 工具中的错误配置和公开分享数据	Cloudflare CASB，DoControl，Netskope，Zscaler CSPM
第二阶段	☐	建立企业身份	Microsoft Azure AD，Okta，Ping Identity PingOne，OneLogin
	☐	对所有应用启用基本 MFA	身份提供商：Microsoft Azure AD，Okta，Ping Identity PingOne，OneLogin 应用反向代理：Microsoft Azure AD App Proxy，Akamai EAA，Cloudflare Access，Netskope Private Access，Zscaler Private Access (ZPA)
	☐	启用 HTTPS 和 DNSSEC	Akamai，AWS，Azure，Cloudflare，GCP
	☐	在 SSL 之后阻止或隔离威胁	TLS 解密：Cloudflare Gateway，Netskope Next Gen SWG，Zscaler Internet Access (ZIA) 浏览器隔离：Cloudflare Browser Isolation，Zscaler Cloud Browser Isolation
	☐	对公开可寻址应用执行 Zero Trust 策略	Zero Trust 反向代理：Azure App Proxy，Cloudflare Access，Netskope Private Access，Zscaler Private Access (ZPA)
	☐	保护应用以防第 7 层攻击	Akamai，AWS，Azure，Cloudflare，GCP
	☐	为应用交付关闭所有对互联网开放的入站端口	Akamai EAA，Cloudflare Access，Netskope，Zscaler Private Access (ZPA)
第三阶段	☐	盘点所有企业应用	安全 Web 网关和 CASB（含影子 IT 发现功能）：Cloudflare Gateway，Microsoft Defender for Cloud Apps，Netskope Next Gen SWG，Zscaler Internet Access (ZIA)
	☐	对 SaaS 应用执行 Zero Trust 策略	Zero Trust 网络访问 (ZTNA)：Cloudflare Access，Netskope Private Access，Zscaler Internet Access (ZIA) CASB：Cloudflare CASB，Netskope CASB，Zscaler CASB

	☐ 隔离用户网络访问	**Zero Trust 网络访问 (ZTNA)：** Cloudflare Zero Trust (Access 和 Gateway 可一起使用)，Netskope Private Access，Zscaler Private Access (ZPA)
	☐ 适用于关键私有可寻址应用的 ZTNA	Cloudflare Access，Netskope Private Access，Zscaler Internet Access (ZIA)
	☐ 实施 MDM/UEM 以管控企业设备	**Mac：** Jamf，Kandji **Windows:** Microsoft Intune
	☐ 定义敏感数据及其所在位置	DataDog，Splunk，SolarWinds
	☐ 发出基于硬件的身份验证令牌	**硬件密钥：** Yubico
	☐ 掌握已知威胁行为者的最新状况	Cloudflare Radar，CISA，OWASP
第四阶段	☐ 实施基于硬件的 MFA	**硬件密钥：** Yubico
	☐ 对所有应用实施 Zero Trust 策略和网络访问	Cloudflare Access，Netskope Private Access，Zscaler Internet Access (ZIA)
	☐ 创建安全运营中心 (SOC)，用于日志检查、策略更新和缓解	不适用
	☐ 实施端点保护	VMWare Carbon Black，Crowdstrike，SentinelOne，Windows Defender
	☐ 清点所有企业设备、API 和服务	**设备盘点：** VMWare Carbon Black，Crowdstrike，SentinelOne，Windows Defender，Oomnitza **API/服务盘点：** Cloudflare 应用连接器，Zscaler Private Access (ZPA)
	☐ 用宽带互联网实现分支机构之间的连接	Cloudflare Magic WAN，Cato Networks，Aryaka FlexCore
	☐ 建立记录和审查敏感应用之员工流量的流程	**安全 Web 网关 (SWG)：** Cisco Umbrella，Cloudflare Gateway，Netskope Next Gen SWG，Zscaler Internet Access (ZIA) **安全信息与事件管理 (SIEM)：** DataDog，Splunk，SolarWinds
	☐ 阻止敏感数据离开您的应用（例如个人身份信息、信用卡、社会保险号码等）	Cisco Umbrella，Cloudflare Gateway，Netskope Next Gen SWG，Zscaler Internet Access (ZIA)
	☐ 采用 DevOps 方法来确保对所有新资源的策略执行	Ansible，Puppet，Terraform
	☐ 实施针对接入资源的自动扩展	**负载平衡器：** Akamai，Cloudflare **基础设施自动化：** Ansible，Puppet，Terraform

010 8524 1783 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3584.2022AUG09