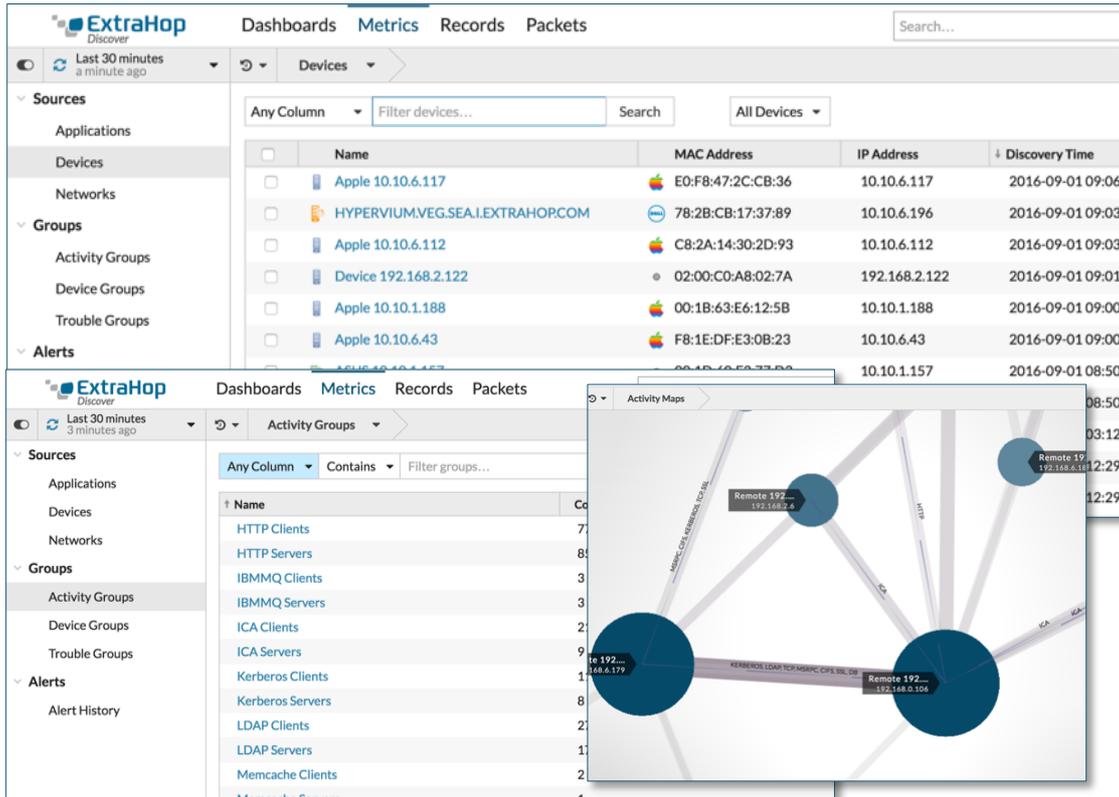




企業的網路流量分析產品，提供企業安全及網路團隊檢測和分析現行網路的各種不同的網路流量，並發現潛在的威脅，並提供高速的資料呈現和可見性，透過簡易及鉅細彌遺的網路流量資料，讓您掌握所有的網路流量，進而快速反應並作出決策。



透過網路流量分析技術，讓你快速掌握內部的威脅，潛在網路可能的勒索軟體活動痕跡及各種端點所在運行的網路流量。

The image shows a grid of six panels illustrating security capabilities:

- Breach Detection & Response:** Detect all stages of the attack lifecycle and expedite forensics. Includes a bar chart showing detection stages: Command & Control, Reconnaissance, and Lateral Movement.
- Insider Threat Detection:** Detect, contain, and document misbehavior and malice. Includes a table of network events with columns for Time, Record Type, Client, and Client IP/Port.
- Ransomware Defense:** Contain and minimize active attacks, recover data. Includes a line graph showing responses and errors, with a specific alert for 'CIFS Server Privileged Pipe Access Denied'.
- SOC Productivity:** Prioritized detection, reduced false positives. Includes a dashboard showing 85 Assets with Detections and 43 Security Detections.
- Red Team/Audit Findings:** Find or validate concerns and vulnerabilities. Includes a network graph with nodes and edges.
- Reduce Attack Surface:** Improve hygiene and decommission assets and services. Includes a bar chart showing 'Sessions with Weak Ciphers by Server' over time.