ThreatAware

How Bird & Bird Gained Complete Asset Visibility

Bird & Bird

Bird & Bird is an international law firm specialising in intellectual property and tech law, serving major technology companies, government entities, sports organisations and pharmaceutical clients worldwide.

Industry: **Legal Services**

Size: **3,700 users**

Locations: **33 offices globally**

Situation

Bird & Bird's security team couldn't obtain a definitive answer on the number of devices they had or confirm that security controls were deployed everywhere. Multiple systems (SCCM, Intune, Tenable, Cortex, ServiceNow) reported different numbers.

The team spent hours exporting data from multiple systems, manually comparing in Excel. Different teams provided contradictory information, and cyber insurers required proof that security controls were functioning, not just deployed.

Impact

The conflicting asset data created dangerous blind spots. Security tools couldn't detect devices where their own agents weren't working. Compliance reporting, like Cyber Essentials, required gathering data from multiple teams across different systems.

Dan Fleming, Information Security Specialist, described the problem: "**I would speak to the desktop team and ask, how many desktops? One number. I'd speak to the server team and ask, how many servers? A different number. Then I'd ask the endpoint protection team and receive yet another different number.**"

Outcomes

- **Identified hidden Windows 10 devices missed by traditional monitoring during end-of-life migration**
- **Eliminated manual data gathering, saving hours on compliance reporting**
- **Discovered running VMs thought to be offline, preventing unnecessary costs**
- **Automated alerts and Tines integration reduced the average time to contain a critical incident**
- **Provided cyber insurance confidence through cross-verified security control validation**

Customer Validation

"Before ThreatAware, we wouldn't have known about devices that don't appear in every asset management platform. It gave us the ability to check everything. I saved myself time, I haven't had to contact multiple teams because I've got all the integrations set up in ThreatAware."

Dan Fleming, Information Security Specialist

"You can't be 100% certain that your security controls are deployed and correctly functioning throughout your estate when relying on disparate tools. You need a single source of truth that correlates results from multiple systems and corroborates evidence. That's just a reality of modern computer systems."

Martyn Styles, Chief Information Security Officer

Results

ThreatAware unified data from 13 integrations into a single platform, providing real-time visibility across 3,000+ users in 33 global offices. The deployment was fast and simple: within a few hours, data was flowing and made sense from day one.

No complex installation was required, the cloud-based platform used simple API integrations with minimal IT resources needed. Integration with Tines automation enabled automated remediation workflows. The introduction of AI Studio transformed how Bird & Bird uses ThreatAware, making it easy to create reporting dashboards through a conversational interface.

Discover how ThreatAware can provide complete visibility across your asset estate and eliminate hours of manual reporting.

threataware.com