Using Darktrace Cyber AI to Support CCPA Requirements

Overview

The California Consumer Privacy Act of 2018 (CCPA) lays out a variety of requirements concerning how organizations manage and secure consumers' personal information and data. Darktrace Cyber AI technology helps companies maintain visibility over their entire digital estate to continuously monitor sensitive data, supporting obligations in accordance with CCPA and similar regulations. Darktrace also offers customizable compliance models that specifically monitor and safeguard user data to support a business's efforts to comply with CCPA.

CCPA Summary

The CCPA is the most comprehensive and significant data protection regulation enacted in the United States to date. While the CCPA continues to evolve as California's legislature considers implementing a variety of additional regulations, effective onward from January 1, 2020, the CCPA applies to many for-profit entities (see 'Scope of Coverage' below) conducting business in California — a state which ranks as the world's fifth-largest economy. Thus, like the European Union's General Data Protection Regulation (GDPR), the CCPA has global ramifications.

The CCPA provides California residents with a number of foundational data privacy rights, including:

- **"The right to know"** what personal information a business has collected about them, where it was collected, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold.
- **"The right to opt out"** of allowing a business to sell their personal information to third parties.
- **"The right to erasure"** that compels a business to delete their personal information.
- **"The right to non-discrimination"** that generally requires businesses to offer consumers equal service and price regardless of whether the consumer exercises rights under CCPA.

Although the CCPA does not directly impose data security requirements, the California Attorney General has the authority to stipulate concrete cyber hygiene guidelines, and CCPA allows consumers to bring private actions against companies that fail to "implement and maintain reasonable security procedures and practices" appropriate to the nature of the information under their care. To help minimize risks, businesses should implement and maintain robust information security practices. See more for "Enforcement and Penalties" below.

Scope of Coverage

In addition to conducting operations in California, a company must satisfy at least one of the below thresholds to be covered by the law:

- Possess annual gross revenues in excess of $25 million.
- Process the personal information of at least 50,000 consumers, households, or devices.
- Earn more than half of its annual revenue from selling consumers' personal information.

The CCPA takes an exhaustive view of what can constitute "personal information" identifying a particular consumer or household. However, the CCPA does not apply to personal information that is already regulated by applicable, sector-specific U.S. federal laws, such as:

- The Health Insurance Portability and Availability Act (HIPAA), which regulates "protected health information" and the healthcare sector.
- The Fair Credit Reporting Act, which regulates consumer reporting agencies and the use of consumer reports they supply.

Enforcement and Penalties

The CCPA is more than a merely symbolic step toward robust data privacy, as evidenced by its precise specification of noncompliance penalties. The CCPA authorizes the California Attorney General to seek civil penalties of $2,500 per violation, or up to $7,500 per violation if the conduct is deemed "intentional". Data breaches that are deemed the result of a lack of reasonable security procedures will trigger sanctions of up to $750 per consumer per incident — or the actual damages suffered, whichever is greater. While it remains unclear, it is likely that each affected individual consumer constitutes a distinct "violation", leading to large expected fines.

Perhaps most significant, the CCPA provides a private right of action for consumers against companies when their personal information is subject to unauthorized access or disclosure, which breach results from the business's failure to implement reasonable security practices and procedures appropriate for the particular types of information. Coupled with the potential for class actions, this provision suggests that future breaches affecting California residents will be far more likely to face intensive legal and media scrutiny.

Supporting Compliance with Darktrace

With CCPA in effect, it is imperative that firms enact compliance measures with the utmost urgency. And while the CCPA's definition of "reasonable security procedures" are subject to further amendments, the Act compels organizations to actively monitor and protect personal information wherever it is housed or transferred — from the network to email to the cloud.

Darktrace's Enterprise Immune System provides 100% visibility into all movement of data through an organization's digital infrastructure, including all parties who have access to that data. Self-learning AI is deployed to learn the 'pattern of life' of every user across cloud, SaaS, email, and on-premise networks. Darktrace Cyber AI can automatically alert or take autonomous action when an access policy is breached. While the California Attorney General must give businesses a 30-day period to assess and remediate alleged violations, Cyber AI provides real-time understanding of cyber incidents, including data exfiltration. Further, Cyber AI's autonomous response works to prevent escalation of cyber incidents with targeted action.

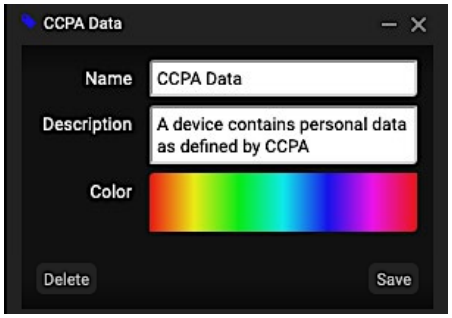
When a customer invokes their right of erasure, a company will also need to have traceability of that customer's corresponding data record throughout its IT applications and networks. Once a database has been tagged in Darktrace, it can be used to help the company understand where that data moves on its network or cloud environment.

In addition to supporting compliance with CCPA, Darktrace has models for supporting other data privacy laws as well as cyber security frameworks, including GDPR, New York DFS, NIST, and the UK NIS Directive.

CCPA Enhanced Protection Models

Businesses who handle consumer data effectively need to be constantly aware of all activity involving that data. The Model Editor within the Threat Visualizer, Darktrace's user interface, provides security teams the ability to track specific parameters for this targeted, continuous monitoring. Darktrace offers customizable compliance models for customers to specifically monitor and safeguard user data as stipulated by the CCPA.

To activate these models, use the tag "CCPA Data" to flag a device as potentially containing personal information subject for CCPA Data.



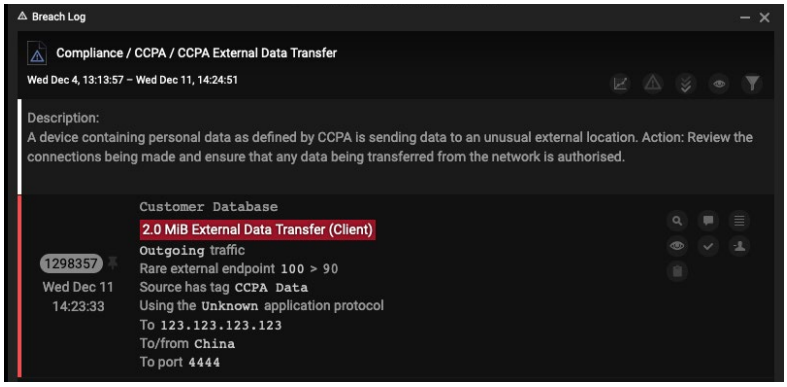
Devices and users can have multiple tags and be subject to multiple models. This allows specific parameters to be flagged according to the needs of your unique business.

Giving a device the CCPA Data tag activates coverage under three models designed to track particular activity:

- `CCPA External Data Transfer`
- `CCPA Internal Data Transfer`
- `CCPA Unusual Activity`

When relevant data from the tagged devices leaves the environment, moves anywhere else on the infrastructure, or is involved in any abnormal activity that does not fit the 'pattern of life', Darktrace flags the behavior immediately and cites the pertinent model for real-time investigation.

Below is an example of such an alert.



These models come standard with Version 4 of the Enterprise Immune System and are also available to existing customers via updates. Utilize the power of Cyber AI to identify and protect the critical personal data of your customers.