CLOUDFLARE

數位轉型實踐：單一供應商 SASE 解決方案

Marsha Hsu 許庭瑜
SASE 商業發展產品經理
2024/5/16

Agenda

1 數位轉型的挑戰

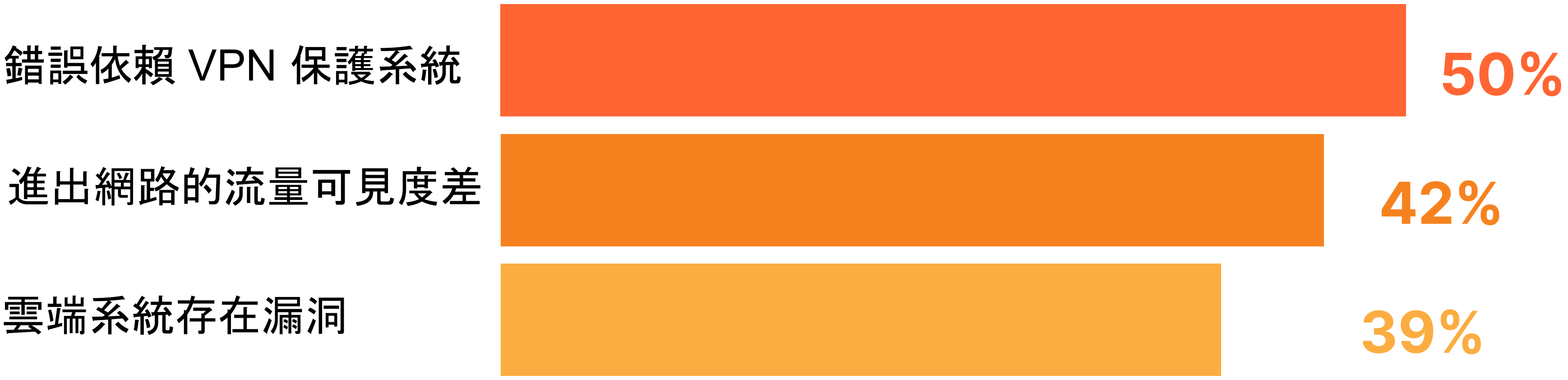
2 攻擊者如何被放行至企業內

3 員工是如何將數據是外流的

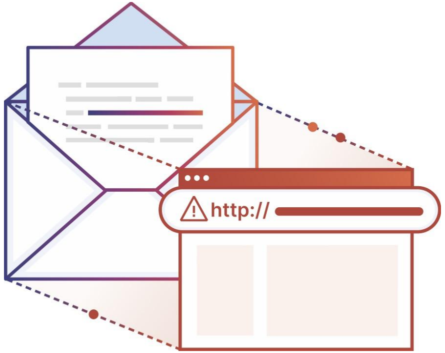
4 如何透過單一供應商解決所有問題

企業面臨全方位的網路安全挑戰

我們調查了亞太區14 個市場的 4千餘名安全決策者:

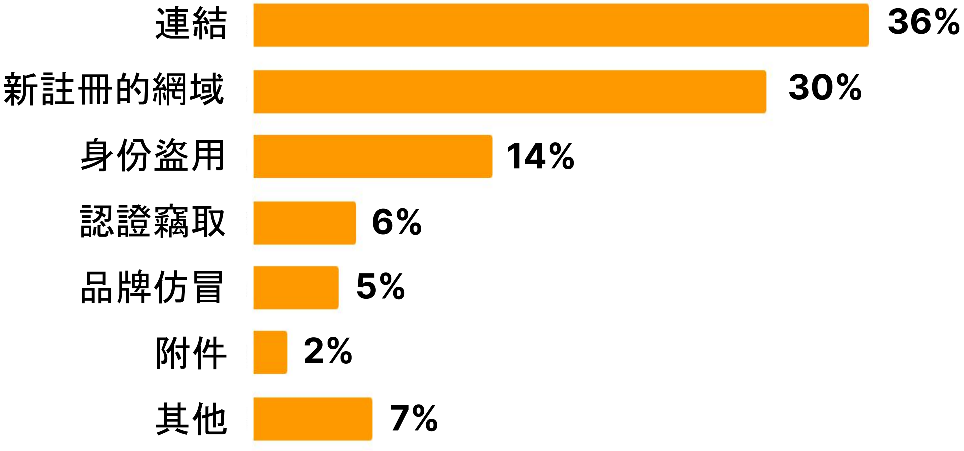


(Source: Cloudflare)



連結是最常被偵測到的網路釣魚威脅

(Results of 2023 Phishing Threats Report)



企業內安全存取 (ZTNA+SWG+RBI) 安全地將使用者連接到對的資源

把檔案分享給媒體的行為，你永遠不知道外流到底是誰幹的！

您對員工使用 SaaS 產品有足夠的可見性嗎？(知道 1 分，不知道 0 分)

1. 銷售管理系統

您是否知道離職的銷售員工匯出多少銷售記錄？

salesforce HubSpot

2. 商務模組

您知道內部文件和資料夾被分享給任何有連結的人嗎？

Google Workspace Microsoft 365 box

3. 身份認證

您知道員工停用了組織的最低密碼強度要求嗎？

okta

4. 企業溝通

您是否會看到組織外部的個人被添加到公司私人頻道？

slack

5. 版本控制

開發人員關閉原本強制代碼審查要求，您會收到警報嗎？

GitHub GitLab

6. 視訊會議

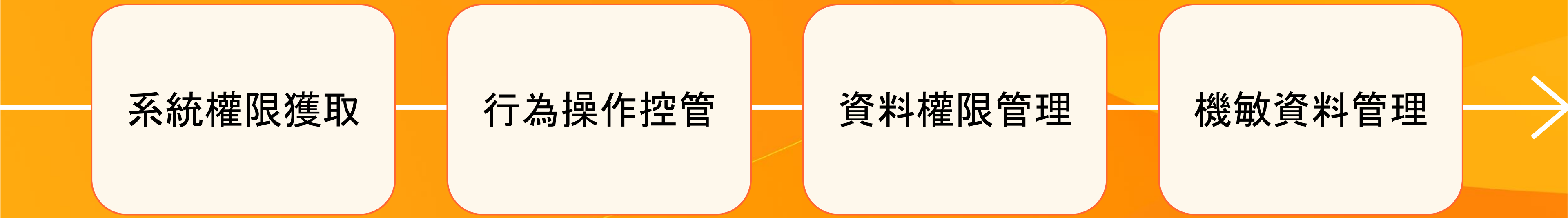
如果您的員工沒使用密碼，您會知道嗎？

zoom

Section

資料是怎麼外流的？

如何杜絕資料外流？



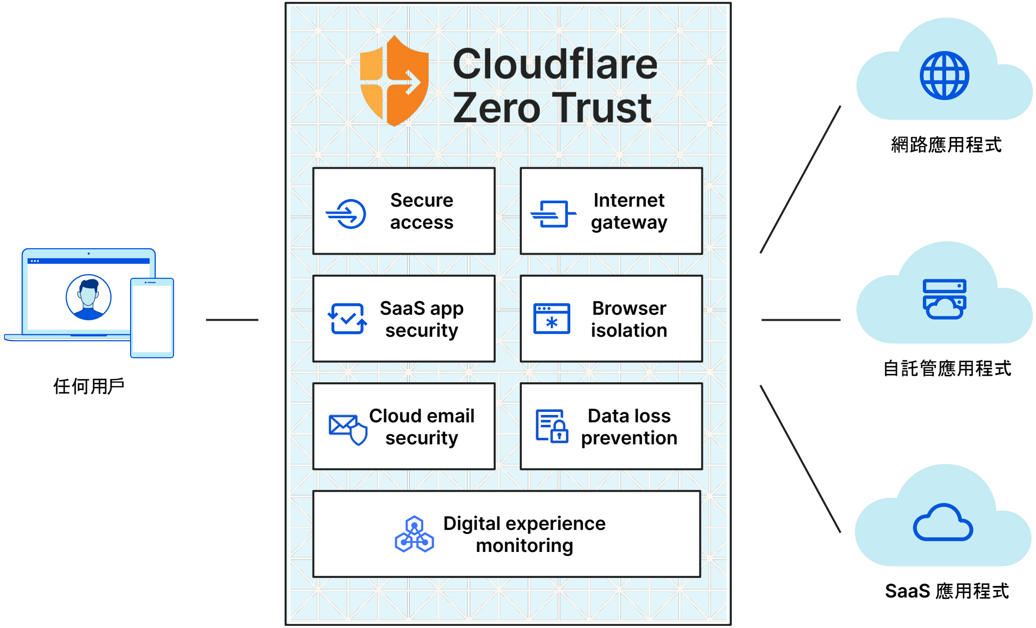
系統權限獲取

行為操作控管

資料權限管理

機敏資料管理

Cloudflare 單一供應商 SASE 解決方案



企業內安全存取

(ZTNA+SWG+RBI)

簡化並安全地將任何使用者連接到任何資源

威脅防禦

(SWG+CES+RBI)

確保您的資料安全，免受任何連接埠和協定的威脅

確保SaaS/PaaS安全

(CES+CASB+ZTNA)

應用程式的可見性和控制

Section

許庭瑜 Marsha Hsu

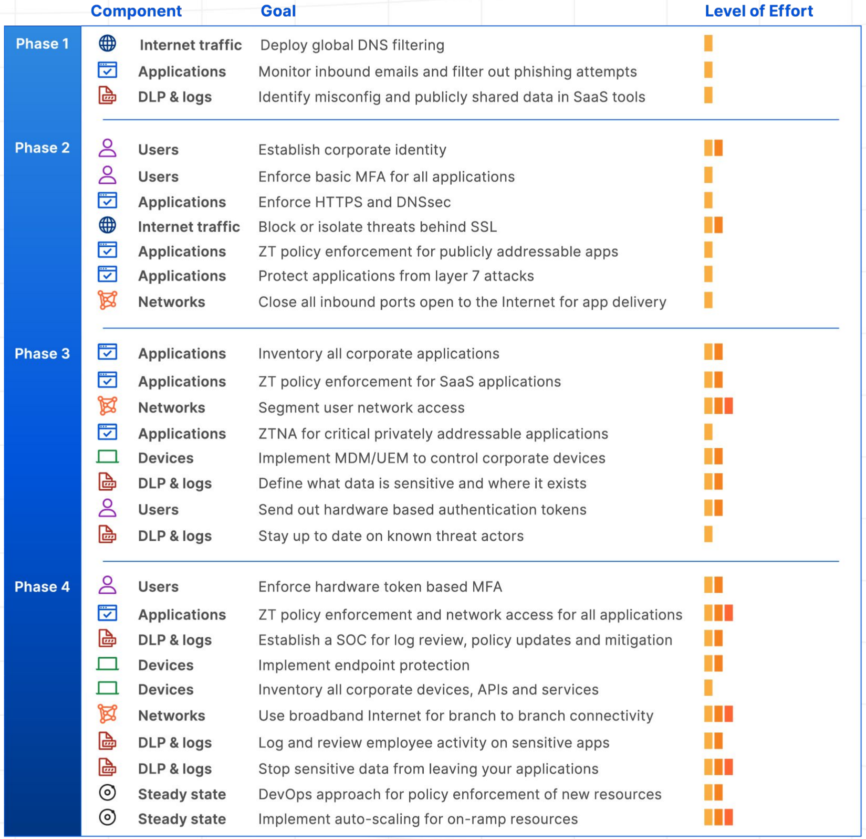
0910911561

marsha@cloudflare.com

Download the complete Roadmap to Zero Trust Architecture

cfl.re/architecture-roadmap

Then, view our specific reference doc: cfl.re/architecture-reference



	Component	Goal	Level of Effort
Phase 1	Internet traffic	Deploy global DNS filtering	▮
	Applications	Monitor inbound emails and filter out phishing attempts	▮
	DLP & logs	Identify misconfig and publicly shared data in SaaS tools	▮
Phase 2	Users	Establish corporate identity	▮▮
	Users	Enforce basic MFA for all applications	▮
	Applications	Enforce HTTPS and DNSsec	▮
	Internet traffic	Block or isolate threats behind SSL	▮▮
	Applications	ZT policy enforcement for publicly addressable apps	▮
	Applications	Protect applications from layer 7 attacks	▮
	Networks	Close all inbound ports open to the Internet for app delivery	▮
Phase 3	Applications	Inventory all corporate applications	▮▮
	Applications	ZT policy enforcement for SaaS applications	▮▮
	Networks	Segment user network access	▮▮▮
	Applications	ZTNA for critical privately addressable applications	▮
	Devices	Implement MDM/UEM to control corporate devices	▮▮
	DLP & logs	Define what data is sensitive and where it exists	▮▮
	Users	Send out hardware based authentication tokens	▮▮
	DLP & logs	Stay up to date on known threat actors	▮
Phase 4	Users	Enforce hardware token based MFA	▮▮
	Applications	ZT policy enforcement and network access for all applications	▮▮▮
	DLP & logs	Establish a SOC for log review, policy updates and mitigation	▮▮
	Devices	Implement endpoint protection	▮▮
	Devices	Inventory all corporate devices, APIs and services	▮
	Networks	Use broadband Internet for branch to branch connectivity	▮▮▮
	DLP & logs	Log and review employee activity on sensitive apps	▮▮
	DLP & logs	Stop sensitive data from leaving your applications	▮▮▮
	Steady state	DevOps approach for policy enforcement of new resources	▮▮
	Steady state	Implement auto-scaling for on-ramp resources	▮▮▮