



主動式防禦對付 勒贖程式和進階持續性攻擊

Attivo Networks

AGENDA

01 為什麼需要主動式防禦

02 Attivo Networks

03 總結

04 Q&A

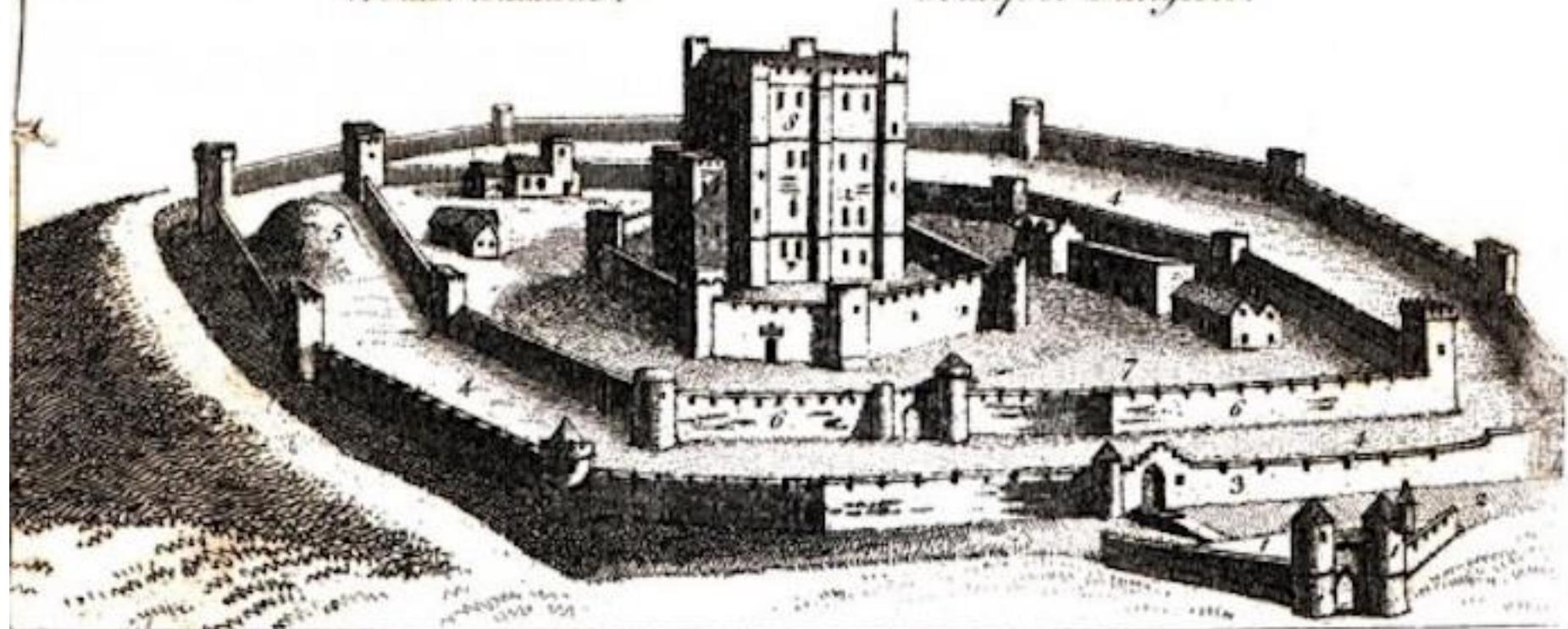
為什麼需要主動式防禦

傳統資安防護：被動式抵禦攻擊

禦敵於邊界之外，只能預防可被辨識的攻擊與惡意入侵

References.

- 1. The Barbican.
- 2. The Ditch or Moat.
- 3. Wall of the outer Battlement.
- 4. Outer Battlement.
- 5. Artificial Mount.
- 6. Wall of the Inner Battlement.
- 7. Inner Battlement.
- 8. Keep or Dungeon.



軍事上的主動式防禦

“對於一個我方防守的區域，或者是敵我雙方爭奪的區域，以有限度的攻擊行動或是反擊，把敵人拒絕阻止於這區域之外”

—美國國防部

MITRE Shield : 主動式防禦

不分企業規模大小



- 反制目前的攻擊
- 更深入了解敵人
- 為未來的新攻擊做更好的準備



Foundational Defensive
Techniques For All
Defensive Plans

Shield 矩陣

8 tactics, each employs part of
36 techniques to form a Matrix

MITRE Shield 矩陣 – Attivo 覆蓋

引導 (18/18)	收集 (16/19)	限制 (9/11)	偵測 (17/20)	破壞 (11/16)	促成 (16/16)	仿真 (12/12)	測試 (18/19)
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Admin Access
API Monitoring	Application Diversity	Baseline	Application Diversity	Application Diversity	Application Diversity	Burn-In	API Monitoring
Application Diversity	Backup and Recovery	Decoy Account	Behavioral Analytics	Backup and Recovery	Behavioral Analytics	Decoy Account	Application Diversity
Decoy Account	Decoy Account	Decoy Network	Decoy Account	Baseline	Burn-In	Decoy Content	Backup and Recovery
Decoy Content	Decoy Content	Detonate Malware	Decoy Content	Behavioral Analytics	Decoy Account	Decoy Credentials	Decoy Account
Decoy Credentials	Decoy Credentials	Hardware Manipulation	Decoy Credentials	Decoy Content	Decoy Content	Decoy Diversity	Decoy Content
Decoy Diversity	Decoy Network	Isolation	Decoy Network	Decoy Credentials	Decoy Credentials	Decoy Network	Decoy Credentials
Decoy Network	Decoy System	Migrate Attack Vector	Decoy System	Decoy Network	Decoy Diversity	Decoy Persona	Decoy Diversity
Decoy Persona	Detonate Malware	Network Manipulation	Email Manipulation	Email Manipulation	Decoy Persona	Decoy Process	Decoy Network
Decoy Process	Email Manipulation	Security Controls	Hunting	Hardware Manipulation	Decoy System	Decoy System	Decoy Persona
Decoy System	Hunting	Software Manipulation	Isolation	Isolation	Network Diversity	Network Diversity	Decoy System
Detonate Malware	Network Diversity		Network Manipulation	Network Manipulation	Network Manipulation	Pocket Litter	Detonate Malware
Migrate Attack Vector	Network Monitoring		Network Monitoring	Security Controls	Peripheral Management		Migrate Attack Vector
Network Diversity	PCAP Collection		PCAP Collection	Standard Operating Procedure	Pocket Litter		Network Diversity
Network Manipulation	Peripheral Management		Pocket Litter	User Training	Security Controls		Network Manipulation
Peripheral Management	Protocol Decoder		Protocol Decoder	Software Manipulation	Software Manipulation		Peripheral Management
Pocket Litter	Security Controls		Standard Operating Procedure				Pocket Litter
Security Controls	System Activity Monitoring		System Activity Monitoring				Security Controls
Software Manipulation	Software Manipulation		User Training				Software Manipulation
			Software Manipulation				

網路欺敵把內網變成一個大陷阱

迷惑、誤導攻擊者，觀察並互動以確認其意圖，早期啟動自動化事件回應

未加 Deception 之前



企業設備

實施 Deception



企業設備



擬真誘餌

實施 Deception 後攻擊者所見

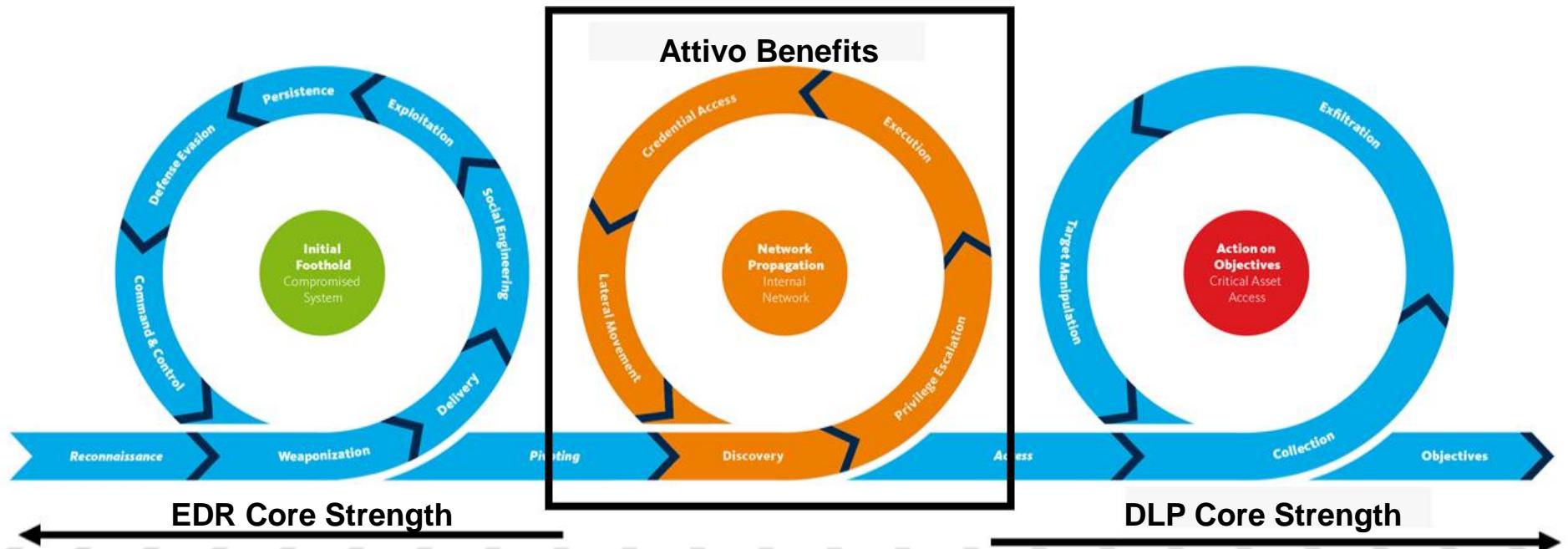


可偵測到的企業設備



Attivo EDN 提升APT29 測試結果

Vendor	Weighted			Flat		
	Solo	w Attivo	Improvement	Solo	w Attivo	Improvement
A	280	442	58%	151	191	26%
B	214	413	93%	91	176	93%
C	637	743	17%	288	298	3%
D	407	526	29%	192	225	17%
Average			49%			35%



企業如何扭轉資安防護被動局勢...



過去...

我們的防衛必須100%完美，每一次都成功才行，而駭客只需要幸運一次即可成功入侵。



現在...

主動式防禦，改變資安遊戲規則- **反守為攻**
駭客也必須100%完美，不能犯一丁點錯誤。

ATTIVO NETWORKS

Attivo對主動式防禦的詮釋：提供完整的憑證和身分保護

端點，Active Directory，和雲端

能見度



- Lateral Movement Paths (LMP) on endpoints
- AD Misconfigurations and Realtime Threat Detection
- Cloud Identities and Entitlement (CIEM)

ThreatPath, ADAssessor,
IDEntitleX

縮小攻擊面



- Remediate LMP from Endpoint to Cloud
- Recommendation engine to reduce AD attack surface
- Identity Least Privileges

ThreatPath, ADAssessor,
IDEntitleX

防止攻擊



- AD Attack Prevention
- Data Cloaking and Ransomware Protection
- Credential Theft Prevention
- East-West Lateral Movement Prevention

ADSecure, EDN, BOTsink

ThreatDefend架構

彈性、可橫向擴充的部署

1 從端點設備設置誘餌

- 偵測憑證盜取 (credential based) 之攻擊
- 引誘攻擊者以取得完整TTPs及犯罪證據

2 部署伺服器高仿真誘餌

- 勘察威脅攻擊
- 資料中心中間人攻擊 (Man-in-the-Middle attack) 偵測
- 提高伺服器網路可視性

3 本地網路部署

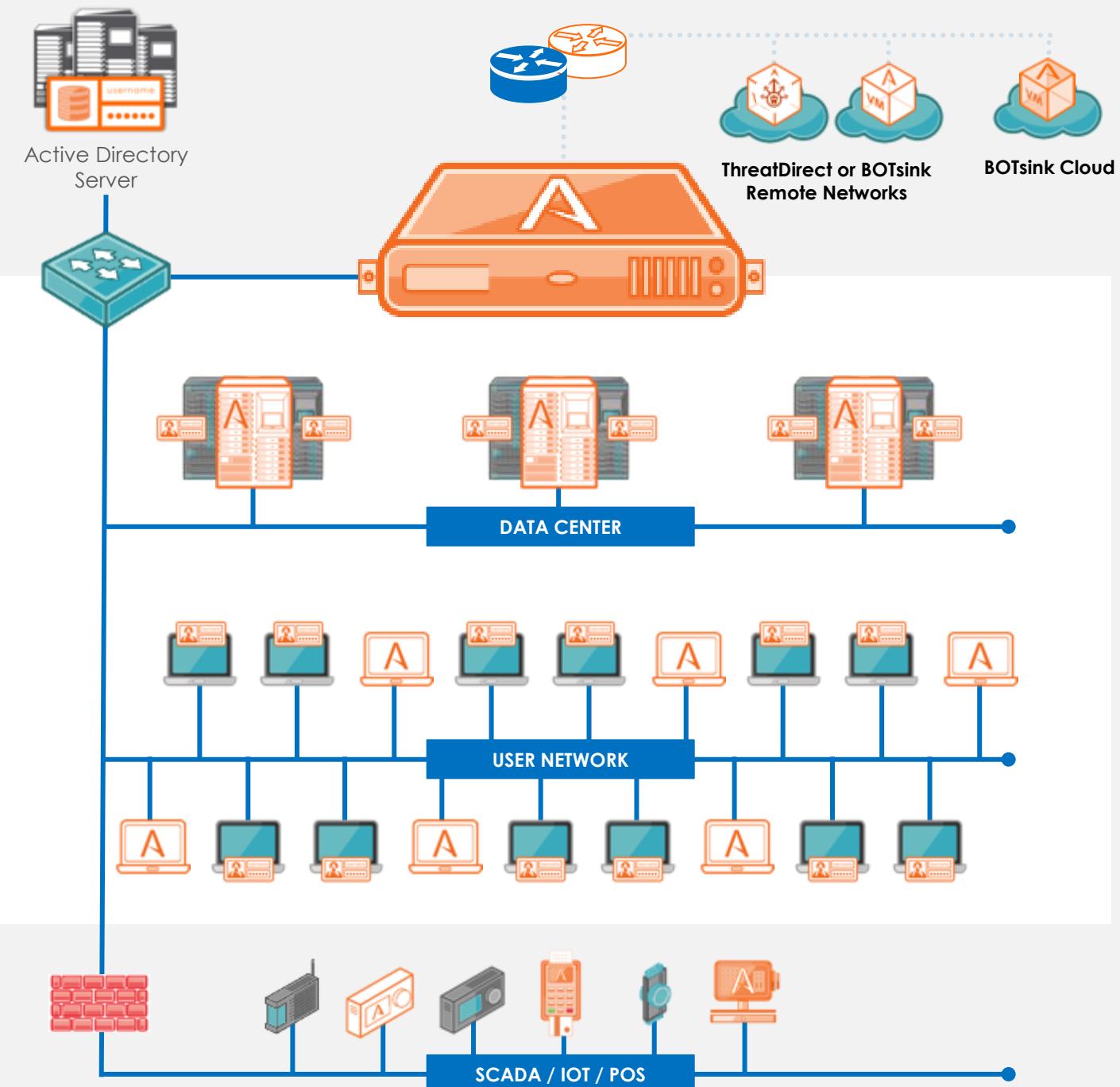
- 內部網路中間人攻擊偵測
- 提高使用者網路可視性

4 彈性擴充部署

- 支援雲端部署
- 遠端辦公/分公司/三層式架構
- 基礎架構及AD防禦
- SCADA / IOT / POS

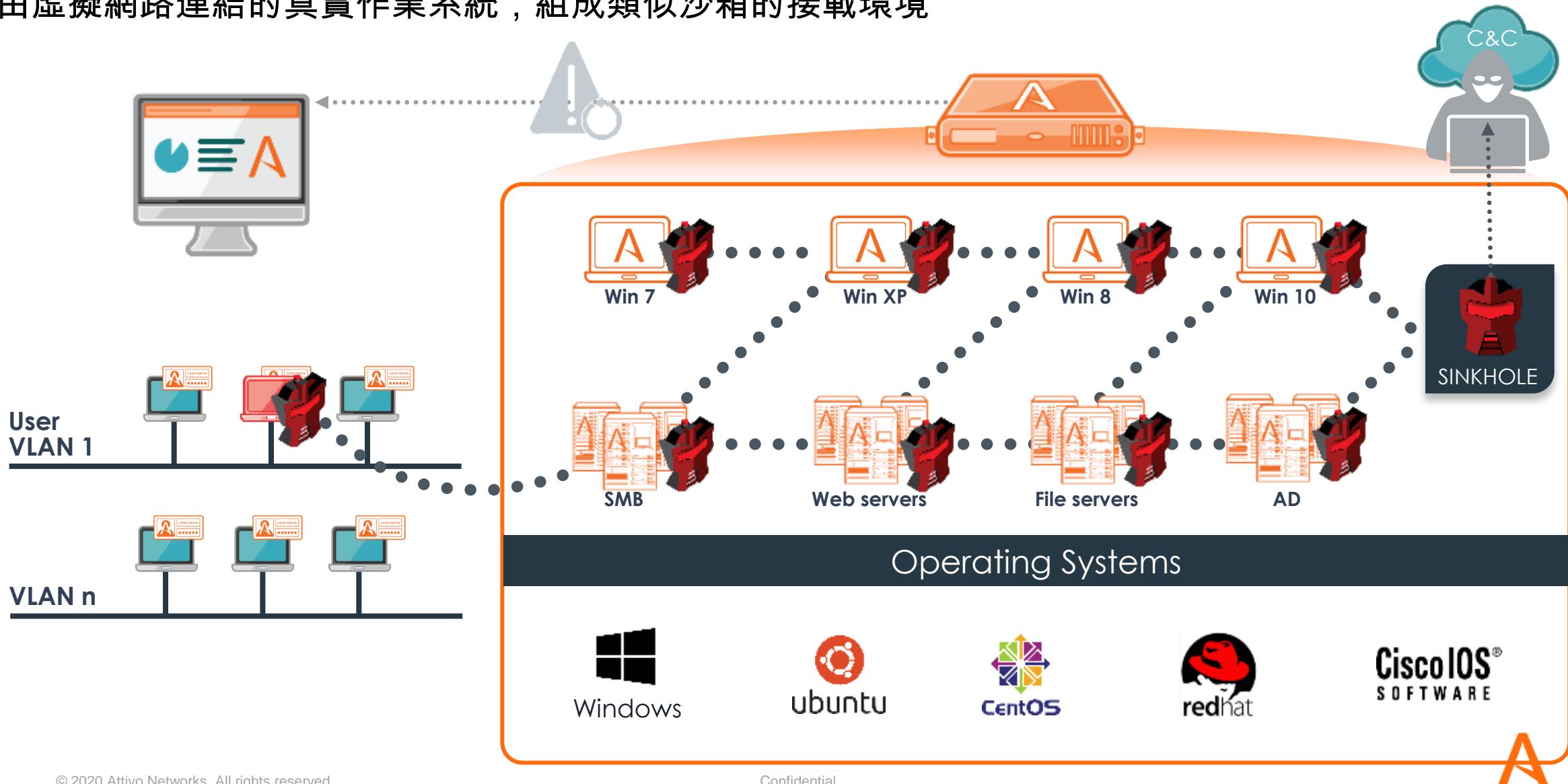
效益

- 多重欺敵防護 (Comprehensive deception)
- 可客製化防禦需求 (Scales with customer needs)
- 中央系統嚴密控管 (Central management)



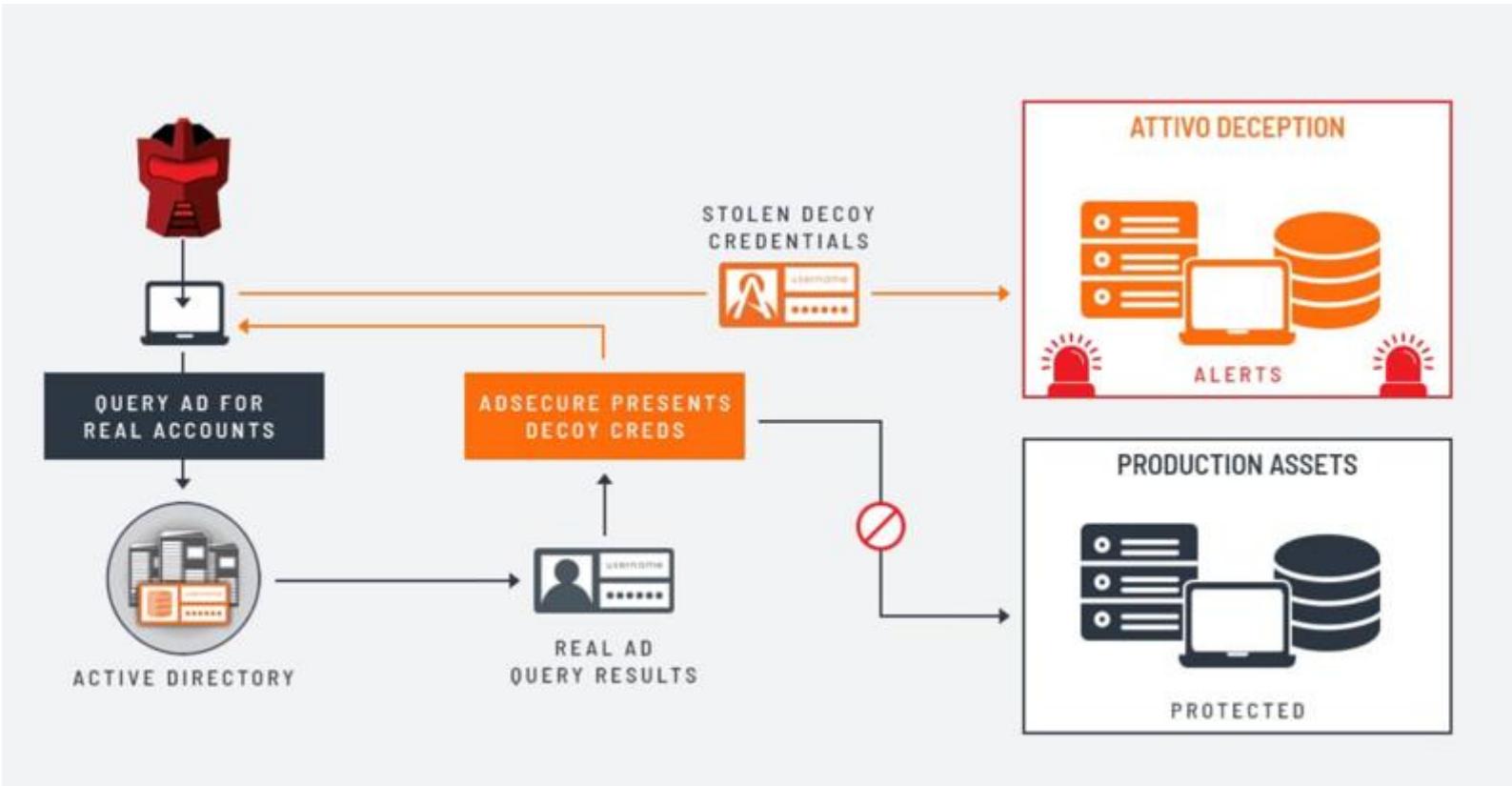
主動式防禦：與敵人交戰

由虛擬網路連結的真實作業系統，組成類似沙箱的接戰環境



ADSecure

破壞攻擊者的節奏，讓攻擊者懷疑它的工具



* Supports popular AD objects (admin, service, critical computers, net sessions)

What Attivo Does

- Hides info, protect critical objects
- Returns deceptive objects
- Fake data steers attackers to decoys
- Telemetry for visibility & hunting

Benefits

- Prevents attackers from exploiting Active Directory
- Stops privilege escalation
- Alerts on early attack activity
- Fake data steers attack to decoys
- No changes to production AD

大幅減低AD曝露的風險

One Attivo Customer (5,000 employees & 7,000 devices) Reduced AD Attack Surface by over 90%

AD Access Type	Quantity	% of population	Quantity	% of population	Risk Reduction
			After ADSecure Deployed		
Users Who can read data from AD	5,000	100%	50	1%	99%
Systems authorized for High Risk AD Queries	7,000	100%	35	.5 of 1%	99.5%
Applications authorized to query AD	100	100%	15	15%	85%
Users Authorized for High-Risk AD Queries*	5,000	100%	10	.2 of 1%	99.8%
Remote Workers can query AD via VPN	3200	100%	50	1.5%	98.5%
Interns and Contractors can query AD	ALL	100%	none	0	100%

*Mapping AD Servers, Profiling Admins and other privileged users, profiling key applications and data stores, searches for regular users with admin status, profiling service accounts, etc.

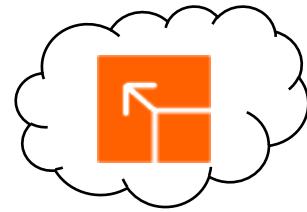
總結

Attivo Networks的優勢

主動防禦，欺敵戰術



主動且有效
防禦潛在的
內網威脅
勒贍程式
AD攻擊



流暢佈署
彈性拓展
不影響既有環
境



全面覆蓋
網路, 端點, 雲端,
SCADA,IOT



簡易操作
補強原有資安
工具防護



依據情報採取反制



可呈堂的鑑證與自動化回應

Questions?

