Funding Circle

At a Glance

- Achieved 100% on-premise and AWS visibility with unified view
- Dramatically reduced the incidence of false positive alerting
- Detected serious compliance breaches including crypto-mining

Funding Circle is a peer-to-peer lending marketplace that empowers private investors, governments, and financial institutions to lend money directly to small businesses.

Security Pressures in the Financial Services Industry

The first website to facilitate peer-to-peer business financing in the UK, Funding Circle now also operates in the US, Germany, and the Netherlands. Its 81,000 global investors have lent approximately £7 billion to date, creating an estimated 115,000 new jobs in 2018 alone. Given the rapid evolution of the cyber-attacks targeting these funds — as well as the equally rapid expansion of the company itself — Funding Circle sought a security solution capable of keeping pace with both the changing threat landscape and its own changing network.

The financial services industry suffered more cyber security incidents than any other economic sector in each of the last two years, with European financial firms facing an average of 85 annual attempted breaches. To protect its valuable assets and sensitive data, the industry has responded by investing heavily in conventional cyber defenses. Yet criminals have countered by launching never-before-seen attacks designed to bypass traditional security tools, which rely on rules, signatures, and prior assumptions to detect known threats.

Beyond the overarching challenge of preempting never-before-seen malware, Funding Circle was especially concerned by threats to its cloud infrastructure, which introduced key security blind spots. Indeed, gaining visibility into AWS — where the company houses sensitive corporate data — is a priority for many organizations migrating to the cloud. From social engineering attacks to insider threats to stolen credentials, many of the risks to services like AWS are user-dependent. As a consequence, any security tool up to the task of defending an AWS environment must understand how these users work and collaborate across the entire digital infrastructure — not just within one application or service.

Finally, Funding Circle found that, as it made changes to its AWS infrastructure, its security stack struggled to differentiate between benign modifications and genuinely malicious activity, generating a flood of false positive alerts. Without enough time in the day to sort through so many false positives, the company needed an AI tool to automatically prioritize the most serious incidents on behalf of its security team.

Funding Circle

Boosting AWS Defenses with Darktrace/Cloud

Following the completion of a successful Proof of Value (POV), Funding Circle deployed Darktrace, including Darktrace/Cloud to defend its AWS workloads. Powered by Self-Learning AI, Darktrace immediately began learning the normal 'pattern of life' of every user, device, and container at the company. This continuously refined sense of 'self' enables the AI to detect even subtle deviations from normalcy, such as never-before-seen threats that exhibit highly anomalous behavior.

With Darktrace/Cloud, Funding Circle's lean security team also gained total oversight over cloud activities that had previously been invisible. As CSPs like Amazon continue to bolster their defenses, cyber-criminals are increasingly targeting the customer's portion of the cloud's Shared Responsibility Model, rendering visibility all the more important. In fact, industry experts estimate that 99% of cloud security failures will have occurred at the customer end through 2023. But with Darktrace DETECT flagging unusual malicious activity in the cloud, Funding Circle's workflows are secured across its digital environment.

Uncovering Insider Threats and Vulnerabilities

Darktrace rapidly transformed Funding Circle's security posture, affording it real-time insights into all activity across its cloud infrastructure. Among the numerous cyber hygiene issues that Darktrace DETECT has drawn out are insider BitTorrent usage, connections to unauthorized SaaS applications, and crypto-mining using company resources. Moreover, because Darktrace AI intelligently prioritizes potential threats based on its nuanced understanding of 'self,' it all but eliminated the company's flood of false positives. "Our infrastructure is pretty volatile, since we have a lot of containers coming online and offline frequently," commented Martinez. "In the past, this volatility has led to a high number of false positives, but Darktrace is able to sift through the noise to find the genuine threats".

> "For our small security team, the unified view that Darktrace gives us over our hybrid and multi-cloud infrastructure has been a game-changer."
>
> Alberto Martinez,
> Senior Information Security Engineer, Funding Circle

> "Darktrace was extremely easy to deploy compared to the other vendors we tried, and the visibility it gave us over our cloud environment was night-and-day compared to the capabilities we had before."
>
> Alberto Martinez,
> Senior Information Security Engineer, Funding Circle