

SOCURA

Case study ■ Harneys

Faster, hands-on threat response for a global offshore law firm

Harneys is an international offshore law firm with 12 offices worldwide, advising multinational corporations, financial institutions, investment funds and private clients. Keeping their highly sensitive information safe - around the clock and across every time zone - is central to how the firm operates.

When its previous security operations provider couldn't keep pace, Harneys moved to Socura for Managed Detection and Response (MDR). Faster triage and hands-on response mean threats are now dealt with quickly, without landing back on the firm's own team.

HARNEYS

The security challenge

Harneys already outsourced its security monitoring to a security operations centre (SOC), but the service wasn't keeping up. Triage was slow - so slow that the firm's own security team was often spotting, reviewing and resolving incidents before the provider had even escalated them.

When alerts did come through, too many were simply handed back for Harneys to deal with. Rather than taking work off the internal team, the service was quietly adding to it.

At the same time, Harneys was moving a large part of the business from SentinelOne to Microsoft Defender for Endpoint (MDE), while the rest stayed on SentinelOne. It needed a partner that could support the move and cover both platforms.

Put simply, Harneys wanted a SOC that would get to threats first - and deal with them, rather than passing them back.

Main security concerns

- **Protecting confidential client data across 12 international offices**
- **Speeding up the triage of alerts and incidents**
- **Reducing the number of incidents handed back to the internal team**
- **Moving to Microsoft Defender for Endpoint while keeping SentinelOne covered**

The solution

Harneys appointed Socura as its MDR partner. Socura's UK-based Security Operations Centre now monitors the firm's environment 24/7, triaging, investigating and responding to alerts as they come in.

Triage is much quicker than it was with the previous provider, and Socura's analysts take response actions on Harneys' behalf - such as isolating endpoints and resetting compromised accounts - so far fewer incidents need to go back to the internal team.

Socura also supported Harneys through its move to Microsoft Defender for Endpoint, and continues to monitor SentinelOne across the rest of the business - one consistent service across both platforms.

Why Socura MDR

A genuinely managed service

Socura's analysts act on threats rather than passing them on.

Microsoft and SentinelOne expertise

Able to guide the move to MDE while keeping the rest of the estate covered.

UK-based, CREST-accredited SOC

Confidence in the quality and consistency of the service.

What changed for Harneys

	BEFORE	WITH SOCURA
Triage	Slow - Harneys' own team often resolved incidents before the SOC escalated them	**Much quicker, so genuine threats are picked up and acted on early**
Response	A high volume of incidents passed back for Harneys to handle	**Socura takes response actions on Harneys' behalf**
Internal team	Picking up work the SOC should have been doing	**Free to focus on supporting the business**
Endpoint coverage	Part of the business moving from SentinelOne to MDE	**Supported through the move, with MDE and SentinelOne both monitored**

> Socura brings enterprise level security expertise without losing the personal touch. They are big enough to handle complex threats, yet small enough to know our team by name and always be there when we call.

Mike Duff
Chief Security Officer, Harneys

Talk to our team

SOCURA

© Socura Limited. All rights reserved.

hello@socura.co.uk
0800 640 4067
LinkedIn
Bluesky