oomnitza

USE CASE - CCPA

How Enterprise Technology Orchestration can streamline CCPA compliance efforts

Introduction

The California Consumer Privacy Act (CCPA) is a sweeping privacy law that went into effect January 1, 2020. Considered to be among the strictest privacy laws in the United States, CCPA gives California residents broad powers to control how businesses acquire, store and process their personal information. Attorneys expect CCPA to spark considerable litigation; the first class-action lawsuit under CCPA was filed in February 2020.

CCPA affects any company doing business in the state of California meeting any of the following three basic criteria:

ANNUAL GROSS REVENUES	HOLD, RECEIVE, ACCESS	DERIVE AT LEAST 50%
greater than $25 million	or disclose personal information of 50,000 or more California residents, households, or devices per year	of annual revenues from selling personal information of California residents

This law extends to for-profit companies doing business in California including subsidiaries. As a result of this broad definition, many thousands of companies not just in California but around the world will need to comply with CCPA. While the primary focus of CCPA is use of data and privacy breaches, the law has specific and strong implications for IT asset management. For example, the CCPA expands the definition of data breaches for which consumers could sue companies.

This list includes:

- Social security number, military ID number and passport number
- Driver's license number and CA identification card number
- Credit or debit card number in combination with any required security code that would permit access to a consumer's financial account
- Medical information, or health insurance information
- Biometric data
- Tax identification numbers

The first step in responding to a breach would be to identify its source and the kill chain that resulted in the data leak or credential dump. This requires Enterprise Technology Orchestration (ETO) solution that can quickly track and trace all IT assets back to users, locations, and specific IP address activity. Additionally, IT teams wishing to comply with CCPA to minimize the impact of any breaches or problems will need to proactively build an ETO capability to reconcile, track and trace all IT assets across the entire enterprise estate. This also will have the benefit of helping the company fulfill what the California Attorney General has determined to be minimum reasonable security procedures, which include a list of controls and a level of compliance that can be more easily tuned and checked when ETO is functioning well.

To deliver CCPA compliance a company will need to conduct a bottoms-up and system-wide accounting of all assets under management. Different ITAM systems, including CMDB, SAM, MDM, SaaS and cloud infrastructure management, all manage and track key components of what would be reviewed during a CCPA-triggered audit.

The core of what will need to be asked is the following:

QUESTION 1	QUESTION 2	QUESTION 3
Who has access to the assets?	Where are the assets physically and virtually located?	How are the assets secured and what controls are in place?

Enterprise Technology Orchestration to reduce CCPA Risk

CCPA risk (and asset management risk more broadly) have grown infinitely more complicated as more and more assets (hardware, software, laptops/phones, Cloud, SaaS) enter the digital estate. This creates particular challenges for legacy ITAM systems:

MANUAL ITAM-CENTRIC
processes cannot keep up with exponential device and software/SaaS asset growth

CONTINUOUS CCPA COMPLIANCE
requires process-driven yet agile and adaptive track-and-trace of any new asset types

SILOED ASSET MANAGEMENT
Redundancy and missing assets in traditional ITAM systems can further extend risks

INABILITY TO TRACK & VALIDATE
the presence of reasonable controls in disconnected ITAM tools may contradict California guidance and expose legal risk

The upshot? An accurate, comprehensive cross-silo ETO capability allows for more cost-effective and efficient CCPA prep and compliance. Unlike point solutions and siloed ITAMs, ETO enables automation of key discovery and reconciliation portions of CCPA prep. An ETO system also normalizes data formats across all ITAM types, creating a single database of record that is programmatically addressable and allows export of data via APIs into other systems; this is a critical component of empowering agile and adaptive track-and-trace. Ideally, ETO transforms manual CCPA compliance and prep into software code and scripts that are easy to document and generate actionable insights for better securing the IT estate against CCPA risk.

Use Cases for Enterprise Technology Orchestration mitigation of CCPA risk

ETO has several use cases that can improve, streamline and automate CCPA risk mitigation. Here are some example use cases that illustrate the benefit of ETO.

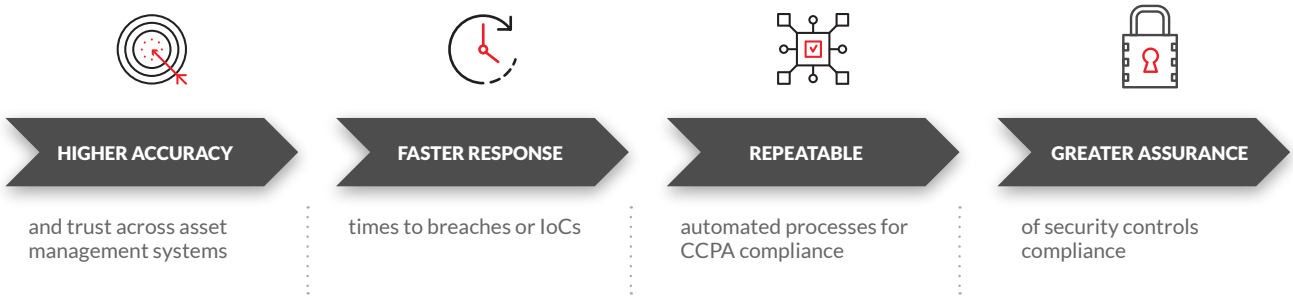
CREATE A SINGLE SOURCE OF TRUTH FOR ALL ASSETS

As previously noted, many organizations have multiple asset management tools and systems, each adopted to solve a specific problem (e.g. hardware vs. software). For the most part, different tools have different ways of pulling in, structuring and updating data. Many lack proper APIs and export as CSV or spreadsheets. Some have automated discovery and others require manual recording by IT personnel. Specifically, many systems have differences in:

- **DATA FORMATS** and schemas
- **VARIETY &** flexibility of data fields
- **CAPABILITIES** for data export
- **LEVELS OF** automation of data capture
- **FREQUENCY** of updates
- **ACCURACY &** reliability of information

As a result of these disparities, IT teams often rely on manual calculations and spreadsheets for asset counting and identification, and for reconciliation processes across asset management tools. This wastes time, results in significant inaccuracies due to human errors and incompatible information, and delivers sub-par results when teams attempt to account for all assets. When a rapid track-and-trace is required as a result of a breach or an Indication of Compromise (IoC), it can take days or weeks to tie a breach to its source, location and asset owner.

ETO that includes automated data capture for all asset management systems eliminates these problems. A properly integrated ETO solution automates data capture, maps fields and schemas into a unified master database, and reconciles across siloed ITAM point solution tools to create an accurate, reliable system of record. This system makes it far simpler to prevent CCPA breaches and to quickly respond to breaches by identifying compromised assets and breach sources. With ETO as well, IT teams can more easily monitor which systems have the proper controls in place in correspondence with CCPA expectations of reasonable security measures. Specifically, ETO's unified system of record and data ensures:



How to leverage Enterprise Technology Orchestration for improved CCPA compliance and response

Installing and rolling out an ETO as part of your CCPA strategy requires some basic thought and planning. Start by determining the key requirements of CCPA mitigation and compliance.

This means you must undertake each of the following steps

After you have run through the CCPA planning process, you should see if you can fix gaps or blind spots in asset management information capture via programmatic means (either code and scripts or workflow automations). Set an initial goal and milestones to ensure your proposed process works as planned. After you have either hit or failed to achieve the initial goal and milestones, reassess your process and plan for viability and validate results against desired outputs and end-state.

If you are satisfied, then continue forward with your CCPA process until completion. You will likely encounter some unexpected hiccups and interruptions as any integration project in a modern heterogeneous IT environment is complicated. This is where the flexibility and agility of an ETO platform are essential; the best ones allow easy ways to move data into and out of the platform and connect outputs of multiple ITAM tools quickly and easily.

BUILDING A BUSINESS CASE FOR INTEGRATED ITAM IN CCPA

Generating a business case for ETO for CCPA is not complicated. To start with, consider the potential risks and costs associated with a breach and class action lawsuit; legal fees, reputational risk, and disruption to business activities. Secondarily, consider the benefits that accrue beyond CCPA compliance, which can include enhanced capabilities such as:

Secondary benefits might of incorporating ETO can actually be as significant, if not more significant, than primary benefits. Secondary benefits might include the following:

Tabulate your cost/benefits and build a business case for ETO as a core building block for CCPA compliance and mitigation. Paint a simple before/after picture so approvers understand the potential costs to the organization of inaccurate, manual and hard-to-update asset management systems with regard to CCPA. You may want to touch on softer but relevant benefits like greatly enhanced CISO/C-Suite/BOD confidence in organizational security and compliance overall - and the fact that CCPA compliance also covers most of what is required for GDPR compliance.

Preparing for and complying with CCPA primarily entails answering the most basic questions about your assets: who, where, and what happened? ETO empowers organizations and IT teams to answer these questions and, by extension, all other questions such as where consumer data is stored and what systems are at risk of a breach. Automating this process, connecting various siloed systems, and replacing manual workflows with scripts and code will not only drive CCPA preparedness but also better business results and overall visibility.

About Oomnitza

Oomnitza is an agentless enterprise technology orchestration solution for digital business. By consolidating technology asset data from siloed systems into a single pane of glass, our customers are able to optimize their technology spend, automate their governance processes to meet compliance and auditing requirements, protect from security risks, and ensure great employee experience and productivity. Oomnitza is headquartered in San Francisco

www.oomnitza.com

 2/21