2021 Industry Spotlight: Nonprofit

Recent history has shown that 'the third sector' is a lucrative target for cyber-criminals. Nonprofits tend to hold a breadth of digital records on their systems, including private mailing lists, confidential data, and the credit card information of members and donors. As a result, it is critical that nonprofits bolster their cyber maturity.

At a Glance

- ✔ Autonomously detects and responds to novel and sophisticated attacks in seconds
- ✔ Learns 'on the job', understanding 'normal' for every user and device
- ✔ Full visibility and protection across cloud, SaaS, email, endpoints, industrial systems, and on-premise networks
- ✔ Up to 92% reduction in time to triage with automated investigations

Balancing Growing Digital Complexity With Protecting Sensitive Data

Compared to the private sector, nonprofit organizations often struggle with maintaining robust and up-to-date IT systems. Many charities cannot afford to have on-site IT employees; yet, they operate over a sprawling digital infrastrucutre, often supporting various projects in a variety of locations, and rely on part-time volunteers working from home, frequently from personal devices and public Wi-Fi.

Untrained volunteers and employees can unwittingly compromise a system through falling victim to a phishing attack and opening a malicious attachment. Without the proper protection in place, these attacks can be devastating for an organization.

Furthermore, nonprofits are adopting more complex digital ecosystems, increasingly leveraging cloud infrastructure for its flexibility and cost-effectiveness. Although this may increase productivity, it expands the attack surface and leaves organizations vulnerable. Worryingly, investment in cyber security has not matched this drive to modernize: according to a report by NTEN, 80% of nonprofits do not have a policy in place to deal with cyber-attacks.

When Blackbaud, a third-party software company which hundreds of charities rely on, was hacked last year, the data of millions of customers was exposed. Becoming collateral damage in a larger ransomware or nation-state attack can be fatal to a nonprofit, costing more than the organization can afford. With the third sector already struggling with staffing and a limited internal operating budget, it is essential for these organizations to be properly protected.

> "Darktrace Antigena constantly spots and stops developing threats across our digital infrastructure, without disrupting the crucial services we provide."
>
> Jonathon Koh, IT Manager, AWWA

Protecting Nonprofits With Cyber AI

Darktrace protects the sensitive data and distributed workforces of major charities around the world. Powered by AI, its technology is inspired by the principles of the human immune system, learning what is 'normal' across the entire digital ecosystem for every user and device, and all the connections between them. This allows the self-learning AI to detect subtle deviations indicative of a cyber-attack – no matter how novel or sophisticated.

With Autonomous Response, Darktrace Antigena surgically neutralizes these threats, taking targeted action to contain a fast-moving attack like ransomware in seconds without disrupting normal operations.

Many nonprofits rely on remote workers and international volunteers, making their systems complex, expansive, and difficult to protect. A fundamentally dynamic technology, Darktrace works across the entire digital ecosystem, protecting cloud and collaboration platforms, IoT and OT systems, as well as endpoints devices and the traditional network.

Each threat Darktrace finds is clearly presented in a graphical and intuitive user interface, with Cyber AI Analyst automatically investigating, triaging, and reporting on each security incident – putting teams in a position to take action immediately.

In today's threat landscape, AI technology is no longer a nice to have but a necessity in protecting against advanced attacks.

Detecting Unauthorized Password Access at The Y NSW

The Y NSW is one of the oldest and largest youth organizations in the world, with a small team managing its entire digital infrastructure. Darktrace AI has given the team the ability to identify and remediate threats as soon as they arise, recently detecting unauthorized access to a file containing user passwords.

The threat arose when a file containing passwords was accessed by an unauthorized user on the network. Darktrace instantly alerted the charity's IT team, allowing them to identify the user and remediate the threat immediately – a threat which would have gone unnoticed otherwise.

Last year, when The Y was forced to close its physical facilities and conduct its operations remotely, Darktrace aided its transition. With the Darktrace Mobile App, the charity's security team remain connected to its IT infrastructure at all times and can respond to threats as soon as they occur.

> "The Darktrace Immune System is key to defense in today's world of escalating cyber-threat."
>
> Darren Bisbey, Head of ICT Infrastructure and Cyber Security, RAFA

Threats by Numbers

of nonprofits do not regularly train their users in cyber security.

of nonprofits have not calculated their potential risk exposure or run a vulnerability assessment.

Over half of nonprofits do not have multi-factor authentication (MFA) to access online accounts.

Cyber AI Analyst automatically generates Incident Reports which detail every stage of an attack