

# 集成式資安架構 綜合安全

網絡威脅繼續擴散，組織用來保護自己的工具庫也不斷增加。與其添加更多工具，不如通過集成SIEM，業務流程和語境威脅情報集中資安操作。

## 當今的資安監控：工具太多，語境太少

當出現新的威脅時，許多組織會購買更多的專用工具。

結果是工具太多了.....



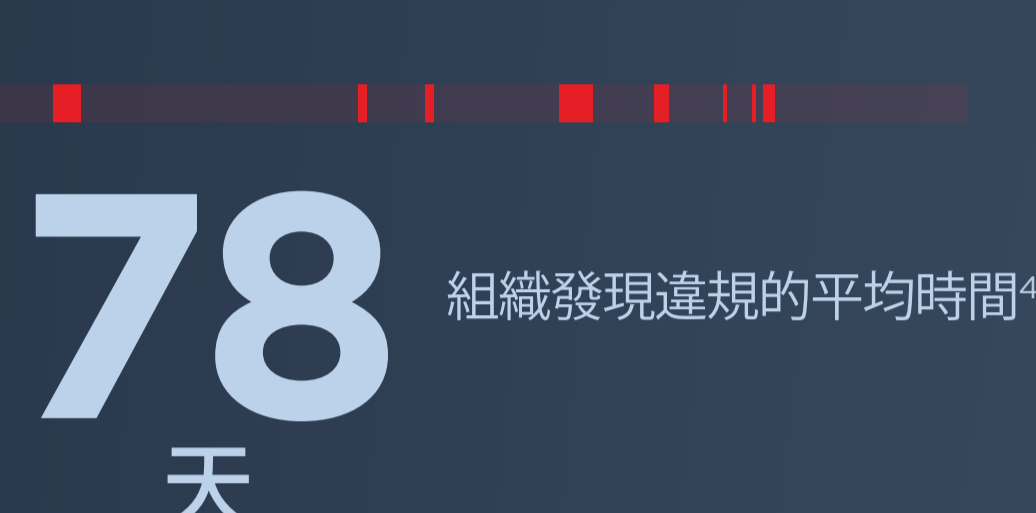
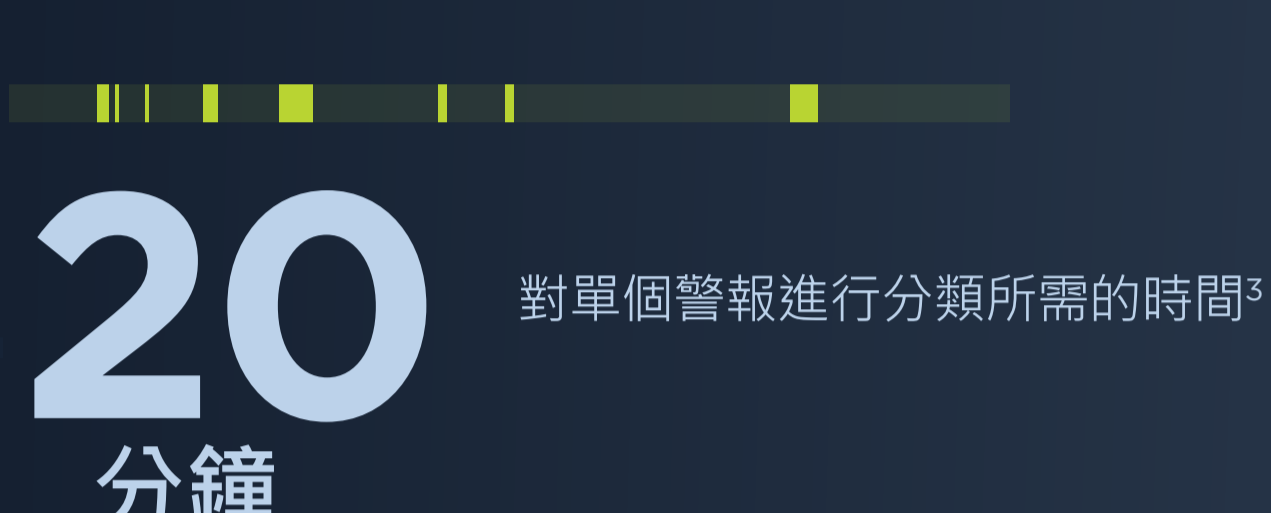
這些工具會產生太多警報...



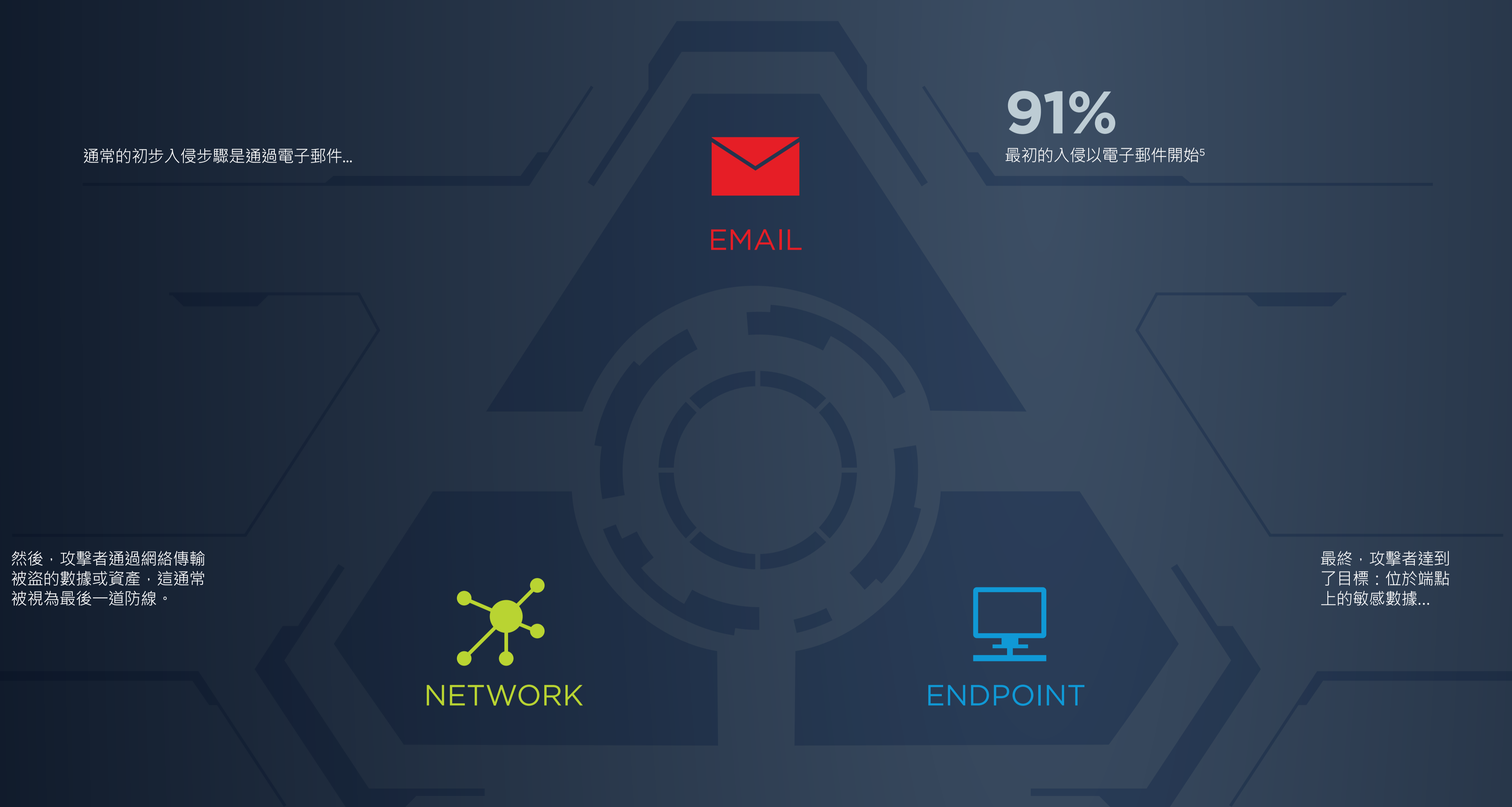
而且安全團隊沒有足夠的時間來確定哪些警報很重要...

結果，不良分子可以訪問網絡並將其隱藏幾個月。

當團隊分心更長的時間時...



## 攻擊者針對三個主要媒介



您需要將工具和數據集中化與對電子郵件，端點和網絡的可見性結合起來，以清楚地了解攻擊者的目標和應對方式。

## 借助集成式資安架構，您可以獲得<sup>6</sup>



## 當投資回報率不僅僅是資產負債表上的時候<sup>6</sup>

	BEFORE	AFTER		BEFORE	AFTER
在日間的，容易出錯的過程上花費更少的時間 在集成安全平台之前/之後花費在核心SOC活動上的平均時間			花更多時間在關鍵威脅識別和響應活動上		
充實和驗證	39%	5%	響應	10%	44%
票務和報告	35%	10%	狩獵	4%	34%
通知和升級	7%	5%			

要了解有關 FireEye Helix 的更多信息，請訪問：[www.FireEye.com/solutions/helix\\_tw.html](http://www.FireEye.com/solutions/helix_tw.html)

1 Security Intelligence (January 28, 2019). Break Through Cybersecurity Complexity With New Rules, Not More Tools.  
 2 CSO (May 3, 2017). False positives still cause threat alert fatigue.  
 3 FireEye (March 2018). M-Trends 2018.  
 4 FireEye (March 2019). M-Trends 2019.  
 5 PhishMe (2016). Enterprise Phishing Susceptibility and Resiliency Report.  
 6 Internal FireEye performance measurement results.