safetica®

Safetica

資料外洩防護產品簡介

Data Loss Prevention

您公司的業務以數據資料為主。當重要或敏感性資料外洩或被偷盜時，公司的聲譽，競爭優勢和盈利能力都會受到損害； 更甚者，也可能要承擔法律責任。

數據洩露的平均成本為386萬美元。*

60% 的小公司在重要資料丟失後 6 個月內歇業。**

Safetica DLP 可以防止數據外洩，協助您易於遵守資料保護法規，並保護您的業務免受於人為疏失的影響。

Safetica 是一種易於使用的數據外洩防護（DLP）解決方案，並且提供親民的價格於所有規模的公司。

* 2018 Cost of Data Breach Study Global Overview, Ponemon Institute, July 2018

** How Data Breaches Affect Small Businesses, withlayr.com, August 2017

Safetica 如何協助您?

防止資料丟失及協助事件調查

無論存儲在何處或誰在使用，Safetica 都能保護您的公司數據免遭洩漏。

- 個人隱私資料
- 公司營運重要文件
- 客戶資料
- 卡交易資料，例如：信用卡號
- 智慧財產，例如工業設計、營業秘密、及 know-how
- 商業合約

協助法規遵循

Safetica 協助您遵守法律規範和及數據保護標準。

- GDPR
- HIPAA
- SOX
- PCI-DSS
- GLBA
- ISO/IEC 27001
- CCPA

防止人為疏失

即使是優良員工，也有可能會犯粗心大意的錯誤，使您的業務面臨風險。使用 Safetica，您可以教育員工如何處理敏感性資料，而無需更改他們的工作方式。

為什麼 Safetica 是獨特的?

使用方便，快速部署

Safetica可協助您簡單且快速地佈署到端點，無需額外的專責人員或硬體。

您僅需通透過預設定義的安全通道和基本安全策略的點選，即可在幾數小時內完成保護您最敏感的資料及檔案的工作。

清晰的資料流向

無論在何時、何地以及如何使用您的敏感性資料？ Safetica 為您提供了清晰的資料使用情況及其流向，從而可以保護您最有價值的營業機密。

Safetica 如何保護您?

SAFETICA DISCOVERY 協助發現資料風險與審核

即使是優良員工識別企業內部資料的使用方式、存儲何處、及其傳遞方式，防止故意洩漏並提供審核日誌。幫助企業發現所有內部資料流程並調整您的業務環境。Safetica Discovery可協助您了解隱藏的風險，使您的組織擁有更好資料安全防護。

SAFETICA PROTECTION 協助資料防護與教育

Safetica Protection可為整個公司創建一個安全的環境，對您的員工進行教育，確定風險並保護您的數據。

明確的資料保護政策

透過選擇期望的工作流程與預設的防護方式 – 通知或阻擋，來設定個人或群組資料安全保護政策。

建立員工處理敏感性資料的信心

當使用者可能違反資料保護政策時，顯示通知。

監控所有已連線設備

禁止可攜式行動裝置及未授權使用媒體連接。監控行動裝置設備及持續性監控 Office 365 資料流向。

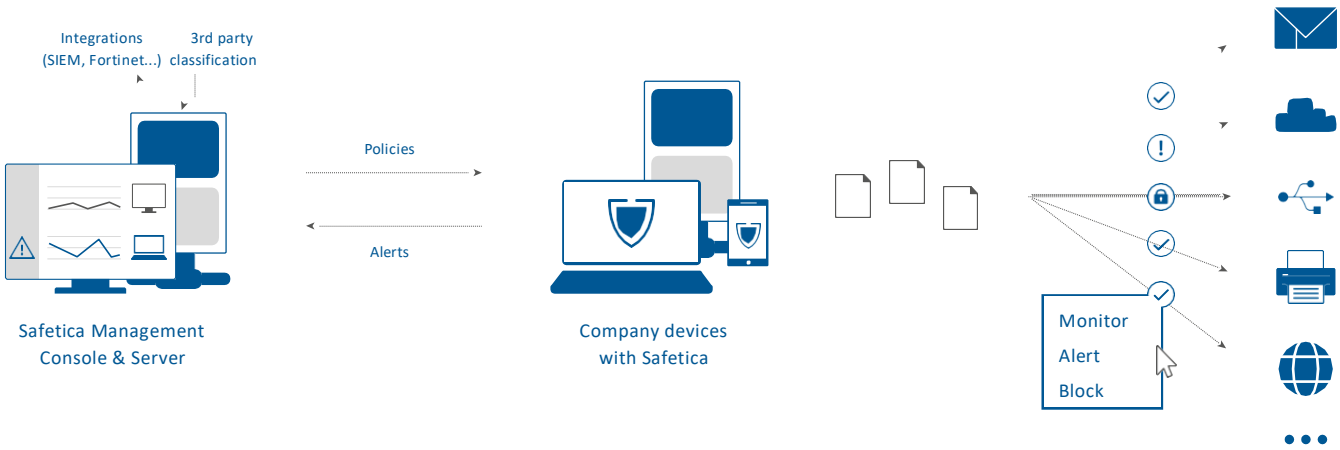
完整連線離線防護

防護公司連線或離線設備的重要資料，無論設備是否連上網路。所有蒐集的記錄將會在下次設備連線後同步。

端點、雲端、閘道整合式防護

Safetica 可監控 Windows和macOS上的資料使用情況。整合Office 365或Fortinet網絡設備以獲得對未知設備的延展控制。使用Safetica Mobile可以從一個地方管理公司的移動設備。

Safetica 如何運作?



Safetica 伺服器運行含有工作站活動和安全日誌的數據庫。系統管理者使用Safetica 管理平台，可以管理安全策略並顯示所有收集到的記錄。

Satetica 客戶端代理程式記錄所有操作且安全策略可套用在工作站、筆記型電腦、平板電腦、及智慧手機。

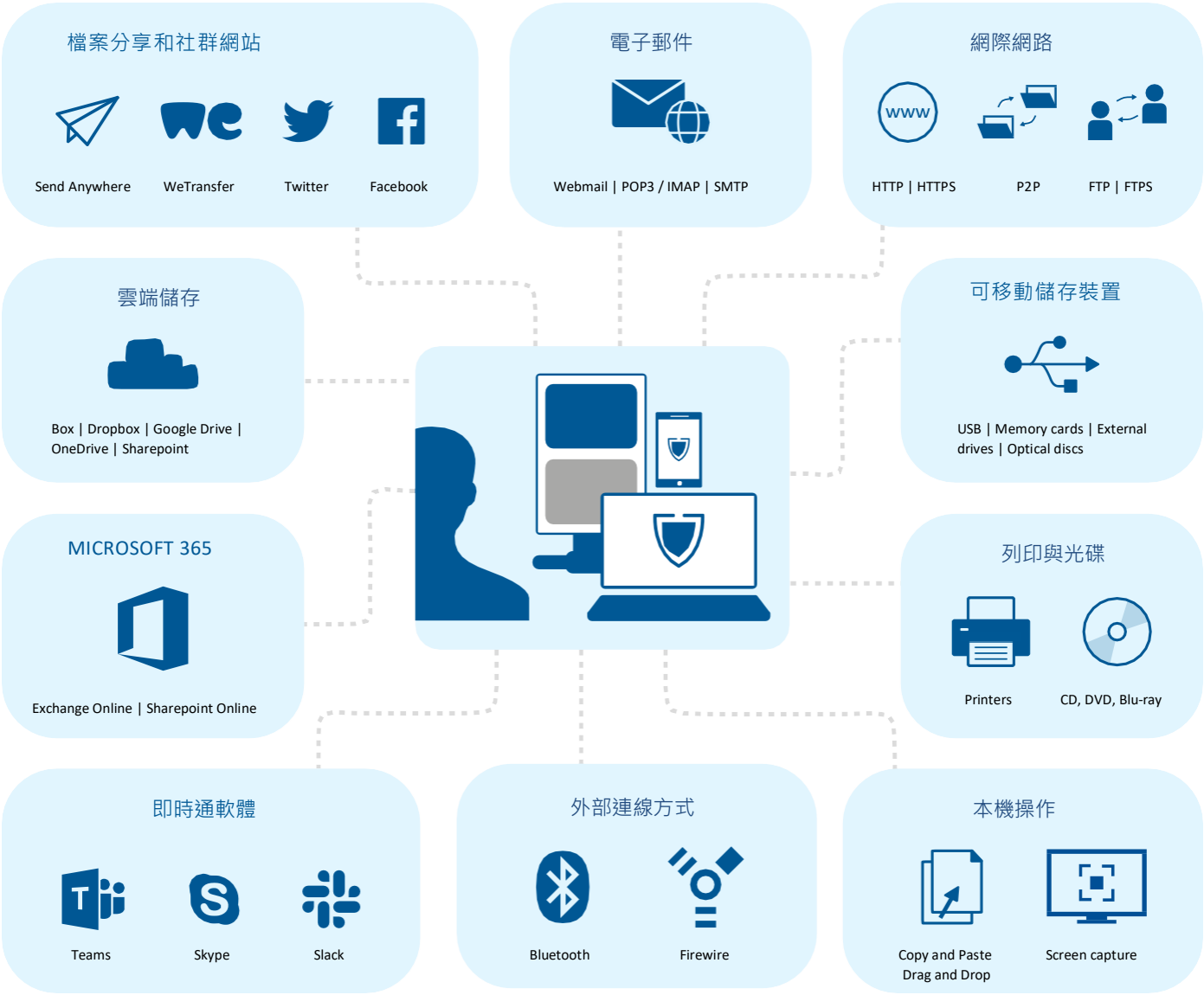
對敏感性資料可能的流出管道，進行防護

關鍵功能

Safetica 可以識別何時有人冒充企業的機密信息。根據 Safetica 的運作方式，它可以阻止危險活動，通知管理員；或提醒您的同仁有關企業的資料防護安全準則。

Safetica 防護的資料通道

Safetica可以跨多平台和資料流管道進行防護，確保無論資料在何處都可以受到保護。



強大的報表功能

Safetica 為您提供快速且單一管理界面中，並顯示及概述所有可能的威脅。您可以隨時透過任何設備（甚至是智慧手機）接收有用的訊息，也可以通過電子郵件或SIEM接收有關可疑行為的告警，並將任何數據顯示到儀表板或將其導出到XLS或PDF作進一步處理分析。

技術需求

SAFETICA 伺服器

- 2.4 GHz 或以上八核處理器
- 16 GB RAM 或以上
- 200 GB 或以上可用磁碟空間
- 支援實體、虛擬或雲端主機
- 需要連結到 MS SQL 2012 或以上資料庫伺服器或 Azure SQL

MS SQL (Safetica 伺服器資料庫)

- 2.4 GHz 或以上八核處理器
- 16 GB RAM 或以上
- MS SQL 2012 或以上資料庫伺服器或 Azure SQL
- 500 GB 或以上可用磁碟空間(依蒐集資料數量增加)
- 支援實體、虛擬或雲端主機

SAFETICA 客戶端

- 2.4 GHz 或以上八核處理器
- 2GB RAM 或以上
- 10 GB 可用磁碟空間

  MS Windows 7, 8.1, 10
  (32-bit [x86] or 64-bit [x64])
- MSI 安裝套件
- .NET 4.5.2 或以上

MAC OXS 客戶端

- 2.4 GHz 或以上八核處理器
- 2GB RAM 或以上
- 10 GB 可用磁碟空間
- macOS 10.15 或以上

Safetica 產品組合

PRODUCTS

Safetica
Discovery

Safetica
Protection

Safetica
Enterprise

EXTRA MODULES

Safetica UEBA

Safetica Mobile

Safetica 其他模組

透過導入Safetica 其他模組進一步強化企業內部資料防護解決方案。

SAFETICA UEBA (使用者和實體行為分析)

– 了解使用者真正的活動及行為

– 全面的了解使用者的工作情況

– 洞察使用者行為進一步防護資料及工作空間

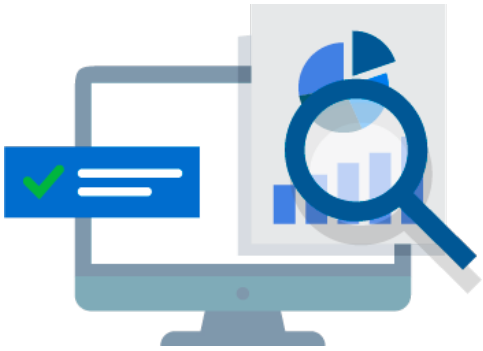
SAFETICA MOBILE

– 保護行動裝置的資料，例如智慧手機和平板電腦

– 了解行動裝置狀態以識別風險

– 審核應用程式和網站的活動

SAFETICA DISCOVERY



- 了解公司的敏感性資料流向
- 所有重要營業資料的詳細使用報告
- 基本使用者行為記錄
- 資安及法規遵循稽核
- 可於數日內發佈第一份資料安全報告

SAFETICA PROTECTION

- 融合了資料分析 (Data Analystics)、資料分類 (Data Classification) 、和資料外洩防護 (Data Loss Prevention; DLP) 功能的多合一安全解決方案
- 完整控制敏感性資料
- 定期安全通報及即時事件告警
- Safetica 區域 (Zones) 可簡化機敏資料安全性防護
- 易於部署、無感使用

SAFETICA ENTERPRISE

- 資料保護解決方案以利完善 IT 資安防護
- 自動化整合第三方解決方案並提供進階資安防護能力
- 支援多網域環境 (Multi-Domain)、流程控制 (Process Control)、及 工作流程 (Workflow)

Safetica Complete Documentation
go.safetica.com/complete_documentation

Safetica 功能概述

Compatibility on	Safetica Discovery	Safetica Protection	Safetica Enterprise
Security Audit	✓	✓	✓
Data-flow security audit Security audit of data-flow in all channels, including external devices, web upload, email, instant messaging, print, and cloud drives.	✓	✓	✓
Office 365 file and email audit Audit of file operations and outgoing email communication in Office 365.	✓	✓	✓
Regulatory compliance audit Discover violations of most common regulations, such as PCI-DSS, GDPR, or HIPAA in all regional variations.	✓	✓	✓
Workspace security audit Audit usage of company devices, applications, networks, and print. Discover unused or misused resources to maintain workspace, ensure retention, and reduce costs.	✓	✓	✓
Content inspection classification Classify sensitive files and emails by powerful content inspection with predefined templates or custom rules and dictionaries.	✓	✓	✓
Detection of suspicious activities React fast thanks to real-time detection of suspicious activitie and			
Endpoint Data Protection	✗	✓	✓
Email and network protection Data protection for email, web upload, instant messaging, and network shares.	✗	✓	✓
Devices and print protection Manage data-flow to external devices and protect sensitive data against forbidden printing on local, network, or virtual printers.	✗	✓	✓
Remote work protection Avoid data leaks on remote endpoints or remote desktop connections. Support a wide range of remote access solutions.	✗	✓	✓
Advanced data classification Use advanced technologies to detect and mark sensitive data based on origin, workflow context, or file type. Take advantage of metadata detection to use 3rd party classifications. Allow users to classify files themselves.	✗	✓	✓
Different remediation policies React flexibly to detected incidents to empower and educate your employees. Incidents can be logged, blocked, or justified/blocked with override.			

Incident Shadow Copy Keep forensic evidence for incidents by creating shadow copies of leaking data. Shadow copies are fully encrypted and can be kept on local computers with a retention policy.	✗	✓	✓
Workspace control Define your secured workspace and reduce perimeter by application and website control. Avoid undesirable behavior in your company and reduce the cost of security management.	✗	✓	✓
Safetica Zones Easy management of safe data perimeter with unique Safetica Zones, which significantly reduce the number of data protection policies.	✗	✓	✓
BitLocker encryption management Centralized management of local drives and external devices with BitLocker encryption.	✗	✓	✓
Cloud Data Protection	✗	✓	✓
Endpoint cloud sync protection Data protection for cloud drives on endpoints, e.g. OneDrive, Google Drive, Dropbox, Box, etc.	✗	✓	✓
Endpoint Office 365 protection Data protection for Office 365 and SharePoint from endpoints. Prevent sharing or uploading data you want to keep away from the cloud.	✗	✓	✓
Azure Information Protection Detection of data classifications from Microsoft Azure Information Protection, even in encrypted form.	✗	✓	✓
Exchange Online Protection Unify email policies across endpoints and cloud email. Manage and filter outgoing data from endpoints and Exchange Online.	✗	✓	✓
Enterprise Features	✗	✗	✓
End-user rebranding End-user notification rebranding, e.g. changing the logo.	✗	✗	✓
Workflow control Application policies and expert policy settings for aligning endpoint workflow with company processes.	✗	✗	✓
Multi-domain support Multiple domain enterprise support for Active Directory.	✗	✗	✓
Security Automation	✗	✗	✓
SIEM integration Automated reporting of incidents to SIEM solutions (Splunk, QRadar, LogRhythm, ArcSight, etc.).	✗	✗	✓
FortiGate integration Automated security integration with FortiGate network appliances to create a robust endpoint-to-network security solution.	✗	✗	✓

關於

SAFETICA

Safetica is a Czech software company that provides its data loss prevention solution to companies of all shapes and sizes. Because in Safetica we believe that every company deserves to know that their data is secure.

300,000+ protected devices

1,600+ satisfied customers

120+ countries

80+ security experts

TECHNOLOGY ALLIANCES

AWARDS & ACHIEVEMENTS

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

FORRESTER

Gartner

@Safetica
Safetica
@Safetica

關於您的資料呢?

原廠授權代理商 - 墩城科技有限公司
意者請洽 卓先生 0926302233