CYBERARK®
THE IDENTITY SECURITY COMPANY®

AI 驅動的風險：機器身份管理與 TLS 憑證的挑戰

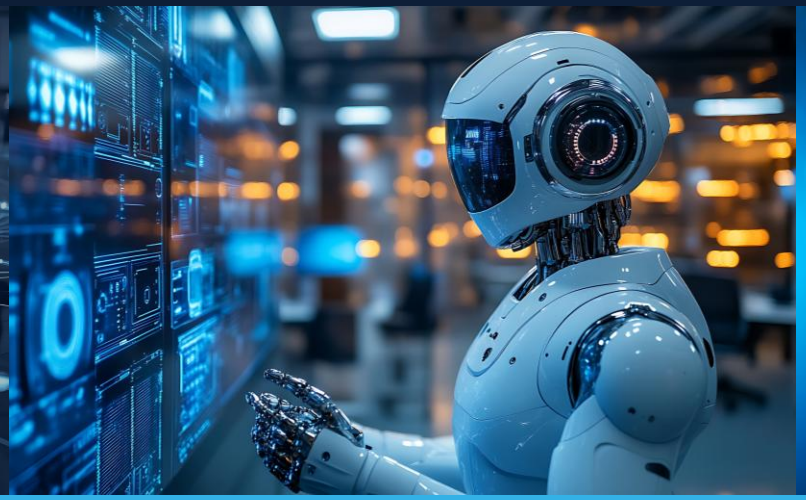
20250415

Billy Chuang

市場趨勢

身分的擴散

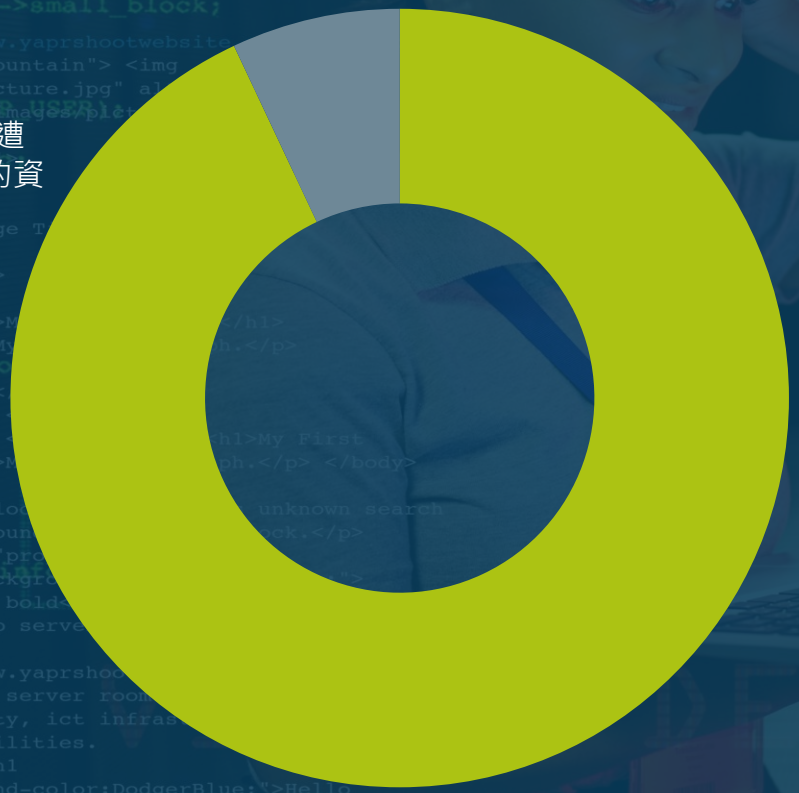
AI 無處不在



機器的崛起

信任的鞏固和平臺化

與身分相關的資安入侵(TWN)



3%
企業在過去 12 個月內遭受過一次與身分相關的資安入侵事件

97%

企業在過去 12 個月內至少遭受兩次與身分相關的資安入侵事件

CyberArk 身分安全威脅態勢報告 2024 (n=100, Taiwan)

各個身分的解決方案

員工

IT

開發人員

機器

保護從端點到應用服務的每一步

員工 & 端點

受管控

未受管控

- 密碼
- 特權
- 瀏覽器

- 生命週期
- 連線
- 存取

原生

SaaS

CYBERARK

生成式AI – 承諾、潛力與危險

CYBERARK®

生成式AI的利與弊(TWN)

AI會帶來負面影響

- AI驅動的惡意軟體
- AI驅動的網路釣魚
- AI模型被攻破導致資料外洩

利用AI加強防禦

- 入侵偵測與防護
  - 進階分析
- 精準的存取控制

相信員工能識別B2B深偽（deepfake）

- 一段顯示你的CEO與罪犯交易現金的影片
- 來自人資部門、財務長、IT主管的影片

CyberArk 身分安全威脅態勢報告 2024 (n=100, Taiwan)

CYBERARK®

生成式AI帶來的迫切影響(TWN)

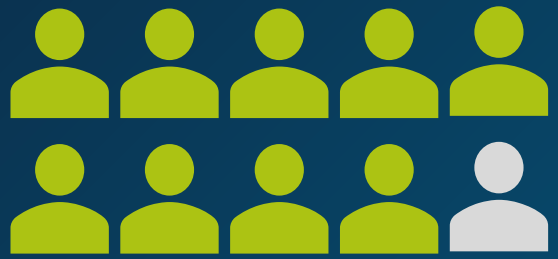
引發身分相關攻擊的三大原因

- 網路攻擊的數量與複雜性 25%
- 脆弱的身分和存取管理（IAM）基礎設施 22%
- 第三方和外部廠商 22%

在過去的12個月中，由網路釣魚和語音釣魚發起的攻擊

9 / 10

的企業組織



遭受入侵

預期AI帶來的三大負面影響

- AI模型被攻破導致資料外洩 43%
- AI驅動的資料集中毒/對抗效應 42%
- AI生成程式碼 37%

我們可以預期100%的企業將很快被AI驅動的網路釣魚攻擊鎖定並入侵

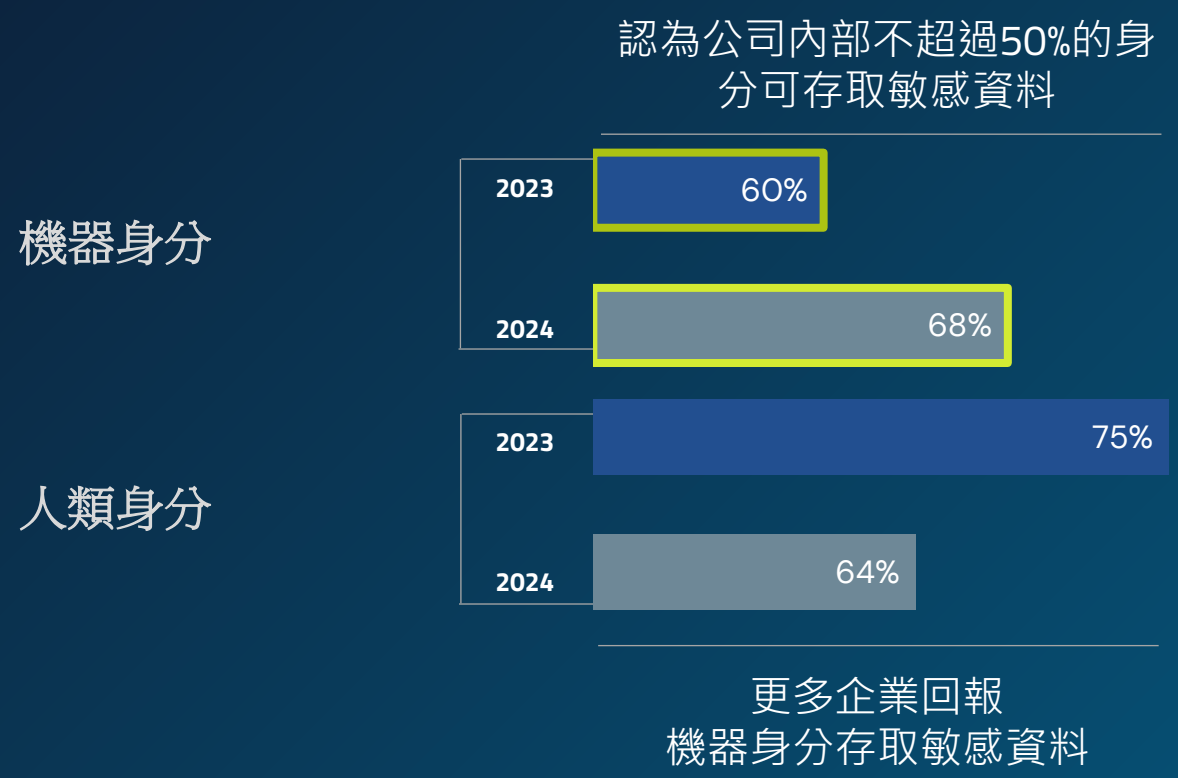
CyberArk 身分安全威脅態勢報告 2024 (n=100, Taiwan)

CYBERARK®

CYBERARK®

機器崛起

更多機器身分能存取敏感資料(TWN)



機器身分安全被嚴重忽略

CyberArk 身分安全威脅態勢報告 2024 (n=2,400, 18 國家)

CYBERARK®

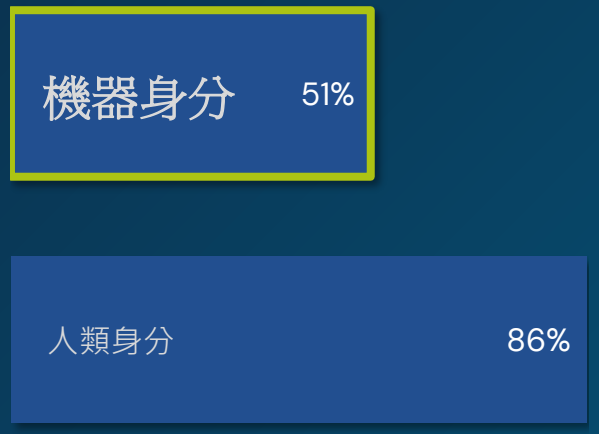
快速孳生且不安全的機器身分帶來的危險(TWN)

機器身分是成長最快的
身分種類 (34%)

#1

機器身分是
最危險的身分種類
(50%)

認為公司內部不超過50%的身
分可存取敏感資料



約一半企業回報
機器身分存取敏感資料

未受保護的機器身分
是一種風險

機器身分相關問題將導致
大量人工作業

機器身分**在入侵事件後**
的投資處於低順位

機器身分安全被嚴重忽略

CyberArk 身分安全威脅態勢報告 2024 (n=100, Taiwan)

CYBERARK

保護機器身分越來越挑戰

關鍵驅動因素增加了風險和複雜度

數量

- 工作負載和機器數量呈爆炸式增長 – AI, IoT, 雲端
- 數量超過人類身分 (45:1), #1 新身分的驅動力
- 大量積壓的為管控憑證和秘密資訊

多樣性

- 多種憑據類型， 例如憑證、秘密資訊、令牌
- 多種環境，例如雲原生、多雲、混合
- 廣泛的工作負載/應用，例如 CSP、K8s、.Net、Java、第三方商用軟體

速度

- 快速開發，例如DevOps、CI/CD、AI Copilot
- 臨時工作負載，彈性擴展

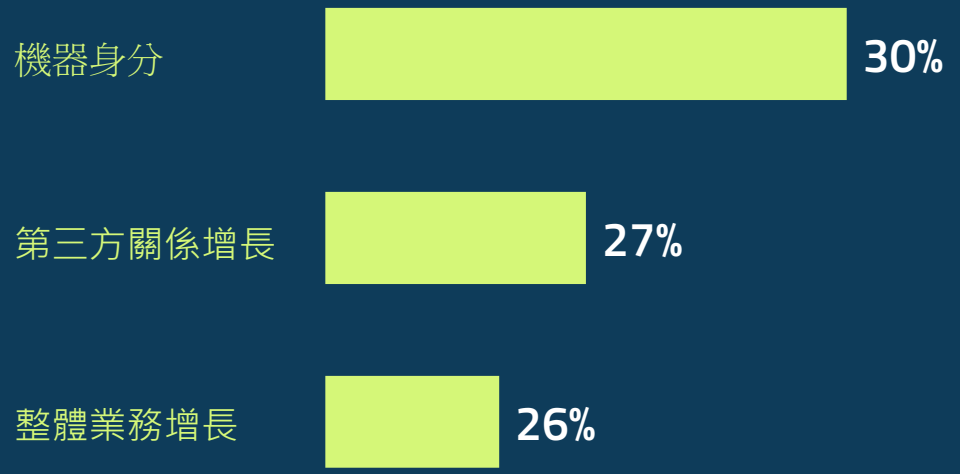
CYBERARK

保護所有機器身分是關鍵

更多機器身分

45 個機器身份對應一個人類身份*
導致攻擊面擴大

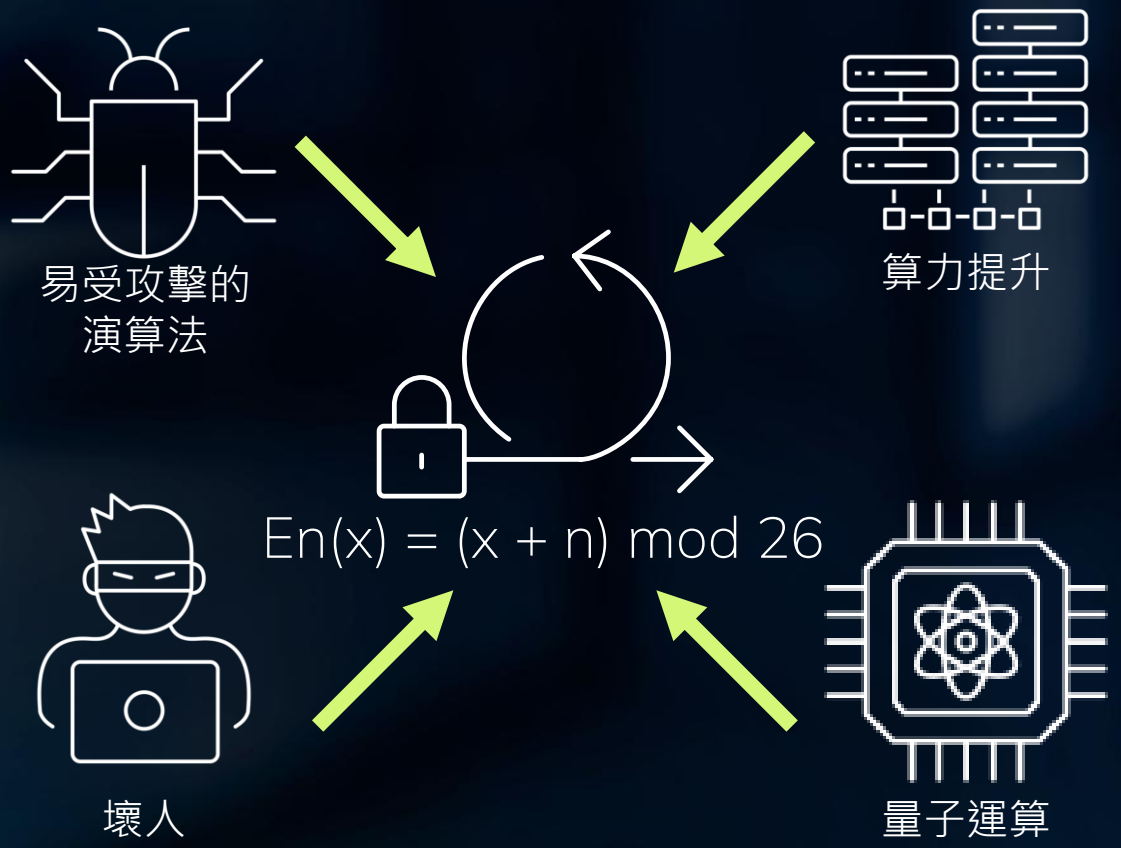
機器身分是整體身分增長的 #1 驅動因素



* From Global survey of 1,750 security decision makers
** CyberArk - Identity Security Threat Landscape Report 2024

對加密敏捷性的需求– 後量子密碼學

密碼學: 受到持續的威脅



密碼學從根本上說是基於創建複雜的數學問題，如果沒有密鑰，電腦很難解決這些問題

運算的能力和速度一直在不斷提高！

量子電腦的工作方式與我們今天所知道的二進位電腦不同

這種超越二進位比對的能力將使一些加密演算法易於解決！

CYBERARK

源於 TLS 憑證問題造成的營運中斷很常見

Certificate-Related Outages | July 10, 2023 | 3 minute read

Expired SSL Machine Identity Wreaks Havoc at Bank of Ireland

HOT POD / TECH / CREATORS

Massive podcast outage caused by Spotify's failure to renew security certificate

/ Podcasts hosted on Megaphone were unavailable on Spotify and

CeptBiro @CeptBiro · 13 Apr 2021

Expired certificate caused a Pulse Secure VPN global scale outage
securityaffairs.co/wordpress/1167...

#Infosec #Secinfo #Security #Ceptbiro #Cybersecurity
#ExpiredCertificate #PulseSecure #VPN

Microsoft 365 Status @MSFT365Status

We've determined that an authentication certificate has expired causing, users to have issues using the service. We're developing a fix to apply a new certificate to the service which will remediate impact. Further updates can be found under TM202916 in the admin center.

11:19 PM · Feb 3, 2020

Elon Musk @elonmu... · 4h

Sorry, slight glitch with @SpaceX Starlink. Coming back online now.

2,082 1,768 19.4K 2.9M

Elon Musk @elonmu... · 4h

Caused by expired ground station cert. We're scrubbing the system for other single-point vulnerabilities.

941 704 8,605 1.6M

營運中斷代價高昂

NEWS

Expired certificates cost $15 million per outage

The average global 5,000 company spends $15 m certificate outage

The average global 5,000 company spends about $1 from the loss of business due to a certificate outage $25 million in potential compliance impact.

These estimates, based on a Ponemon survey of abo respondents, include remediation costs, loss of produ and brand image damage.

This past April, for example, Instagram forgot to rene

O2 reportedly seeking tens of millions in compensation from Ericsson for outage

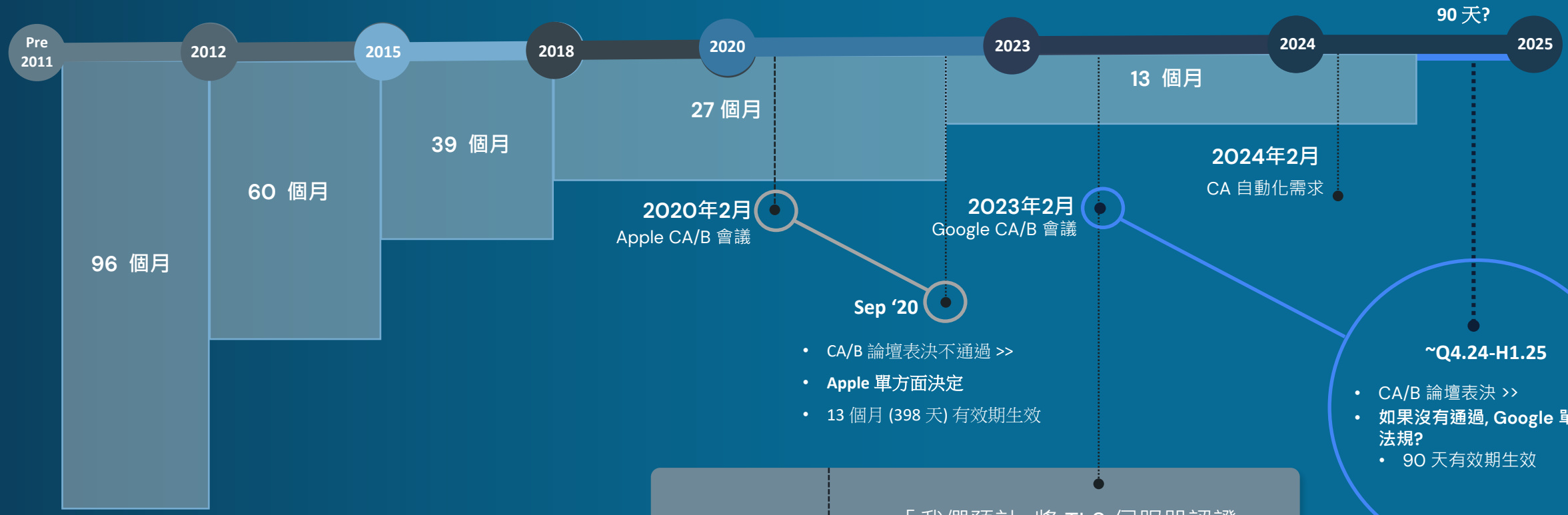
UK media has reported that O2 will be seeking up to £100 million in damage from Ericsson following the mobile data outage last week.

O2 is reportedly seeking tens of millions of pounds in compensation from Swedish networking giant Ericsson following the nationwide mobile data ou last week, which was caused by an expired software certificate.

According to a report by *The Telegraph*, O2 and parent company Telefonica negotiate with Ericsson over the bill, which the publication understands to b around the £100 million mark.

The Guardian reported that Telefonica O2 UK CEO Mark Evans will meet wit Ericsson executives this week to discuss the latter's software, as well as how

Google: 90 天憑證有效期是未來



一起邁向未來

「我們預計...將 TLS 伺服器認證的憑證最長有效期從 398 天縮短為 90 天」

– Google

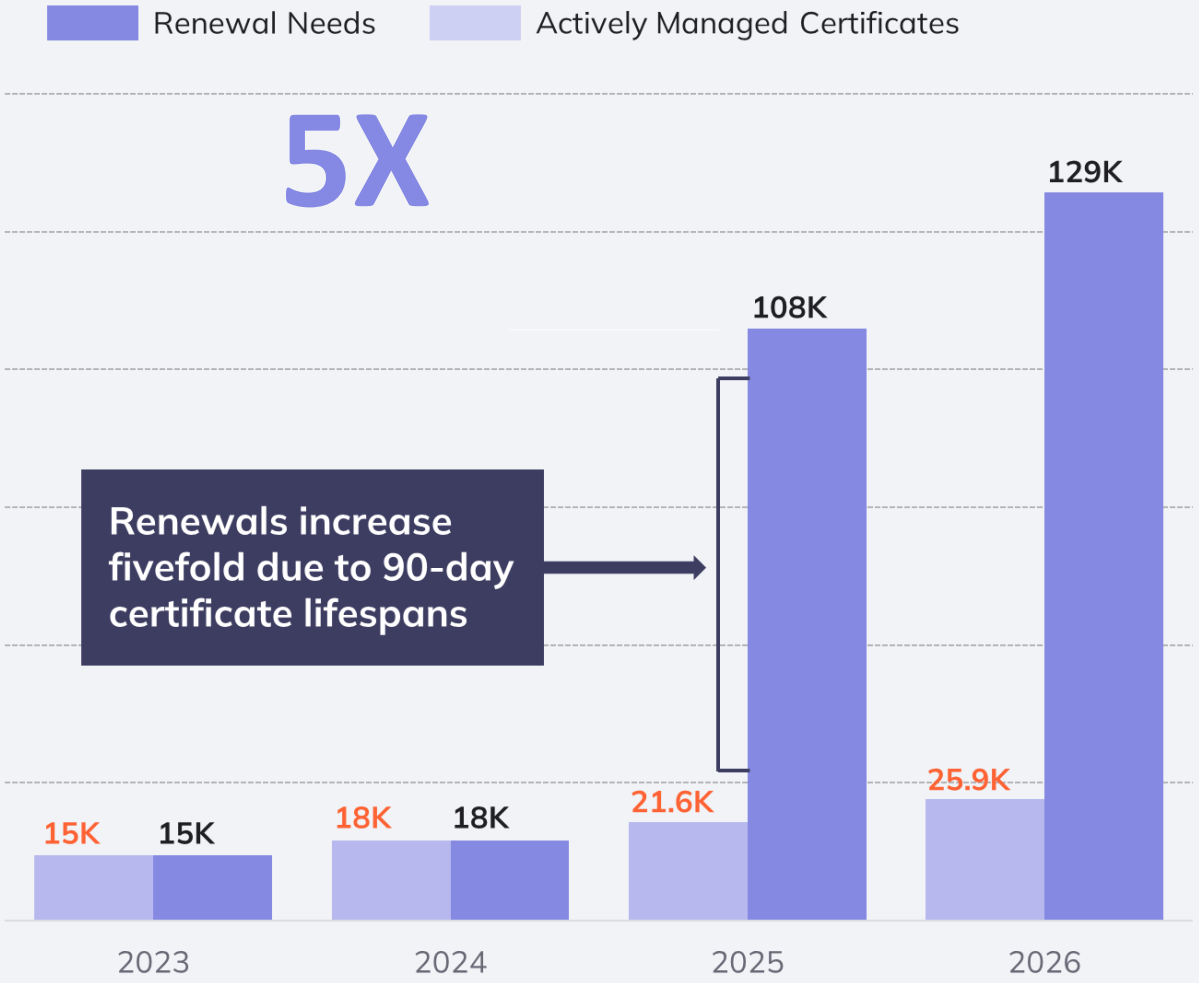
- 著眼 ACME Feb '20
- 66% 瀏覽器市場佔有率
- 內部使用 90 天有效憑證

https://cabforum.org/uploads/11-Apple-Root-Program-Update.pdf

https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/

CYBERARK

影響：90 天有效期



最少更新 5 次:

一年 365 天，而不是 360 天，這意味著您無法擺脫 90 天4次的更新

更新日期一直持續到最後一天是不安全的，所以**實際上它接近 76 天！**

CYBERARK

The Register®

Sysadmins rage over Apple's 'nightmarish' SSL/TLS cert lifespan cuts plot

Max validity down from 398 days to proposed 45 by 2027

Jessica Lyons

Tue 15 Oct 2024 // 19:45 UTC

Apple wants to shorten SSL/TLS security certificates' lifespans, down from 398 days now to just 45 days by 2027, and sysadmins have some very strong feelings about this "nightmarish" plan.

As one of the hundreds that took to Reddit to lament the proposal said: "This will suck.

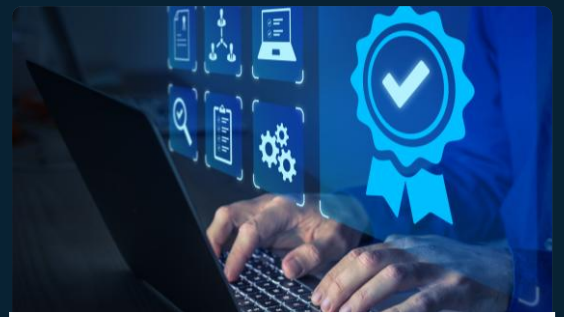
Apple's proposal, if accepted, would shorten the max certificate lifespan to 200 days after September 2025, then down to 100 days a year later and 45 days after April 2027. The ballot measure also reduces domain control validation (DCV), phasing that down to 10 days after September 2027.

Essentially, if the measure is approved by the browser makers and certificate issuers, new TLS certs – needed for things like HTTPS connections to websites – will need to be replaced more often by site owners for web browsers to trust them.

保護憑證和 PKI 的 4 個主要挑戰

停機和業務中斷

- 憑證過期導致收入和客戶損失，聲譽和品牌受損



手動憑證管理

- 手動流程會導致人為錯誤和更高的成本
- 憑證生命週期不斷縮短，複雜性增加
- 憑證簽發機構需要更新救火的問題

傳統 PKI 成本和風險

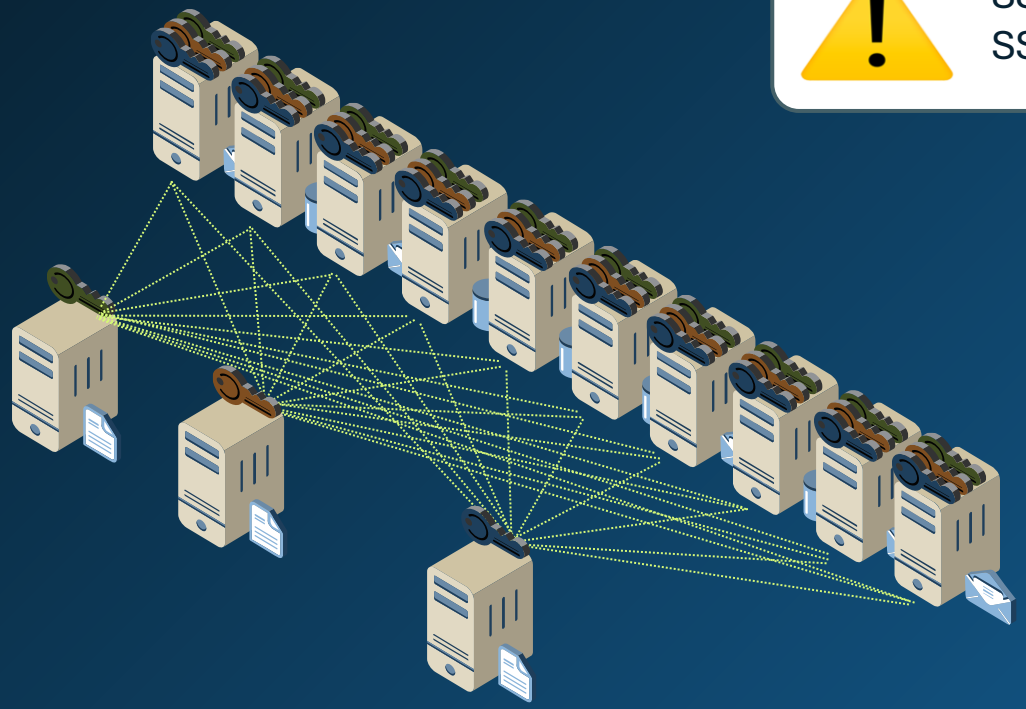
- 傳統 Windows PKI 無法擴展和滿足動態雲環境和行動裝置的需求
- 不必要的高風險和運營成本

安全性、合規性和稽核失敗

- 違規風險、代價高昂的停機時間、安全漏洞和潛在的罰款

CYBERARK

使用 SSH 密鑰進行伺服器到伺服器身分驗證的挑戰



SSH 密鑰集通常在構建系統時發放或通過自動化分發
SSH 密鑰永不過期，很少輪換或刪除

機器→機器

3台機器

– 協作 –

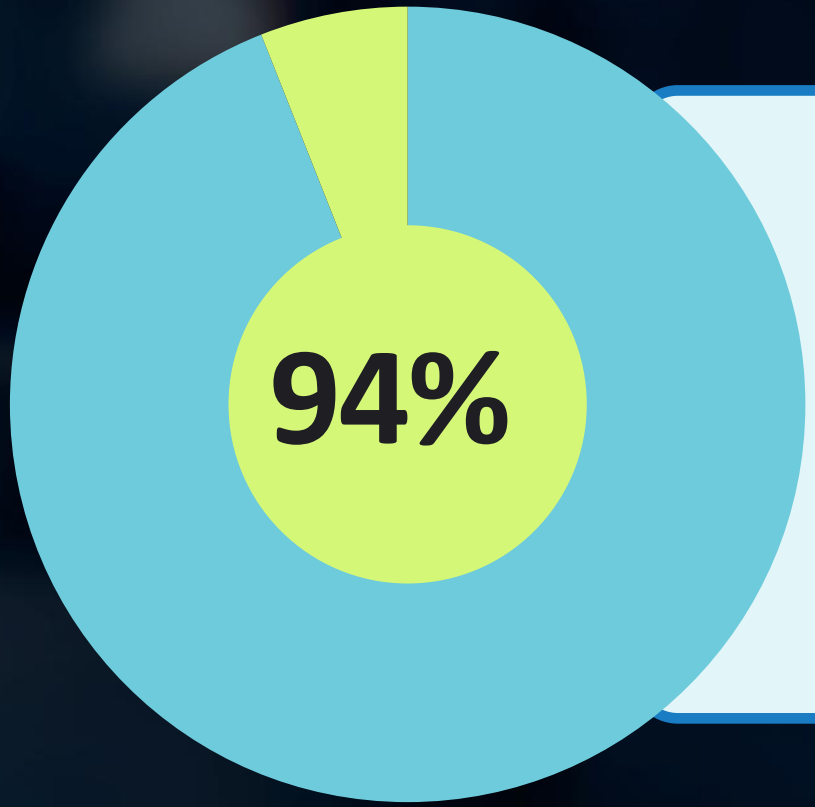
10 台其他機器

有 3 個唯一的密鑰集，但已建立 30 個信任關係！

在企業環境中，經常會看到密鑰（公鑰 + 私鑰）達到數百萬個！

CYBERARK®

Kubernetes 的資安事件呈上升趨勢



…在過去 12 個月內，在其 Kubernetes 環境中至少通報一次資安事件

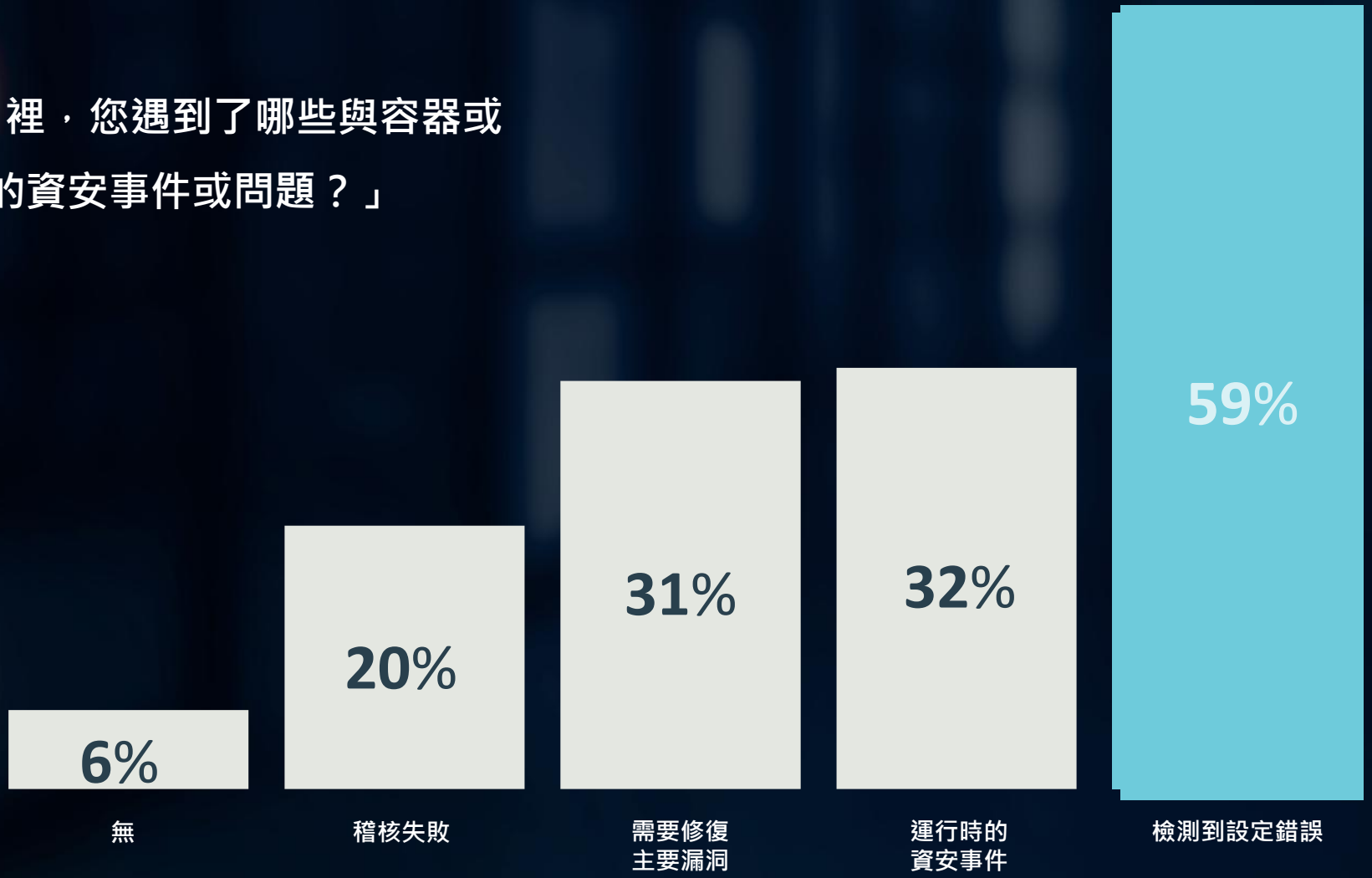
但是為什麼？

Palo Alto Networks State of Kubernetes Report 2021.

CYBERARK®

資安事件的原因

「在過去的 12 個月裡，您遇到了哪些與容器或 Kubernetes 相關的資安事件或問題？」



Data from Red Hat State of Kubernetes Report 2021.

CYBERARK

Kubernetes 也不能倖免

機器身分

$15M
每次營運
中斷損失

憑證設定錯誤是 Kubernetes / OpenShift 的
頭號資安挑戰

Data from Red Hat State of Kubernetes Report 2021.

CYBERARK

CyberArk 提供可觀察性、一致性、可靠性和自由選擇

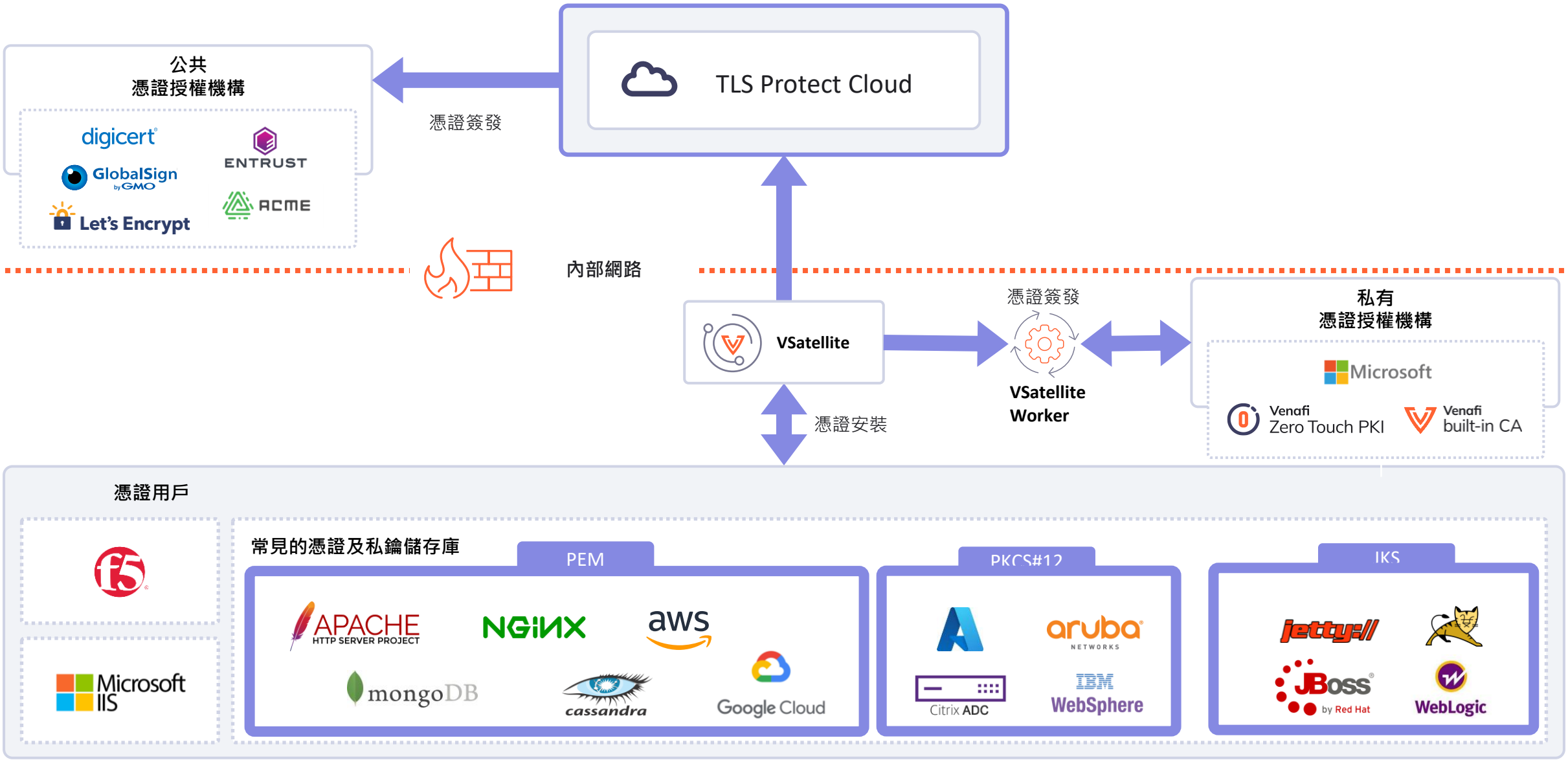
TLS Protect

SSH Protect

- 快速識別所有 TLS 密鑰和憑證
- 持續監控和驗證憑證是否有效、安裝和運行正常
- 自動化整個密鑰和憑證管理生命週期
- 自動化 SSH 憑證的生命週期以落實更好的控制和管理
- 無與倫比的合作夥伴生態系統

CYBERARK®

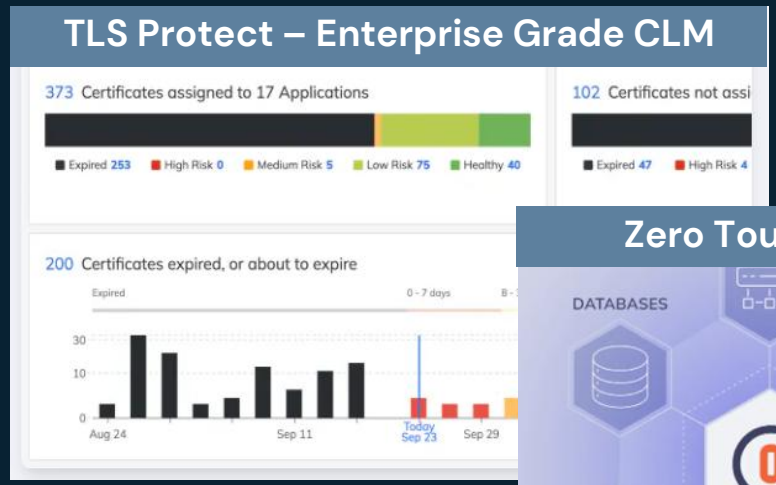
主動自動安裝


公共
憑證授權機構
digicert
ENTRUST
GlobalSign by GMO
ACME
Let's Encrypt
憑證簽發
TLS Protect Cloud
內部網路
VSatellite
憑證簽發
VSatellite
Worker
憑證安裝
私有
憑證授權機構
Microsoft
Venafi
Zero Touch PKI
Venafi
built-in CA
憑證用戶
常見的憑證及私鑰儲存庫
PEM
APACHE
HTTP SERVER PROJECT
NGINX
aws
mongoDB
cassandra
Google Cloud
PKCS#12
aruba
NETWORKS
Citrix ADC
IBM
WebSphere
IKS
jetty://
JBoss
by Red Hat
WebLogic
Microsoft
IIS

CyberArk 解決方案:

保護憑證和 PKI

1. 自動查找、保護和更新憑證
2. 使用 SaaS 降低傳統 PKI 的風險、成本和低效率
3. 使CyberArk PAM客戶能夠輕鬆保護CLM和PKI流程（具有開箱即用的整合）
4. 降低任何機器、團隊或環境中憑證管理的複雜性。



機器身分應用案例

機器身分

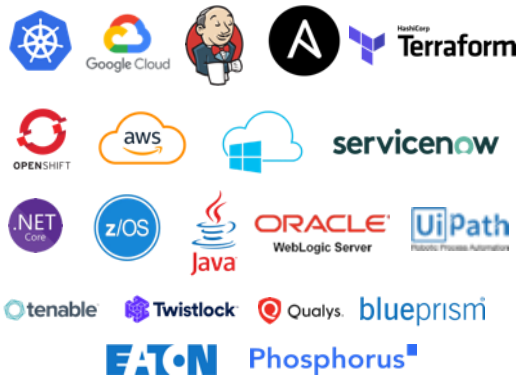
- SSL/TLS 憑證
- SSH 密鑰和憑證
- 行動裝置憑證
- Kubernetes 憑證
- 數位簽章
- IoT 憑證
- JSON Tokens
- SPIFFE

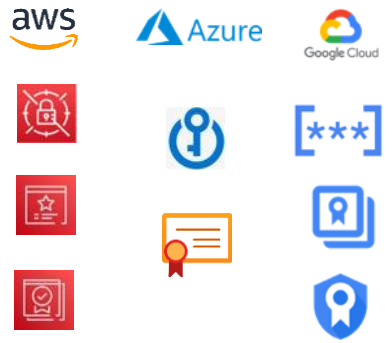
CYBERARK®

機器身分安全解決方案

CyberArk 機器身分安全解決方案

保護所有秘密資訊	保護憑證及PKI	保護雲端上的秘密資訊及憑證	保護 K8S 應用
集中管理端雲、混合雲、 CI/CD 、自行開發及商用第三方軟體中的秘密資訊	集中自動化管理及更新由 CA & PKI 簽發的憑證	集中盤點及保護雲原生中的秘密資訊及憑證，支援管理者使用原生工具	動態簽發及管理 K8s叢集內的憑證及秘密資訊





CYBERARK

現在，客戶可以更有效地保護所有機器身分

從憑證到秘密資訊和管理者存取

降低成本

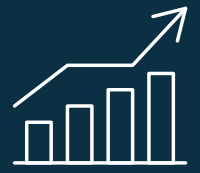
通過自動化流程避免代價高昂的服務中斷

- 防止過期的憑證、被盜的憑證和資安事件導致中斷。
- 避免因應用系統憑證和 CI/CD 流水線洩露而造成的資安事件
- 自動化數位憑證的生命週期，簡化流程並確保可重複性

更快地降低風險

在所有環境中保護秘密資訊和憑證

- 保護和管理所有類型的機器身分，包括應用程式、工作負載、CI/CD 以及雲和混合環境的密鑰
- 自動化 CLM 和密鑰載入; 通過滿足開發人員和使用者「所在位置」的靈活解決方案加速用戶採用
- 滿足合規性要求



提高效率

自動化、簡化管理者對IT資源的存取

- 通過靈活的解決方案實現自動化
- 統一所有身分管理 - 從員工到憑證、秘密資訊和 IT 資源
- 大幅地減少負責機器身分安全的團隊（運營、開發人員、DevOps、雲工程師、 PKI、憑證管理者、IT 等）的負擔

CYBERARK®

Thank You!