

THE BUSINESS

One of the leading private equity firms in the US with locations across North America, Europe, and Asia. The company invests on behalf of many of the world's most respected investors, including government and private sector pension and retirement funds, charitable foundations and university endowments, insurance companies, family offices, sovereign wealth funds, and high net worth individuals.

Industry

Private Equity

Location

New York, USA

“LightCyber was the only solution they could find that would allow them to identify actionable anomalies on their internal network without requiring a massive amount of IT resources and storage space.”

Stephen Harrison, Director of Sales,
EverSec Group, Inc.

THE NEED

The company has a strong investment in Perimeter defenses, including the market leading firewall provider, as well as a vendor to oversee their Constant Monitoring as a Service (CMaaS) for vulnerability assessment. After high profile breaches across the retail and financial services sector, this business realized that it needed to augment its existing network security solutions with a reliable, effective, easy-to-deploy solution that could identify and neutralize active attackers inside the company's network.

WHY LIGHTCYBER MAGNA?

- **Magna** monitors all internal network traffic, profiles normal behavior of all users and endpoints, and detects deviations that could represent malicious activity
- **Magna** significantly tightens network security, discovering previously-undetected threats, notably zero-days and other APTs, as well as more common malware that has evaded existing protections
- **Magna** offers simple deployment and rapid roll out enterprise-wide

THE RESULTS

- The first real glimpse of the potentially malicious activity within the network, **Magna** immediately identified active malware
- In addition, **Magna** highlighted previously unknown behaviors of privileged users that exposed the organization to risk
- Deployed in 2 hours, **Magna** began delivering actionable results in less than a week

WHAT THEY'RE SAYING

"LightCyber was deployed as a proactive measure to identify potential attacks across our network," said the director of network security at a large NYC-based private equity firm. "It is successfully helping identify and mitigate potential attacks that otherwise, may have been difficult to trace."

Stephen Harrison, director of sales with EverSec Group, Inc., the reseller for the NYC-based private equity firm, said this: *"LightCyber was the only solution they could find that would allow them to identify actionable anomalies on their internal network without requiring a massive amount of IT resources and storage space. When they recognized that much larger financial services firms with dramatically bigger cyber defense budgets were getting breached they realized that they need this solution now, before it was too late."*

THE STORY: THE CHALLENGE

A leading private equity firm with a significant investment portfolio and top-tier investors was looking to augment perimeter security with active breach detection. Specifically, the company was seeking an easy-to-deploy, enterprise-wide solution that would help it deal with any malware or attackers that evaded the perimeter.

THE STORY: THE SOLUTION

The company chose LightCyber **Magna** to identify and neutralize active attackers inside the corporate network.

The **Magna** appliance was installed and operating within an afternoon, from the central datacenter to provide the best visibility to both internal and outbound network traffic. **Magna** monitors the internal applications access, profiling the normal behavior of users and devices and detecting subtle behavior deviations that could represent malicious activity.

Immediately following deployment, within less than a week of profiling, **Magna** started to show alerts for active malware. The company has also used LightCyber **Pathfinder** as an agentless endpoint tool to augment detection from LightCyber **Magna**, as well as to provide additional forensic and investigative information from suspicious endpoints.

Products Deployed

1 D-300 Detector in the main datacenter, with integrated Master PFC-1000 Magna Pathfinder & Magna Cloud license.

