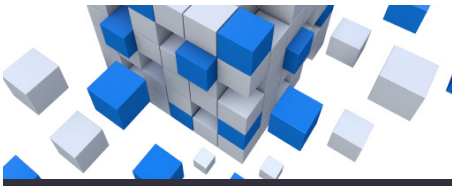
DARKTRACE

Darktrace for Mergers & Acquisitions

AI for Cyber Security Due Diligence

PRODUCT OVERVIEW

Measuring Cyber Risk in Mergers and Acquisitions



Key Benefits

- Detects and responds to latent threats prior to network integration
- Minimizes cyber risk during M&A
- Generates unified view in a single, intuitive UI
- Identifies critical vulnerabilities and misconfigurations
- Monitors bespoke compliance breaches

"In today's cyber environment, companies can never be too vigilant given the increasing complexity of cyber-threats in M&A deals. Darktrace's Enterprise Immune System is helping us stay proactive and aware of our cyber risk profile."

Robert Dennehy, SVP
MACOM

"Darktrace detects and responds to threats that other tools miss."

Jonas Knudsen, Research Director, IDC

The assessment of cyber risk is becoming a critical part of Merger and Aquisition (M&A) due diligence, as the impact of an unknown cyber-intrusion on valuation and reputation can be significant. In addition to the audit of financial statements, the inspection of buildings, and the validation of intangible assets, M&A teams must add to the checklist a comprehensive evaluation of an organization's digital estate and identify incidents that represent a potential liability.

Thus, one of the fundamental challenges when it comes to M&A is determining the cyber hygiene and security of the target network before it is integrated into the parent network. To achieve this level of visibility and due diligence, a new approach to cyber security is needed.

Challenges in M&A Due Diligence

Firstly, the acquirer team must be able to identify a pre-existing or past cyber-intrusion. This could manifest itself as a customer data breach, the disclosure of which would harm the company's brand reputation, or as evidence of a reconnaissance campaign that undermines the value of intellectual property.

Secondly, the merging of two networks, on completion of the deal, is a process that can expose the parent company's networks to vulnerabilities from the child company's network that they were not aware of. To protect against this, the acquirer needs to understand exactly what is going on inside that new network and mitigate risk, before joining them up.

This understanding of the digital network is lacking for most M&A teams. Today's networks are interconnected and dynamic, and in reality, it is not feasible to shut out all potential attackers or vulnerabilities. Most companies face some level of threat from within, whether from sophisticated attackers that bypass traditional security controls or an insider with a grudge against their firm. While their existence is inevitable, these threats can be managed through good policy and technology, but it has been difficult to assess that level of digital resilience from the outside.

As we enter a new era of increasingly advanced attack types, it is imperative for M&A teams to gain a high-level understanding of the state of the digital infrastructures that they are set to acquire, and mitigate vulnerabilities that may exist, in order to fulfill the potential of a successful transaction and avoid any damaging fall out.

AI for Cyber Due Diligence

A major aspect of cyber due diligence is ensuring that the target company's intellectual property has not been compromised or stolen by a competitor or nation state. Moreover, threats often remain hidden in the noise of the network by leaking or manipulating data slowly over days and weeks. Traditional security tools fail to detect such subtle threats and breaches.

Darktrace's Enterprise Immune System uses machine learning and AI algorithms to learn the normal 'pattern of life' for every user, device, and network in an organization. It continually updates its understanding of normal and detects and responds to threats in real time.

Darktrace for M&A

This capability generates a holistic overview of network architecture, as well as a detailed perspective on the behaviors of every user and device. The parent company can use this self-learning technology to assess the networks of firms they have acquired and those they plan to acquire, prior to completing the transaction.

The Enterprise Immune System installs in less than an hour, and it immediately generates a unified view on a 3D graphical interface. Using the intuitive Threat Visualizer, the parent company can conduct a thorough investigation of any vulnerabilities or threats in the target network.

Armed with Darktrace's AI technology, companies minimize the security risk of the acquisition, evaluate whether a threat actor is entrenched in the network, and gain unprecedented visibility throughout the cyber due diligence process.

Compliance and Network Configuration

Darktrace's customizable cyber AI platform allows companies to configure model breaches to raise alerts based on the parent's compliance policies. For instance, if the parent company prohibits Dropbox usage, they can create a model breach that detects Dropbox usage in the child organization in real time. Similarly, companies can identify anomalies in the target network's configuration – for instance, ports being used for unauthorized tasks.

In some cases, firms have identified significant misconfigurations and vulnerabilities. In others, companies have discovered the target network had a 'clean bill of health' and continued to use Darktrace for due diligence and the eventual merger.

A global manufacturing company, which makes several acquisitions per year, uses Darktrace's self-learning technology to automatically understand and detect early-stage threats. Additionally, Darktrace can generate models to monitor compliance and policy discrepancies. By continually monitoring both networks for anomalies and compliance breaches, the organization was able to achieve a smooth transition and avoid introducing novel threats into their network.

"Darktrace's technology gave us visibility into potential implementation differences and policy discrepancies. Leveraging Darktrace allowed us to identify and remediate these differences before connecting the two networks, thus mitigating potential integration risks."

Robert Dennehy, SVP
MACOM

"When you buy a company, you're buying their data, and you could be buying their data-security problems. Cyber risk should be considered right along with financial and legal due diligence considerations."

Jason Weinstein,
Former Deputy Assistant Attorney General,
US Department of Justice

About Darktrace

Darktrace is the world's leading AI company for cyber defense. With over 7,000 deployments worldwide, the Enterprise Immune System is relied on to detect and fight back against cyber-attacks in real time. The self-learning AI protects the cloud, SaaS, corporate networks, IoT and industrial systems against the full range of cyber-threats and vulnerabilities, from insider threats and ransomware, to stealthy and silent attacks. Darktrace has 800 employees and 39 offices worldwide. It is headquartered in San Francisco, and Cambridge, UK.

Contact Us

North America: +1 (415) 229 9100
Latin America: +55 (11) 97242 2011
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
info@darktrace.com
darktrace.com