bluechip infotech

ManageEngine Cloud Security Plus

公有雲平台
日誌管理與稽核監控工具

藍籌科技
張慶振
Kerry Chang

Helping your business grow

20
YEARS
2020

Celebrating 20 Years with Bluechip

PLATINUM SPONSORS

acer CyberPower LogMeIn SOPHOS

GOLD SPONSORS

EATON hp

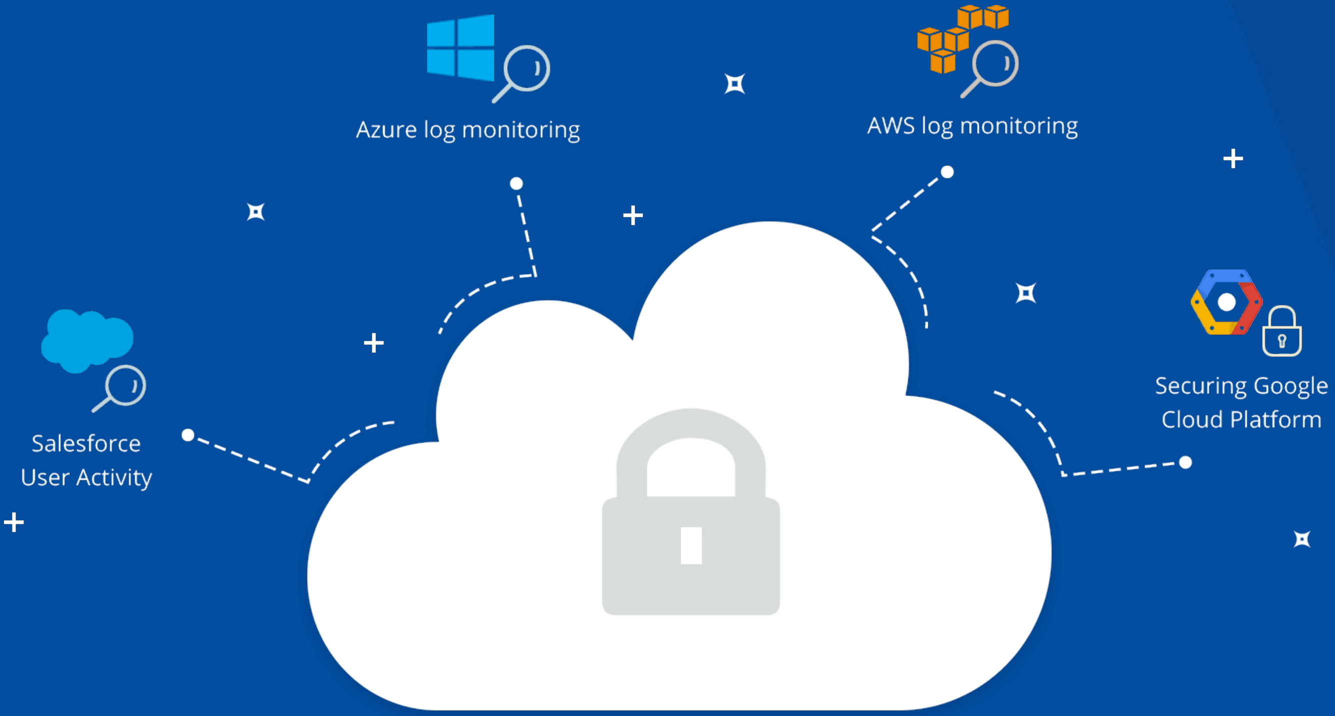
bluechip 與您的企業一起成長

- 總部位於澳洲雪梨，與其他據點
  - 墨爾本
  - 布里斯本
  - 阿得雷德
  - 伯斯
  - 台北
- 超過101名員工，提供您最佳服務
- 2020上半年營收突破14億台幣(71M AUD)

公有雲日誌管理

A comprehensive cloud log management solution

整合各大雲平台


Azure log monitoring
AWS log monitoring
Securing Google Cloud Platform
Salesforce User Activity

收集了哪裡的日誌呢?

Microsoft Azure

日誌來源	說明
Azure 活動記錄	活動記錄是 Azure 中的平臺記錄 ，可提供訂用帳戶層級事件的見解。 這包括修改資源或啟動虛擬機器時的資訊。
網路安全性群組流量記錄	流量記錄是 Azure 網路監看員的一項功能，可讓您記錄流經 NSG 之 IP 流量的相關資訊。 流量資料會傳送Cloud Security Plus。

Amazon Web Services (AWS)

日誌來源	說明
AWS CloudTrail	CloudTrail 可以記錄、持續監控和保留 AWS 基礎設施中所有與動作相關的帳戶活動。
Server access logging	當您啟用Server access logging時，Amazon S3 會為來源儲存貯體，提供存取日誌給您所選擇的目標儲存貯體。
Elastic Load Balancing Access logs	Elastic Load Balancing 提供存取日誌，可針對傳送到負載平衡器的請求，擷取其詳細資訊。

Google Cloud Platform

日誌來源	說明
Cloud Audit Logging	Cloud Audit Logs 為每個 Google Cloud 專案、資料夾和組織維護三種審核日誌：管理員活動、資料存取和系統事件。 Google Cloud 服務會將稽核資訊寫入這些日誌，以說明在您的資源中，哪些使用者在何時何處，執行了什麼操作。

收集之後呢?

Cloud Security Plus 主要功能

- 可自由調整的管理介面
- 提供AWS 詳細的報表
- 針對Azure 上活動提出見解
- 針對GCP 上的事件提供建議
- 提供簡易且全面的搜尋功能
- 定期且自動的提供報表
- 提供email告警功能

比AWS提供還詳盡的報表

- Amazon S3 log management
- Amazon S3 bucket activity
- Amazon IAM user activity
- AWS security group change auditing
- AWS auto–configuration
- AWS Elastic Load Balancing traffic analysis
- Amazon Relational Database Service (RDS) activity
- Forensic analysis of AWS CloudTrail logs

提供Azure上的各類報表

- User activity
- Changes made to permissions and network security groups
- Virtual networks
- DNS zones
- Storage accounts and databases
- Resource locks
- Network security group traffic
- Allowed and denied flows
- Virtual machines

提供GCP上的各類報表

- User activity and identity and access management
- Network security and services
- VPC activity
- Hybrid connectivity
- Cloud functions
- App Engine
- Google storage
- GCP resource management

定期且自動產出報表

- 支援格式
  - PDF, HTML, XLS, and CSV
- 可自訂報表產出時間
- 直接透過email發送

提供簡易且全面的搜尋功能

- 可在日誌中，搜尋任何關鍵字或欄位
- 甚至特殊符號、群組、布林函數等

Email告警，即時關注

- 不同緊急性，三階段告警
  - Attention
  - Trouble
  - Critical
- 自訂告警設定
- 可自訂告警門檻值

使用情境

1. AWS 運算之內部資安事件

- EC2狀態改變了!
  - 內部人員啟動或關閉instance
- Cloud Security Plus 可以提供什麼協助?
  - 透過”Recent EC2 Instance State Changes” 報表查詢哪些 instance 的狀態改變，包含Start or Stop.
  - 設定告警提醒管理員

2. Azure 網路之內部資安事件

- 網路安全群組上的規則改變了!
  - 內部人員改變網路安全群組，允許未知存取進來

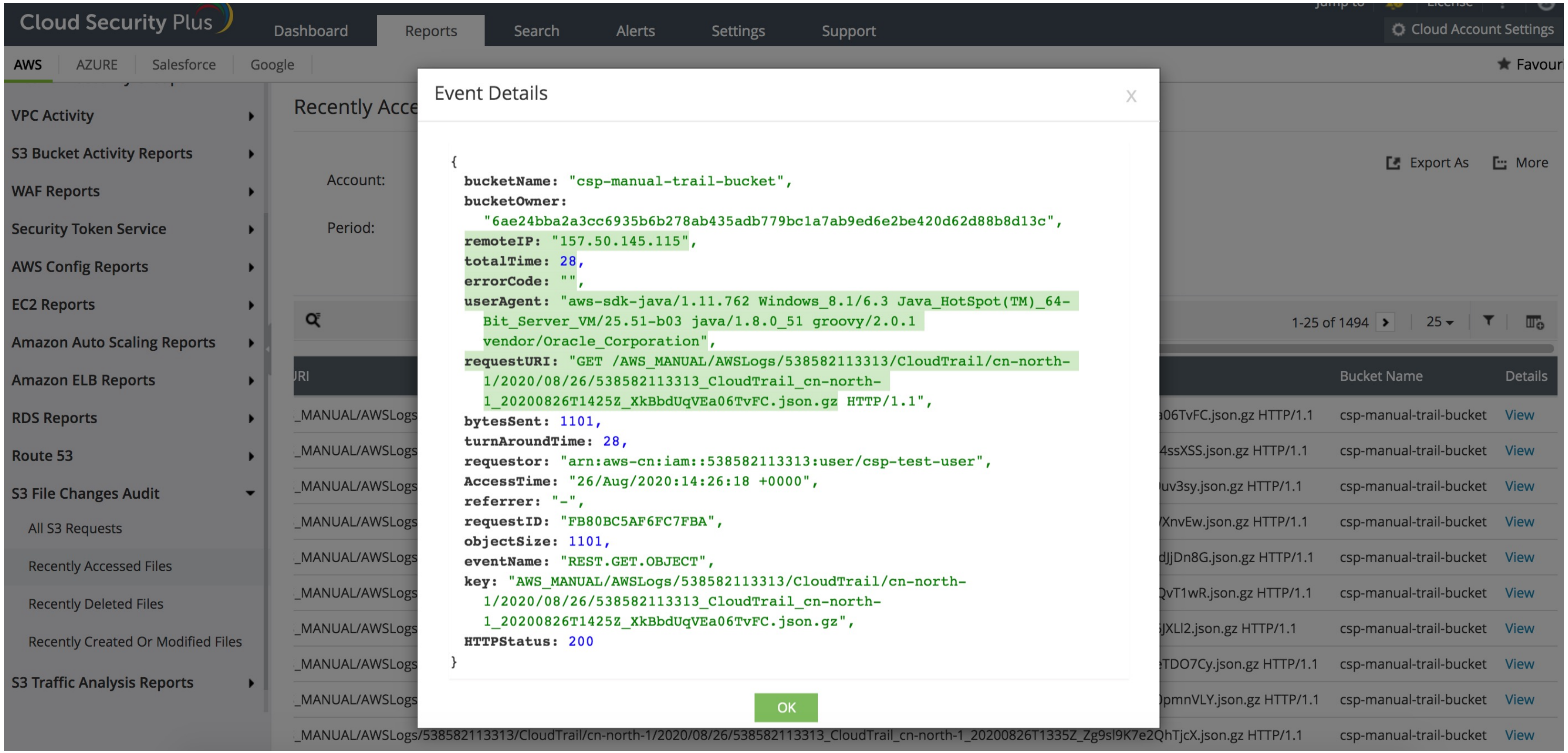
- Cloud Security Plus 可以提供什麼協助?
  - 透過報表了解，變更了哪些網路安全群組、權限變更、子網域變更等等。
  - 並設定告警提醒管理員

目前還在進化中

- 未來將開發更多功能，包括：
- 稽核更多AWS服務
  - CloudFront, VPC Flow, RDS, Lambda, Glacier, DynamoDB, Redshift, Elastic Beanstalk, Kinesis
- 稽核更多Azure服務
  - Web Apps, Content Delivery Network, Storage Analytics, Data Lake, Data Factory

管理介面

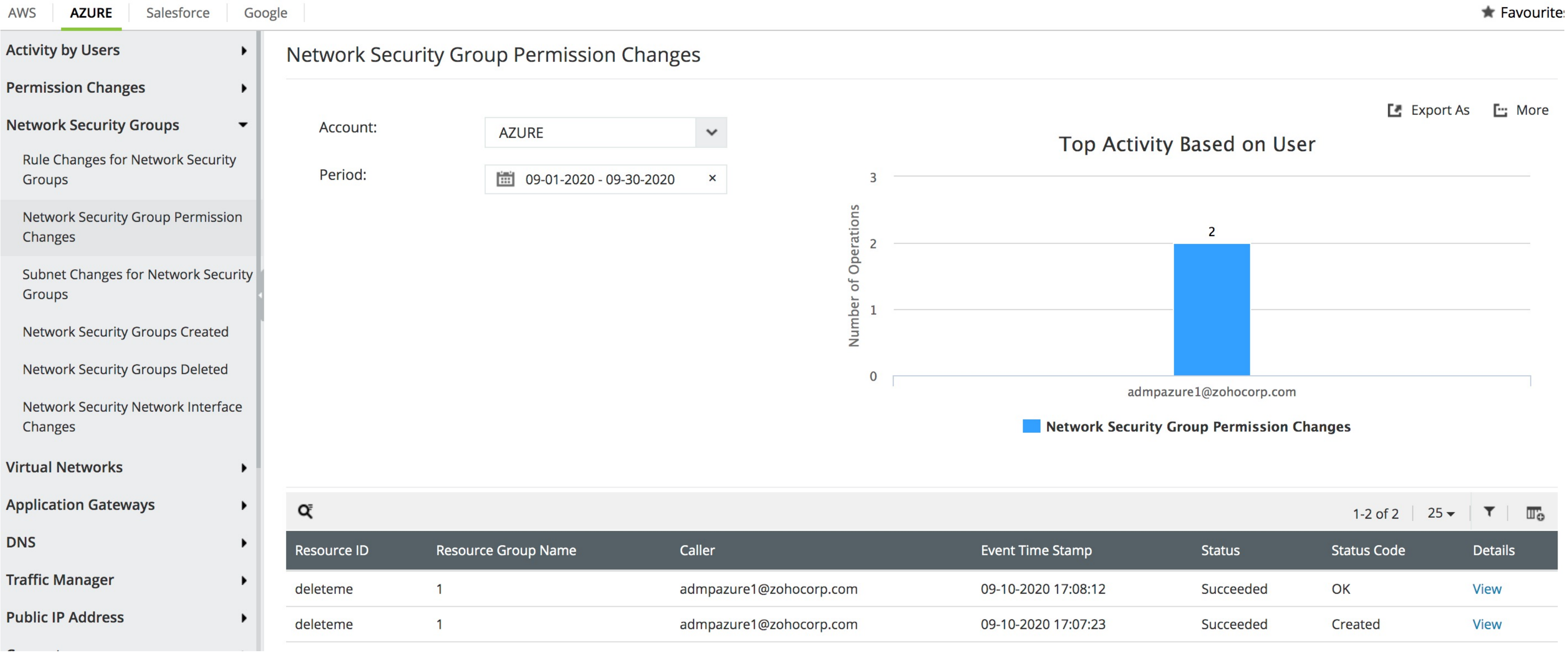
AWS S3 上，時間點/存取IP/存取路徑



```
{
  bucketName: "csp-manual-trail-bucket",
  bucketOwner:
    "6ae24bba2a3cc6935b6b278ab435adb779bc1a7ab9ed6e2be420d62d88b8d13c",
  remoteIP: "157.50.145.115",
  totalTime: 28,
  errorCode: "",
  userAgent: "aws-sdk-java/1.11.762 Windows_8.1/6.3 Java_HotSpot(TM)_64-
    Bit_Server_VM/25.51-b03 java/1.8.0_51 groovy/2.0.1
    vendor/Oracle_Corporation",
  requestURI: "GET /AWS_MANUAL/AWSLogs/538582113313/CloudTrail/cn-north-
    1/2020/08/26/538582113313_CloudTrail_cn-north-
    1_20200826T1425Z_XkBbdUqVEa06TvFC.json.gz HTTP/1.1",
  bytesSent: 1101,
  turnAroundTime: 28,
  requestor: "arn:aws-cn:iam::538582113313:user/csp-test-user",
  AccessTime: "26/Aug/2020:14:26:18 +0000",
  referrer: "-",
  requestID: "FB80BC5AF6FC7FBA",
  objectSize: 1101,
  eventName: "REST.GET.OBJECT",
  key: "AWS_MANUAL/AWSLogs/538582113313/CloudTrail/cn-north-
    1/2020/08/26/538582113313_CloudTrail_cn-north-
    1_20200826T1425Z_XkBbdUqVEa06TvFC.json.gz",
  HTTPStatus: 200
}
```

JRI		Bucket Name	Details
_MANUAL/AWSLogs	a06TvFC.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs	4ssXSS.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs	uv3sy.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs	XnvEw.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs	dJjDn8G.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs	QvT1wR.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs	JXLl2.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs	TDO7Cy.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs	pmnVLY.json.gz HTTP/1.1	csp-manual-trail-bucket	View
_MANUAL/AWSLogs/538582113313/CloudTrail/cn-north-1/2020/08/26/538582113313_CloudTrail_cn-north-1_20200826T1335Z_Zg9sl9K7e2QhTjcX.json.gz HTTP/1.1		csp-manual-trail-bucket	View

Azure 上，時間點/帳號/網路安全群組權限變更


AWS
AZURE
Salesforce
Google
Favourite
Activity by Users
Permission Changes
Network Security Groups
Rule Changes for Network Security Groups
Network Security Group Permission Changes
Subnet Changes for Network Security Groups
Network Security Groups Created
Network Security Groups Deleted
Network Security Network Interface Changes
Virtual Networks
Application Gateways
DNS
Traffic Manager
Public IP Address
Export As
More
Top Activity Based on User
Number of Operations
3
2
1
0
2
admpazure1@zohocorp.com
Network Security Group Permission Changes
1-2 of 2
25

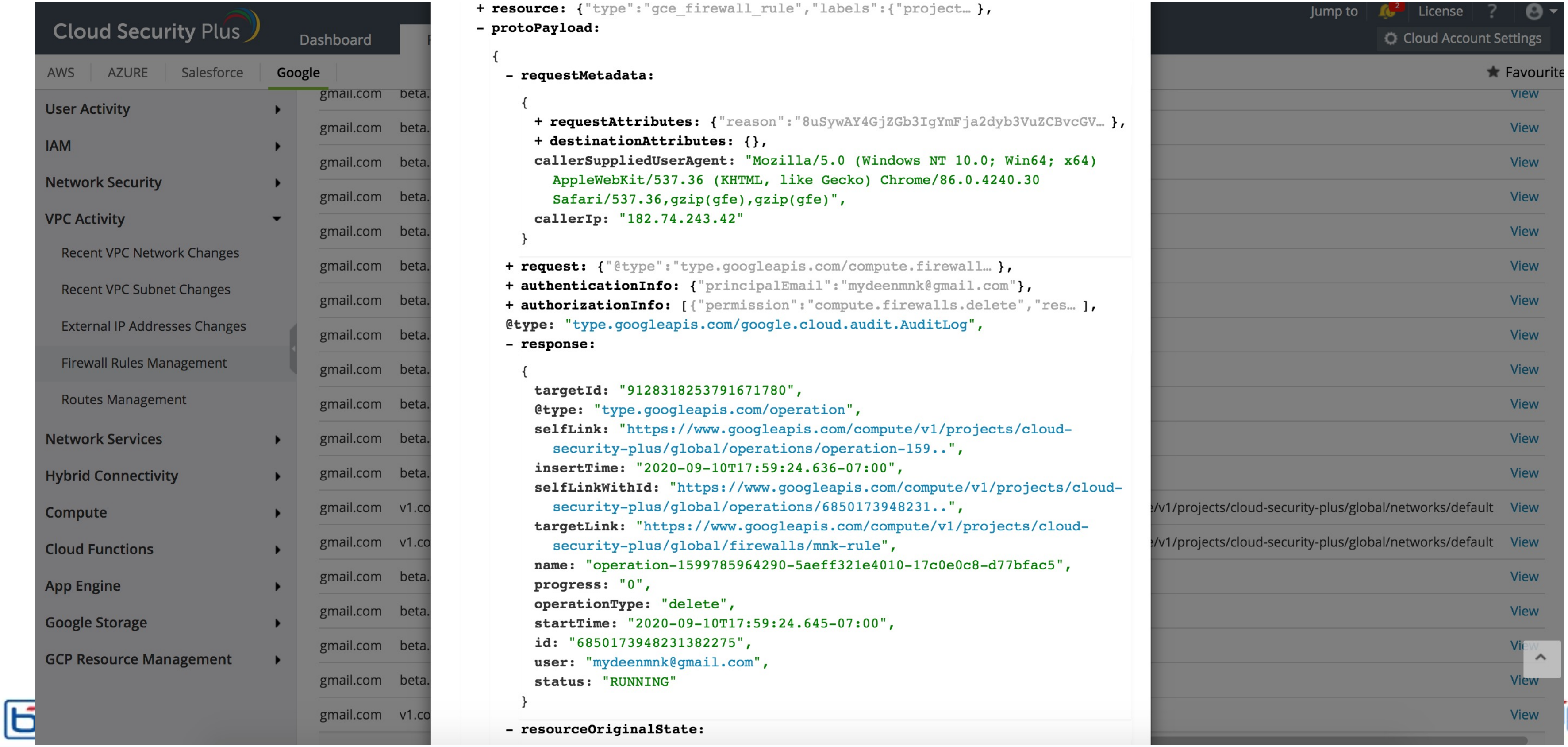
Network Security Group Permission Changes

Account: AZURE

Period: 09-01-2020 - 09-30-2020

Resource ID	Resource Group Name	Caller	Event Time Stamp	Status	Status Code	Details
deleteme	1	admpazure1@zohocorp.com	09-10-2020 17:08:12	Succeeded	OK	View
deleteme	1	admpazure1@zohocorp.com	09-10-2020 17:07:23	Succeeded	Created	View

GCP 上，時間點/帳號/IP/刪除防火牆設定



```
+ resource: {"type":"gce_firewall_rule","labels":{"project… },
- protoPayload:
  {
  - requestMetadata:
    {
     + requestAttributes: {"reason":"8uSywAY4GjZGb3IgYmFja2dyb3VuZCBvcGV… },
     + destinationAttributes: {},
     callerSuppliedUserAgent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
       AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.30
       Safari/537.36,gzip(gfe),gzip(gfe)",
     callerIp: "182.74.243.42"
    }
  + request: {"@type":"type.googleapis.com/compute.firewall… },
  + authenticationInfo: {"principalEmail":"mydeenmnk@gmail.com"},
  + authorizationInfo: [{"permission":"compute.firewalls.delete","res… ],
  @type: "type.googleapis.com/google.cloud.audit.AuditLog",
  - response:
    {
     targetId: "9128318253791671780",
     @type: "type.googleapis.com/operation",
     selfLink: "https://www.googleapis.com/compute/v1/projects/cloud-
       security-plus/global/operations/operation-159..",
     insertTime: "2020-09-10T17:59:24.636-07:00",
     selfLinkWithId: "https://www.googleapis.com/compute/v1/projects/cloud-
       security-plus/global/operations/6850173948231..",
     targetLink: "https://www.googleapis.com/compute/v1/projects/cloud-
       security-plus/global/firewalls/mnk-rule",
     name: "operation-1599785964290-5aeff321e4010-17c0e0c8-d77bfac5",
     progress: "0",
     operationType: "delete",
     startTime: "2020-09-10T17:59:24.645-07:00",
     id: "6850173948231382275",
     user: "mydeenmnk@gmail.com",
     status: "RUNNING"
    }
  - resourceOriginalState:
```

建議系統安裝環境

- 雙核CPU / 2G RAM
- 50GB 硬碟空間
- Windows 10 / Server 2012

- 可參考線上DEMO
  - https://demo.cloudsecurityplus.com/index.html#

為何選用Cloud Security Plus?

- 簡單部署
- 多雲集中介面
- 多平台日誌分析與管理
- 稽核使用者行為，保障雲端安全
- 即時資安告警
- 提供大量資安相關報表

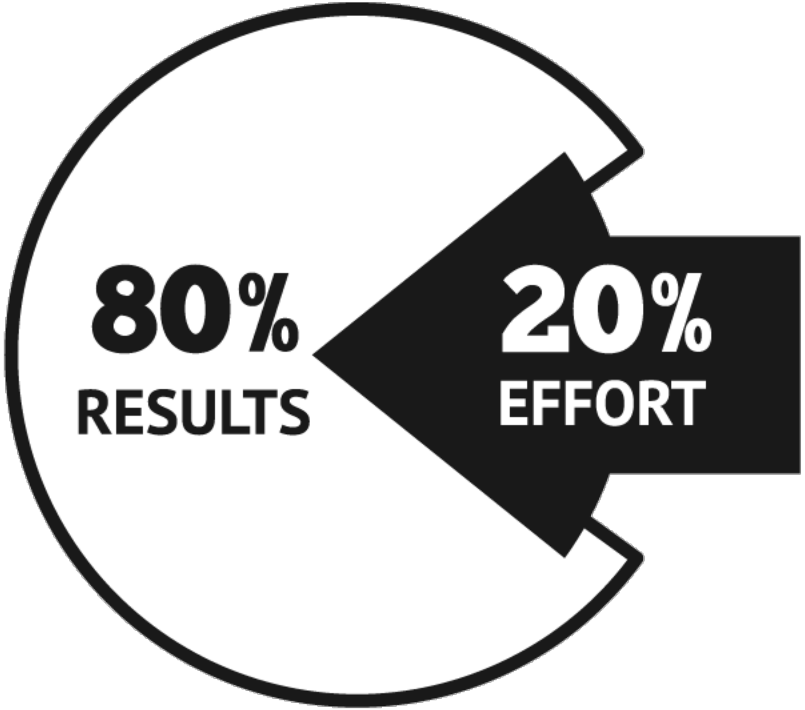
為你呈現

ManageEngine

Introduing ManageEngine

ManageEngine的概念就是

- 花更少的預算
- 得到相同的功能
- 甚至更多!



全方位IT管理解決方案

- IT整合管理
  - 提供 90 多種，價格合理，滿足您的所有 IT 管理需求之產品。
- IT簡化管理
  - 易於下載、安裝、設定和部署，無需第三方支援服務或幫助。
- IT實惠管理
  - 更高的價格並不始終意味著更好的產品

180,000+
家全球企業

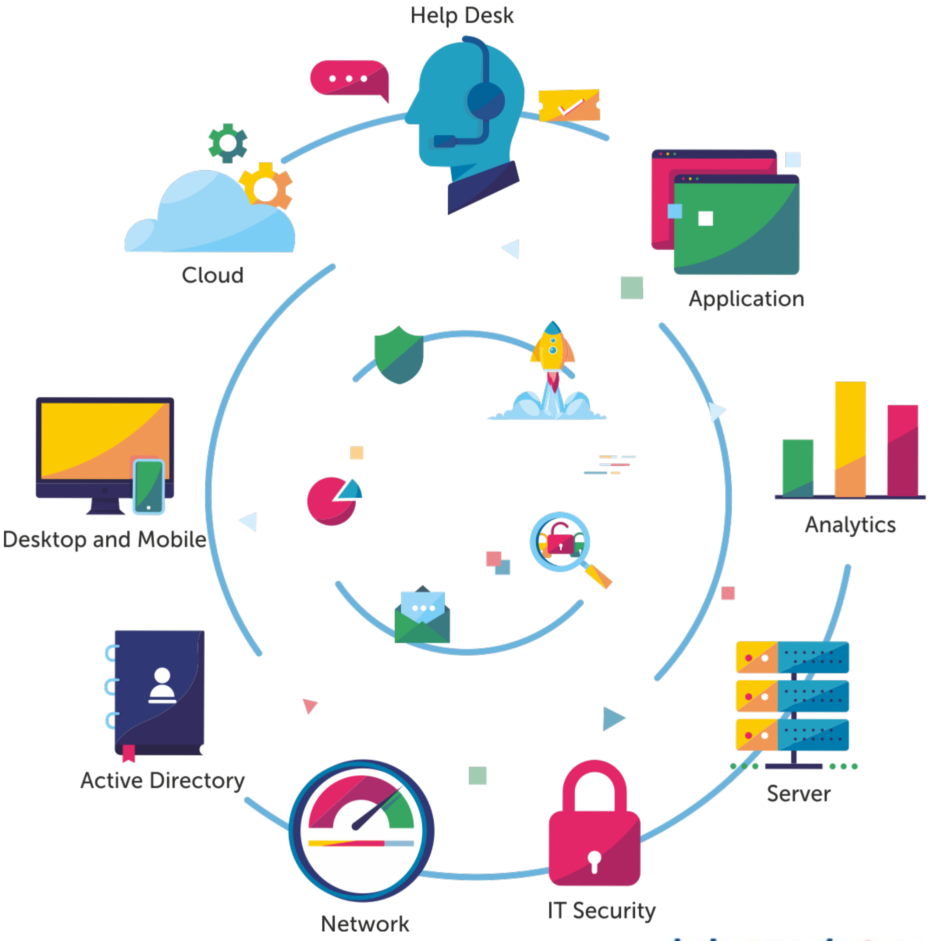
9/10
財富 100 強公司

3,000,000+
管理者

..信任 ManageEngine 來管理其 IT。

ManageEngine 協助您

- ITIL整合式資產和服務管理
- 更有效的管理雲平台
- 比讓微軟更實用的AD管理
- 大量端末設備
- 複雜的基礎設施
- 符合資安需求的稽核
- 可滿足所有IT管理需求



用更實惠的價格，滿足相同的需求

MICRO FOCUS

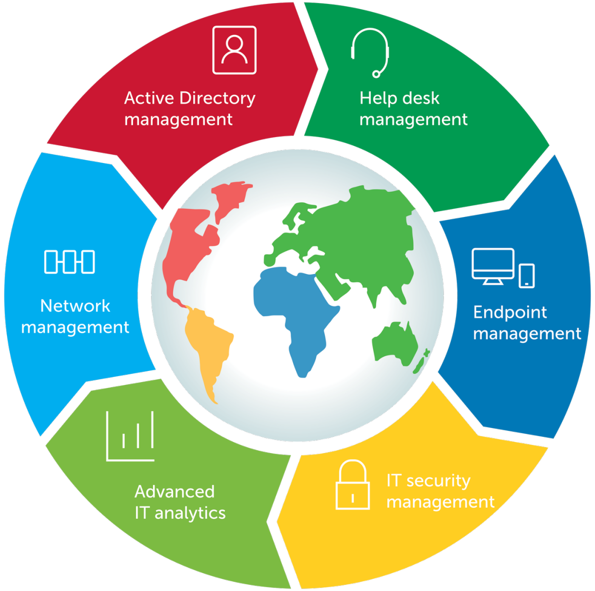
splunk>

netwrix

Quest

NETSCOUT

dynatrace

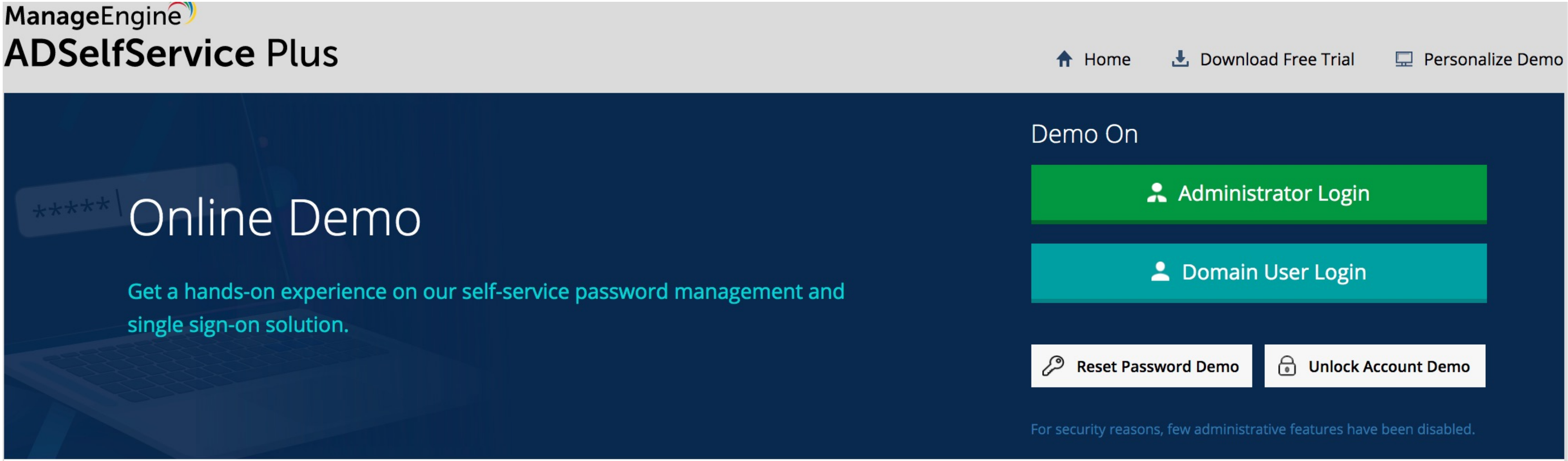


您也可以選用

ManageEngine

每一項產品皆有線上DEMO

- 也可以申請30天 Trial License



Online Demo

Get a hands-on experience on our self-service password management and single sign-on solution.

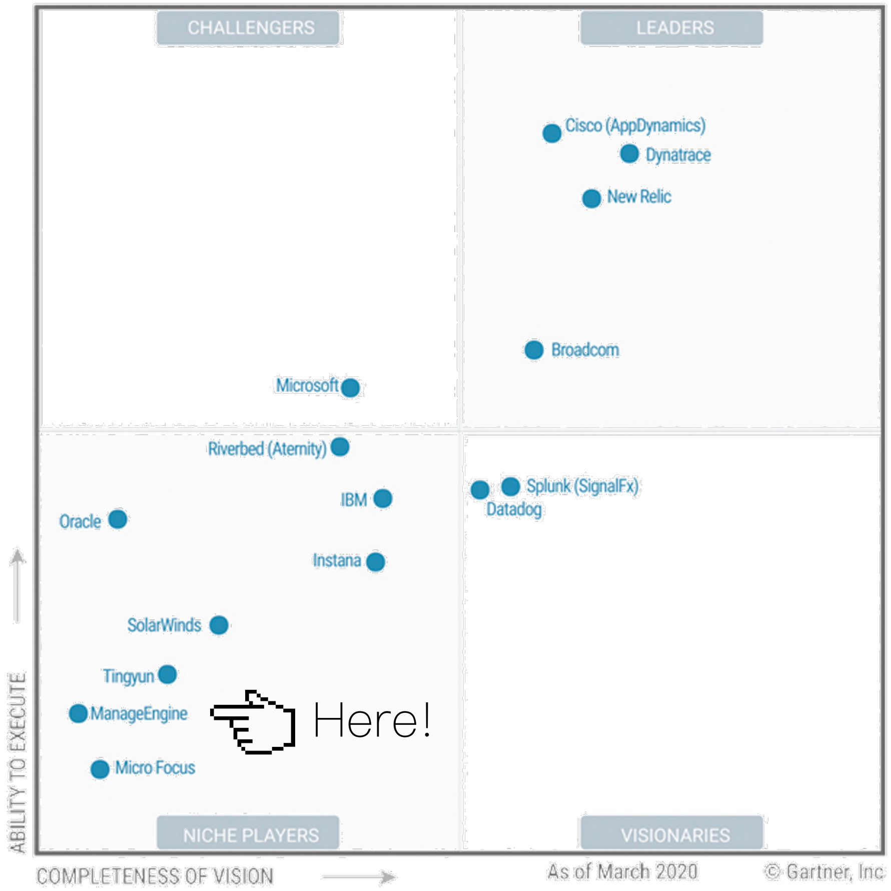
Demo On

For security reasons, few administrative features have been disabled.

入選各項Gartner魔術象限

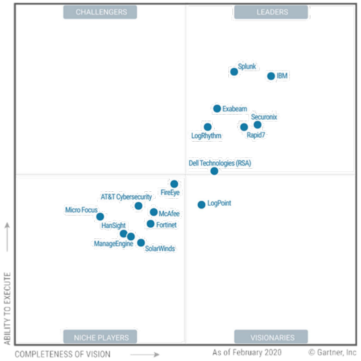
- 應用效能監控解決方案
- 連續八年

Figure 1. Magic Quadrant for Application Performance Monitoring



Source: Gartner (April 2020)

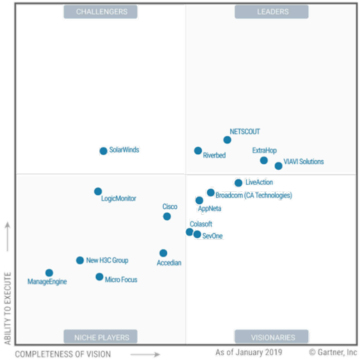
Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (February 2020)

Security Information
and
Event Management
(SIEM)
連續四年

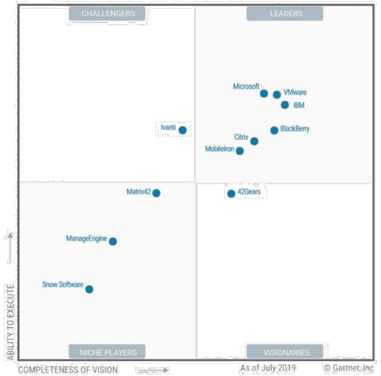
Figure 1. Magic Quadrant for Network Performance Monitoring and Diagnostics



Source: Gartner (February 2019)

Network Performance
Monitoring and Diagnostics
(NPMD)
連續兩年

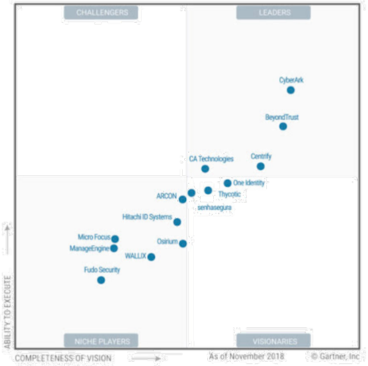
Figure 1. Magic Quadrant for Unified Endpoint Management



Source: Gartner (August 2019)

Unified Endpoint
Management Tools.
(UEM)
連續兩年

Figure 1. Magic Quadrant for Privileged Access Management



Source: Gartner (December 2018)

Privileged
Access
Management
(PAM)

獲獎無數的整合解決方案

PINK

Gartner®

STRONG VALUE
Zoho/ManageEngine
EMA Radar™ for
Mobile Device Management 2016

FORRESTER®

SC MAGAZINE ★★★★★

IDC
Analyze the Future

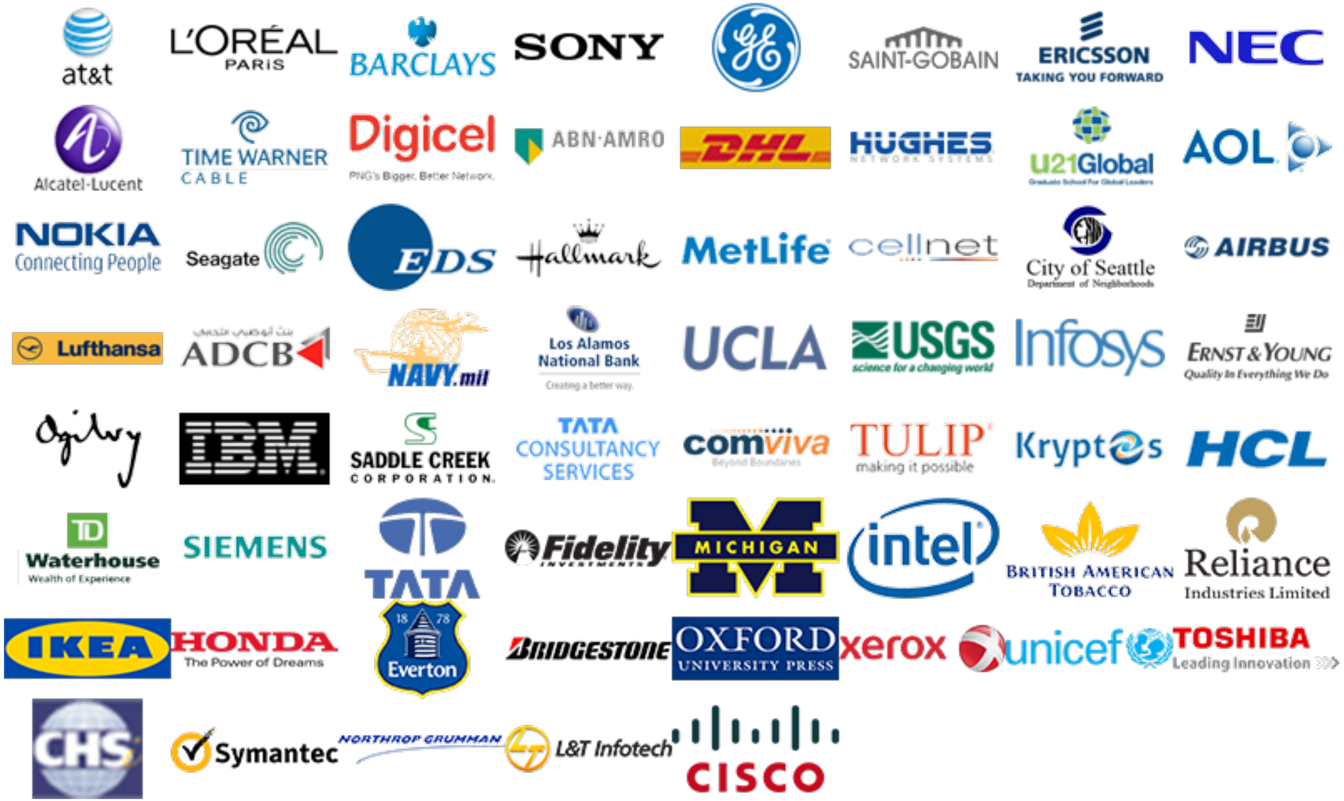
THE INTEGRATOR
ict
CHAMPION AWARDS

VENDOR LANDSCAPE AWARD
BEST OVERALL VALUE
INFO~TECH
research group

EMA™

Redmond
READER'S CHOICE AWARDS
2015

全球各大企業指定使用


at&t
L'ORÉAL PARIS
BARCLAYS
SONY
SAINT-GOBAIN
ERICSSON TAKING YOU FORWARD
NEC
Alcatel-Lucent
TIME WARNER CABLE
Digicel PNG's Bigger, Better Network.
ABN·AMRO
DHL
HUGHES NETWORK SYSTEMS
U21Global
AOL
NOKIA Connecting People
Seagate
EDS
Hallmark
MetLife
cellnet
City of Seattle Department of Neighborhoods
AIRBUS
Lufthansa
ADCB
NAVY.mil
Los Alamos National Bank Creating a better way.
UCLA
USGS science for a changing world
Infosys
ERNST & YOUNG Quality In Everything We Do
Ogilvy
IBM
SADDLE CREEK CORPORATION
TATA CONSULTANCY SERVICES
comviva Beyond Boundaries
TULIP making it possible
Kryptos
HCL
TD Waterhouse Wealth of Experience
SIEMENS
TATA
Fidelity INVESTMENTS
MICHIGAN
intel
BRITISH AMERICAN TOBACCO
Reliance Industries Limited
IKEA
HONDA The Power of Dreams
18 78 Everton
BRIDGESTONE
OXFORD UNIVERSITY PRESS
xerox
unicef
TOSHIBA Leading Innovation
CHS
Symantec
NORTHROP GRUMMAN
L&T Infotech
CISCO

選擇ManageEngine

- 易於安裝、易於操作、易於管理
- 採訂閱制，與企業一同成長，彈性增長規格
- 極具競爭力的價格

WHO can help?

IT’s ManageEngine

找Kerry吧

Email:kerryc@bcit.com.tw

THANK YOU

Any Questions?
Or
Contact Kerry