XCITIUM
Power of Zero

先發制人的遏制技術與
主動端點偵測與回應（EDR）

全球資安新挑戰

未知攻擊和勒索軟體是複雜的新興產業

NEW MALWARE
450,000
RELEASED DAILY

EDR ALONE = BREACHES
99% DETECTION
目前的安全解決方案採用檢測作為保護的主要方法。 這是也意味著，駭客不端研發全新且從未被發現的攻擊手法，將持續造成損害和破壞力。

NEW RANSOMS
11SECS
ENACTED DAILY

REPUTATION SERVICES
UNPREDICTABLE
第三方資安情報服務推動了檢測領域的發展，但分析速度緩慢且效率低下的情況，是無法提供全面保護。.

VICTIMS DAMAGED
$350M
IN RANSOMS PAID

INSUFFICIENT EXPERTISE
HIGH COST SKILLS
為解決風險，不斷投入的資安培訓、較高的學習曲線以及有限的資安人力，再加上告警疲勞所衍生的高昂資安成本。

THE XCITIUM SOLUTION

主動端點偵測與回應（EDR)

毫無疑問，EDR 是現今市場的主流。 然而，使用檢測模型的 EDR 工具所提供的安全性不足，無法檢測到未知。攻擊者很聰明，他們了解「檢測模型」解決方案的工作原理，並不斷研究開發新技術，以逃避每個檢測的雷達檢測，以「未知」的方式進行攻擊，可輕易成功跳脫被檢測到可能性。

好消息的是，XCITIUM 獨家使用即時 ZeroDwell 遏制技術與 EDR 完全整合的資安管理解決方案，讓您具備優先保護的能力，透過XCITIUM 安全管理機制，您可以輕鬆看到資安違規、勒索攻擊與資安事件直線下降的趨勢。

XCITIUM 在使用 ZeroDwell Containment 進行保護之後，EDR 的價值就變得顯而易見。 當駭客發動全新攻擊時，便會被 Xcitium 先發制人地遏制，管理者不會再出現警報疲勞，因為先期遏制攻擊讓威脅不再發生。 在遏制威脅的情況下，即時、持續的端點可見性和可操作的警報管理是 XCITIUM 的功能亮點。 現在，您可以強化您的環境，抵禦零時差攻擊和無檔案攻擊，搭配 EDR 可以讓您全方位可視化實現即時、準確的分析根本原因，從而實施有效的修補和修復。 在這個新的安全管理環境中，XCITIUM 協助您在精確掌握組織內的基本事件級別分析整個組織中發生的情況，以便您獲得詳細的文件和設備軌跡資訊，揭示可能使您的端點容易受到攻擊的潛在更大問題。 ZeroDwell Containment 讓主動資安管理 與 EDR 相輔相成。

THE XCITIUM DIFFERENCE

只有 Xcitium 專利的零時差遏制技術才能防止漏洞、勒索軟體和零時差漏洞造成傷害！
Only Xcitium's patented Zero Dwell Containment prevents breaches, ransomware, and zero-day 's from causing harm!

ZERO TRUST | ZERO BREACH | ZERO DAMAGE | ZERO DOWNTIME

XCITIUM

Xcitium 產品的優勢與高階端點安全防毒 (AV)、Viruscope (NGAV)、端點偵測與回應 (EDR)、主機入侵防禦系統 (HIPS)、防火牆 (FW) 和端點管理結合(EM) 功能，透過集中式SaaS 平台提供漏洞利用預防、全面的視覺化管理、報告的多樣性、威脅搜尋和端點管理。

KEY CAPABILITIES

MITRE 攻擊鏈映射與視覺化

在儀表板上顯示攻擊軌跡。 當與文件軌跡和流程層次結構視覺化相結合時，這可以加速調查。 基於流程的事件以樹狀視圖結構方式顯示，以幫助分析人員更了解流程行為。

持續監控與專家推薦的安全策略

每個 EDR 授權都附帶一個預設端點安全管理策略，該策略可自訂以滿足個人需求。 我們的銷售技術服務團隊可以與您合作，根據您的要求客製化安全管理策略，特別是特定於端點或特定封閉環境的管理策略。

可疑活動偵測和警報

自動獵捕有關無檔案攻擊、進階持續性威脅 (APT) 和權限升級嘗試等事件的通知。 資安分析師可以在採取應對措施時更改警報狀態，從而顯著簡化後續工作。 由於運行時採用ZeroDwell Containment，警報疲勞已成為過去，您可以專注於重要的警報。

事件調查

事件搜尋畫面允許資安分析師執行查詢以傳回基本事件等級的任何詳細資訊。 視覺化的關聯表，使調查人員可以輕鬆深入了解特定事件或裝置。

SaaS雲端管理架構

Xcitium 在端點上使用輕量級代理來監視、處理、網路、下載、上傳、存取檔案系統和周邊設備以及記錄瀏覽器事件，它使您能夠以基本事件層級的粒度深入了解事件。

VERDICT 雲端決策引擎

在虛擬化遏制中執行時，未知檔案會上傳到 Xcitium 全球威脅雲，以進行即時分析並判定是良性還是惡意。 良性實體只需從收容中釋放即可。

無檔案惡意軟體偵測

並非所有惡意軟體都是可被發現的。 當某些惡意軟體內建於端點基於記憶體的架構（例如 RAM）中時，不需要您執行檔案。 Xcitium EDR 可以在這種威脅出現之前對其進行偵測。

主動ZERODWELL遏制技術

請求運行時權限的未知可執行檔和其他文件會自動在 Xcitium 專利的 ZeroDwell 容器中運行，該容器無法存取主機系統的資源或使用者資料。 ZeroDwell Containment 意味著惡意軟體無法在您的網路或組織中橫向移動。

企業級和 MSP 就緒

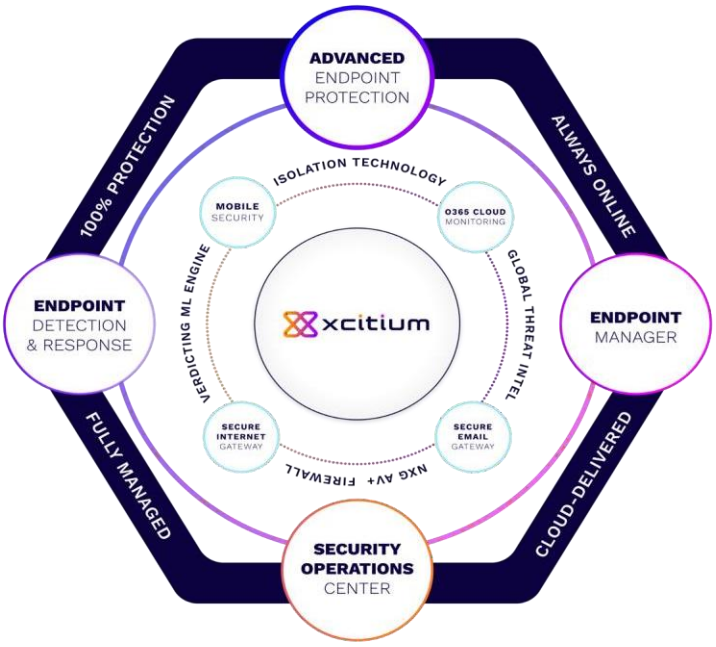
無論您是擁有數千個端點的企業還是為數百個客戶提供服務的 MSP，EDR 代理程式都可以透過群組原則物件或 Xcitium ITSM 立即部署，並在每個版本中自動更新。

主動式EDR

即時遏制威脅，獲得深入可視性，並加強抵禦未來的攻擊

Xcitium 提供連續監測。 積極從您的端點收集攻擊和異常事件，並將其集中 在 Xcitium 威脅雲管理平台中，利用 Xcitium 資安威脅實驗室情報以及建議 的安全策略。然後，我們的自動進行AI雲分析結果並識別在端點上安全虛擬化的所包含的未知文件活動，並快速取得 AI 雲分析所判定的惡意/安全結果，而 EDR 工作則專注於真正的警報，而不是警報疲勞轟炸。

使用 Xcitium 進行端點系統安全管理，您可以獲得基於可自訂安全策略的可操作警報，通知您包含的活動的操作，這些活動可能代表勒索軟體、記憶體漏洞、PowerShell 濫用、列舉 — 包含的威脅以及許多其他 IoC 進行的特定攻擊嘗試。 當違反 Xcitium 的安全性建議策略時，也會觸發警報。 實際在端點上的停留時間上為零，所以並不可能造成任何損壞，而您的 EDR 技術現在可以專注於修復和解決已發現的漏洞。 例如，偽裝成通常由 PowerShell 和 Regedit 等簽署且受信任的應用程式執行的操作的惡意行為不會被其他 EDR 工具類似地標記 — 這正是攻擊者使用可信任應用程式的原因。 但 Xcitium 可以在讓管理者清楚地看到這種行為。 如果沒有我們的 EDR，所包含的威脅通常會被忽視，導致攻擊者竊取或勒索您公司的機密資料。



IMMEDIATE TIME-TO-VALUE

ZERODWELL CONTAINMENT

統一端點解決方案提供執行時間攻擊遏制、威脅偵測和回應生命週期最佳化、漏洞利用預防、無與倫比的可見性、進階威脅搜尋和端點管理，以阻止勒索軟體、避免違規並維持您的業務。 **ZeroDwell Containment 也您與現有資安防禦容。**

Xcitium 成為 EDR 安全基礎設施的第一道防線。

透過 ZeroDwell Containment 從偵測轉向預防，隔離勒索軟體和未知攻擊等攻擊，而不會中斷您的端點或業務營運。

友善的視覺化安全管理

取得攻擊的完整背景，將駭客如何嘗試破壞您的網路的各個點連結起來。

大量減少EDR的告警疲勞

獲得攻擊的完整背景，將駭客如何試圖破壞您的網路的點聯繫起來，而不會出現大量警報給您的安全團隊帶來負擔（遏制的攻擊不再是威脅）。

SaaS端點安全管理中心

透過識別應用程式、了解漏洞所在以及使用修補程式進行修復來實踐網路衛生，以減少攻擊面。

可擴展為託管EDR 服務(MDR)

許多漏洞是由於缺乏資源和維護流程造成的，也可能是由於缺乏整合和協調安全技術所需的技術造成的，但這些問題中的每一個問題都可擴展由 Xcitium MDR完全涵蓋和管理 Xcitium 與 EDR 的 24•7•365 SOC 調查和修復服務。

零信任、 零違規

零停留、 零損壞

端點安全零信任的實踐家

THE POWER OF ZERO UNLEASHED

	Xcitium Essentials	Xcitium Advanced (EDR)	Xcitium Managed (MDR)	Xcitium Complete (XDR)
Cloud-Native SaaS Platform	V	V	V	V
安全防護				
Auto Containment Technology	V	V	V	V
Verdict Cloud File Determination Service	V	V	V	V
(XTRL) Xcitium Threat Research Labs Service Delivery	V	V	V	V
主動威脅管理				
Endpoint Detection and Response	V	V	V	V
NGAV Static	-	V	V	V
Behavioral AI Threat Prevention	-	V	V	V
Data Loss Prevention	-	V	V	V
Firewall Control		V	V	V
Host Intrusion Prevention System	-	V	V	V
AI/ML Threat Intel & Indicators	-	V	V	V
Mobile Device Security	-	V	V	V
Patch Management	-	V	V	V
Vulnerability Scanning	-	V	V	V
5x9 Customer Support	V	V	V	V
SOC 服務				
24/7/365 SOC Services			V	V
Incident Response & Forensics			V	V
X/MDR Network and Cloud				V

ABOUT US

Xcitium 以前稱為 Comodo Security Solutions，全球有 3,000 多家組織客戶和合作夥伴使用。 它的成立只有一個簡單的目標——杜絕網路漏洞。 Xcitium 的 ZeroDwell Containment 專利技術使用核心級 API 虛擬化來隔離和消除零時差惡意軟體和勒索軟體等威脅，以免造成任何損害。 ZeroDwell Containment 是 Xcitium端點套件的基石，其中包括高階端點保護、端點偵測和回應 (EDR) 以及託管偵測和回應 (MDR)。 自成立以來，Xcitium 在完全配置後就擁有零違規、零勒索記錄。