DARKTRACE

WHITE PAPER

General Data Protection Regulation (GDPR)

Real-Time Cyber Defense and Early Threat Detection

Contents

Overview

On April 27th, 2016, the European Council, Commission, and Parliament published the final version of the General Data Protection Regulation (GDPR), which became legally binding in all EU member states on May 25th, 2018.

In material terms, GDPR defines a person and their personal data as:

> 'An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.'

In territorial terms, the law regulates any entity established or proactively offering goods and services within the European Economic Area (EEA). This will include international and cloud-based offerings targeting customers in the EEA.

Additionally, the GDPR specifies that a data breach must be reported to the Data Protection Authority (and in some cases the individuals impacted) within 72 hours of becoming aware of the breach. For processors (those which, alone or jointly with others, process personal data on behalf of the controller) this means they will need to notify the controllers (those which, alone or jointly with others, determine the purpose and means of the processing of personal data) well within the 72-hour window.

> "Darktrace is welcome addition to any cyber-security toolkit increasing visibility while decreasing response times."

VP of IT, Financial Service

This requirement does mean that companies will need to adopt internal procedures to identify breaches and assess the risk in a timely manner, in order to determine if a breach is reportable.

The implementation of GDPR represents one of the most significant events in data protection regulatory history. The regulation is a game changer not only in terms of scope and ambition, but also the significant penalties for non-compliance: the fine for non-compliance can be up to 4% of global annual turnover (sales).

Darktrace is applicable to a range of requirements under GDPR. Darktrace provides the real-time visibility required to make intelligence-based decisions in live situations, while enabling in-depth investigations into historical activity.

Based on important advances in Bayesian probability theory and powered by cutting-edge machine learning, Darktrace ingests communications and creates a unique behavioral understanding of 'self' for each user and device in the organization. Darktrace detects threats that cannot be defined in advance by identifying even subtle shifts in expected behavior.

This technology is ideally suited to detecting cyber-attacks in their earliest stages before they become data breaches; even previously unknown threats that are novel or tailored. By identifying unexpected anomalies, controllers and processors are able to investigate compromises and insider risks as they emerge and throughout the stages of an attack's lifecycle.

A New Era in Automation

Darktrace was founded with a vision to free the world of cyber disruptions, providing organizations with the ability to fight back against threats across cloud, email, endpoints, IT & OT, and more.

Automation is central in keeping up with the quickening speed and sophistication of cyber-attacks, as humans alone are increasingly struggling to defend their networks from attackers. Machine learning is critical to how we deliver automated cyber security solutions.

Advanced machine learning can be used to analyze large data sets, and extract 'meaning', helping us to make sense of overwhelming volumes of information.

Darktrace's approach to cyber defense is based on some of these fundamental advances in probabilistic mathematics and machine learning developed by mathematicians from the University of Cambridge, the core of our technology.

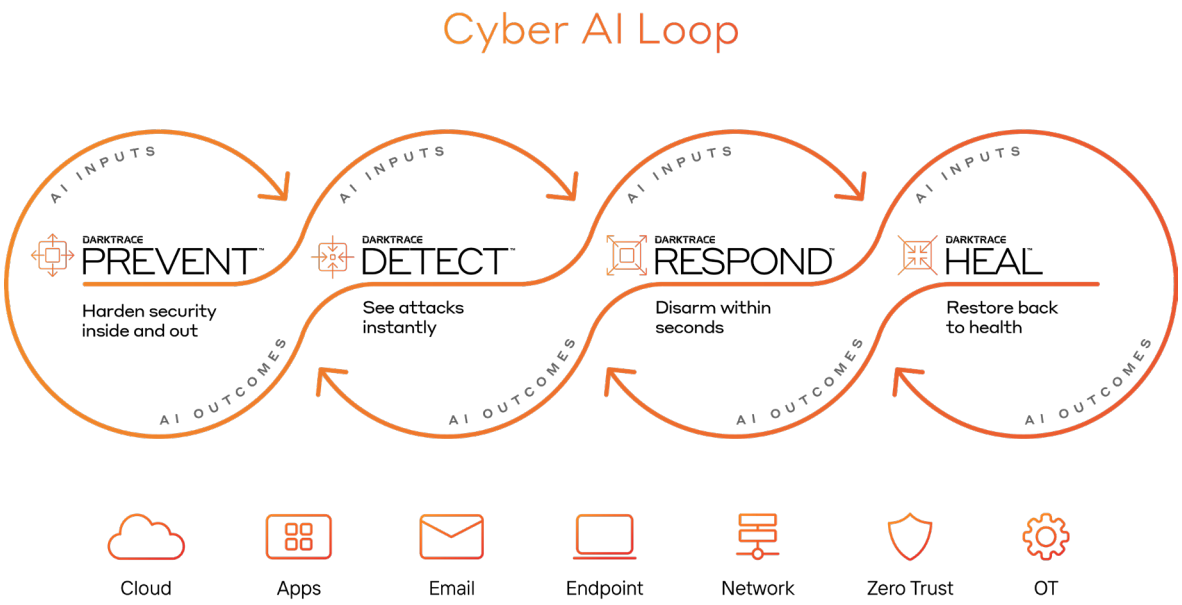
This probabilistic mathematical approach is critical to Darktrace's unique ability to understand important information, throughout the digital estate – even when faced with unfamiliar activity, making it the de facto approach to address today's fast-evolving threat landscape.

> "We see this as a very good tool and complement to our security work. When it comes to the actual monitoring of your real-time IT environment, adding AI driven technology helps and might even be the best and only way to do some things."

CTO, Technology and Telecoms

Cyber AI Loop

Cyber AI Loop is made up of four AI-powered product families - PREVENT, DETECT, RESPOND, and HEAL – that operate in any digital environment. They can operate on external data, internally in cloud infrastructure or applications, email systems, endpoints, the corporate network, or industrial systems. This comprehensive feedback system allows each capability to inform the other and ultimately hardens the entire security system, working throughout the attack lifecycle before an attack even happens all the way through to the aftermath of a cyber-attack.



Darktrace PREVENT

Darktrace PREVENT allows the security team to identify, prioritize, and test vulnerabilities, reducing risk and hardening defenses both inside the organization and outside on the attack surface – continuously and autonomously.

PREVENT continuously analyzes the most critical attack paths on your organization, and feeds that information back into DETECT + RESPOND to support continuous learning and systems hardening.

The PREVENT product family consists of two products: PREVENT/Attack Surface Management (ASM) which continuously monitors your attack surface for known and unknown external risks, and PREVENT/End-to-End (E2E), which hardens defenses internally, allowing security professionals to test and prioritize the most critical attack paths in their organization.

Darktrace DETECT

Darktrace DETECT delivers instant visibility to threats in any digital environment. Anywhere data resides from cloud infrastructure and applications to email systems, endpoints, zero trust technologies, on-prem networks and Operational Technology (OT), DETECT can identify even the most advanced forms of cyber-attacks, including novel malware strains, spear phishing, ransomware attacks.

Darktrace DETECT does not require previous experience of the threat or pattern of activity in order to understand that it is potentially threatening. No rules or signatures are needed. Instead, it uses its evolving understanding of 'normal' for your organization to establish subtle deviations indicative of a cyber-attack.

Darktrace RESPOND

Darktrace RESPOND delivers autonomous, always-on security that contains and disarms attacks within seconds. When a threat is detected, RESPOND interrupts malicious or dangerous activity, by taking proportionate action; for example, locking a link or rewriting an attachment rather than withholding an email or blocking a specific connection over a port rather than quarantining a device, allowing normal business activity to continue while remaining secure.

Because the AI learns 'on the job' to continuously improve its understanding of 'normal', even as your business grows and makes changes, Darktrace RESPOND adapts to new technologies, employees, and systems when they are added.

Darktrace RESPOND is customizable: users can set the parameters to determine how and when it should take action. You might want the AI to only act at certain times of day, or on certain devices, or in response to certain events. AI makes millions of micro-decisions in the background, uplifting human teams to focus on making strategic decisions that align with business needs.

Cyber AI Analyst

Cyber AI Analyst connects individual anomalies across the organization to investigate full security incidents at speed and scale. It produces incident reports on critical events and the context around them, augmenting human security teams and enabling them to focus on the highest priority threats, save valuable time, and direct their expertise to the higher-level and strategic work.

Breach Notification within 72 Hours

The GDPR introduced a duty for all organizations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. If the breach is sufficiently serious to warrant notification to the public, the organization responsible must do so without undue delay.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stores or otherwise processed.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organization becoming aware of it. For processors this means they will need to notify the controllers well within the 72-hour window.

The Ponemon Institute found that the average time to identify a data breach is 201 days and the average time to contain a data breach is 70 days. This requirement means that companies will need to adopt internal procedures to identify breaches and assess the risk in a timely manner, in order to determine if a breach is reportable.

The ability to detect unusual behaviors or anomalous activity early, as it emerges, is therefore critical. Darktrace DETECT's threat detection capability uses a self-learning approach, and it can accurately pinpoint genuinely suspicious behaviors, against its evolving sense of 'normal' behavior.

Darktrace analyzes 100% of network traffic, allowing a full overview of all machine and user activity within an organization's infrastructure in real time.

Real-time visualization of your environment and potential threats helps the process of understanding threat within the context of your day-to-day business activities and improves analysts' ability to uncover vulnerabilities before they are exploited.

The ability to monitor data from any part of the digital environment, in an intuitive and digestible way lies at the heart of Darktrace's user interface. Threat visualization technology gives an unprecedented view into your organization.

Darktrace's fully interactive visualization tool not only provides a high-level oversight of threat levels, but also allows you to dive deep into granular details, such as specific connections of particular devices, or the pace of data transfers outside the organization.

Darktrace is uniquely capable of mitigating threats by facilitating their discovery and limiting their spread. Key to this is that an unknown threat does not go unseen. Darktrace does not use signatures or patterns in the same way as a firewall or antivirus.

Designed to work in all sizes of organizations, from small businesses to large and complex networks with tens of thousands of users, Darktrace's technology learns the normal pattern of life for all users and data, automatically finding the threats that routinely bypass legacy security tools.

International Data Transfers

The GDPR require that protection of personal data should not be undermined when transferred to countries outside the EEA and should be carried out in compliance with the regulation. Given that GDPR applies to all EU citizens, and not just data processed in the EU, the rules around international transfers will become more relevant.

The increasing use of cloud services blurs the picture further as it breaks down geographical barriers, but EU regulation retains very strong geographical boundaries.

In July of 2020, the European Court of Justice concluded that the Shield Framework, which governed the transfer of personal data from Europe to the United States, was inadequate. The development implies that organizations who transfer data to the US or other third parties must assess the state of data protection in said third party. This involves risk assessment and implementing additional protection for the transferred data.

Darktrace PREVENT has the ability to assess risk, while DETECT can identify anomalous behaviors, including data transfers both within a company's network, and to external sources.

Across our customer base, Darktrace has detected a wide range of different anomalies. For example, Darktrace identified that one of the company's database servers was repeatedly allowing unencrypted connections from various internet locations. These machines were using a range of IP addresses allocated to a telecoms company in the Far East. Darktrace's processing of these connections suggested that the data being transferred was financial information. Attackers often target database servers for the high-value information that they hold.

The direct, unencrypted communications from the internet to this server that Darktrace observed were extremely risky. The potential for leaking or changing vital financial information through this server represented a serious risk to the company's operations and reputation.

Privacy & Compliance

Organizations now fall under increasing pressure to conform to an ever-changing set of regulations, standards, and frameworks. This often requires more spending on security systems and labor, across detection and response systems, but also with asset management and risk assessment.

In addition to inducing higher spending, compliance policies also require evidence that your organization is complying to the laws. Darktrace PREVENT can generate the appropriate reporting, risk scoring, and customizable compliance features that are necessary to address specific compliance frameworks that apply to each organization.

Darktrace DETECT also helps with privacy and compliance. DETECT collects and inspects data from within the enterprise's network. This collection and analysis is fundamental to the Darktrace's approach to cyber defense, and its ability to detect novel threats in today's complex business environments. This process has been designed with data protection and controls in place.

The analysis of raw data flow does not include the content of data files, but the information collected is used to correlate data between the source and the receiver for a given traffic session.

To do this, metadata is extracted from rich data flow and Darktrace's unique mathematical algorithms are applied to check for anomalous or suspicious behaviors inside the network.

Extracted metadata is stored in a rolling buffer on the appliance(s) within the customer site and is expired as disk space requires. The customer can back up this data elsewhere, if required. The amount of metadata (such as the amount of data in the transaction body of a packet) stored on the appliance is configurable.

Additional controls define who can access data on the appliance and what data they can access. For example, user accounts can be granted restricted access to subsets of the Darktrace functionality. Stringent access profiles and auditing are applied to all activity on the appliance, which can be recorded and reported to a data controller.

> "Utilizing Darktrace artificial intelligence and behavioral analytics provides our security analysis team with actionable insights for threats and anomalies."

Head of Security Operations, Government and Defense

Security

Darktrace maintains high security standards within the organization, demonstrated by our ISO certification and compliance with Cyber Essentials.

Darktrace has successfully been certified with ISO 27001:2013. This internationally recognized, third-party validation demonstrates how seriously Darktrace takes its internal security and validates the information security management system that it has in place.

Darktrace's compliance with the UK Government-backed and industry-supported Cyber Essentials scheme further validates our approach to security. The Cyber Essentials scheme provides guidance on good cyber security practices to organizations, to ensure they are protected against the most common cyber-threats.

Connections to and from Darktrace are encrypted, using high-grade TLS encryption with perfect forward secrecy. User passwords are salted and one-way hashed for storage. Data in the system is protected from unauthorized deletion or modification by users.

Anonymization Mode

Darktrace can be configured for enhanced anonymization, using Anonymization Mode. If set, this mode anonymizes various aspects of the data seen by Darktrace.

If an incident is identified in Anonymization Mode, the analyst can seek internal approval to conduct an in-depth investigation. Once approval is given, the analyst temporarily logs in as a user with additional privileges. This provides them with the visibility necessary to conduct a thorough investigation of the incident.

Anonymization Mode grants sufficient visibility for analysts to conduct initial triage and to identify incidents, while still protecting the privacy of employees and other users.

Investigative Tools

Darktrace PREVENT brings together several aspects of preventative security into a single end-to-end solution that allows defenders to investigate their most critical attack paths. The technology combines an outside-in view of an organization with an internal view of an organization's every user, device, and how they communicate.

PREVENT/E2E continuously identifies all potential pathways and analyzes every digital touchpoint. From this, it assesses your most vulnerable and critical attack paths, learning the potential impact of each user, device and system, and then how exposed they are.

The technology can use generative AI to simulate a real attack path, creating social engineering messages that mimic a sophisticated attack. This tests the validity of critical attack paths already established, while serving to increase the security awareness of your employees.

PREVENT/E2E then produces prioritized mitigation advice through explainable AI, showing how to reduce risk. With zero impact to actual business operations, you have the capability to view ransomware risk scores, KPI scores for overall risk, and your domain ownership.

Similarly, the ability to monitor and investigate security incidents in an intuitive and digestible way lies at the heart of Darktrace's user interface. Combining the ability to prevent, detect, respond to, and heal from cyber incidents across the digital enterprise allows users to avoid dashboard-switching and uncover the full scope of a compromise.

Darktrace's fully interactive visualization tool not only provides a high-level oversight of threat levels, but also allows you to dive deep into granular details.

As cyber security has become a boardroom issue, the ability to visualize and demonstrate anomalous activity to non-technical personnel, including board directors, is critical, and the Threat Visualizer is an excellent tool to help broaden engagement and encourage common understanding on this issue.

The Threat Visualizer supports collaborative work with its easy-to-use, drag-and-drop functionality, allowing analysts to add comments to incidents and generate threat reports, which may be shared and published. Report generation also facilitates investigation auditing.

As a fully customizable interface, users may include additional business context to enrich any traffic analyzed by Darktrace. For example, users may tag specific devices or prioritize models that are particularly pertinent to the organization.

One-click analysis allows users to visualize and correlate relevant information and provides the context for a breach or incident. Concise summaries of overall behavior for devices and external IPs are provided and can be easily integrated with existing dashboards or tools. This speeds up the analysis process, allowing security teams to make quicker decisions about investigations.

> "Network configurations and known vulnerabilities are constantly changing. Rather than relying on static pentest reports or manual reconnaissance, PREVENT gives us continuous monitoring and reporting of our attack surface - allowing our security team to focus on the most relevant, up-to-date data.

Vanquisher of Virtual Vulnerabilities (V3PO), Food Manufacturer

GDPR Extract

Data Breach Recitals 85, 87, 88 & Articles 33, 34, 83

Recitals

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

Article 33: Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34: Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. L 119/52 EN Official Journal of the European Union 4.5.2016
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in para- graph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in para- graph 1 is no longer likely to materialize; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Article 83: General conditions for imposing administrative fines

Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

a. The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
b. The intentional or negligent character of the infringement;
c. Any action taken by the controller or processor to mitigate the damage suffered by data subjects;
d. The degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
e. Any relevant previous infringements by the controller or processor;
f. The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
g. The categories of personal data affected by the infringement;
h. The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
i. Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
j. Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
k. Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

For more on Article 83, visit https://gdpr-info.eu/art-83-gdpr.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,400 organizations globally from advanced cyber-threats.

Scan to LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

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