Starting Your GDPR Journey With Okta

okta

Index

Disclaimer: *While this article discusses legal concepts, it does not constitute legal advice. If you or your organization needs legal advice, please consult with your or your organization's lawyer.*

Introduction

Consumer-facing enterprises have long been stewards of customer identity data, storing sensitive attributes ranging from a customer's name, to credit card numbers and home addresses. But with the ever increasing number of data breaches, privacy concerns, and misuse of data, lawmakers are now stepping in to arm data regulation with teeth. In the European Union, the General Data Protection Regulation (GDPR) was the first step taken to set a new standard for data privacy. As these organizations embark on the journey of continual data privacy compliance and it becomes a C level initiative, enterprises must take a second look at future-proofing their IT infrastructure.

Part I:

GDPR & Business Effects

At a high level, the GDPR is all about individuals owning their own data. This can manifest itself in a variety of methods, from giving an individual the ability to view what kind of data is collected about them by corporations to requesting the erasure of personal information. In the age of enhanced privacy regulations and hefty fines, IT infrastructures must reconsider their approach to compliance.

With the proliferation of massive security breaches like Marriott and Panera Bread in 2018, new data privacy regulations like the GDPR are being enforced to protect individuals' personal data. As awareness of these breaches rises, loss of individual trust is tied directly to customer sentiment, which in turn affects revenue. According to IBM, 46% of organizations suffered damage to their reputation and brand value as a result of breaches of trust. In addition, violation of the GDPR may lead to fines of up to €20MM or 4% of global revenue. Moving forward, enterprises must carefully implement new controls and processes efficiently to comply with these regulations.

The Irish Data Protection Commission and Future Enforcement

The Data Protection Commission of Ireland (DPC), the national independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected, has been busy at work to ramp up their enforcement of the GDPR. As of October 2018, the DPC had opened 80 cases of violations of the GDPR including a statutory inquiry examining Facebook's compliance with the relevant provisions of the GDPR.

Part II:

The Journey to Compliance

As the DPC and other similar data privacy regulators increase enforcement of the GDPR, IT leaders should consider their readiness. In addition to impending enforcement, companies that are compliant today might have trouble staying compliant in the future. The truth of the matter is, GDPR readiness is an ongoing journey with different stages of compliance.

GDPR Maturity Curve

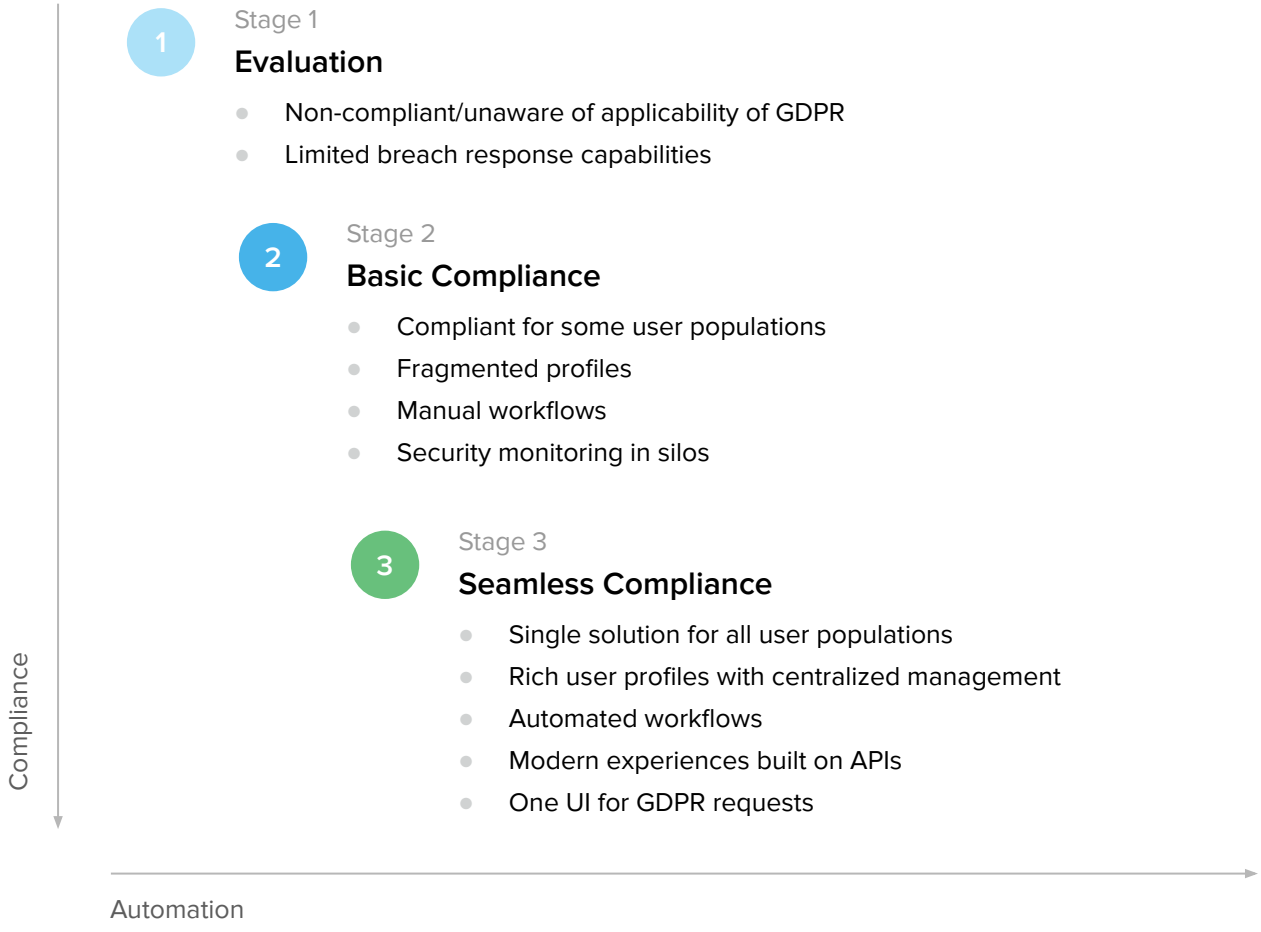


Figure 1

Stage 1: Companies that have not yet started their compliance journey

Since the GDPR came into effect in May of 2018, most companies within the sphere of influence of the GDPR have been scrambling to become compliant. However, there is a significant portion of organizations that may not have thought that the GDPR was applicable to them, or "Stage 1" companies.

According to Article 3 of the GDPR, a company must comply be if it:

- Is a controller or processor in the EU;
- Offers goods and services to EU data subjects; or
- Monitors the behavior of data subjects in the EU.

The language of Article 3 of the GDPR greatly extends the applicability of the GDPR to companies that may not expect a foreign law to apply because it applies even to companies that are service providers, may offer goods and services to data subjects in the EU, or "monitor" the behavior data subjects in the EU. Furthermore, under the GDPR, the definition of personal data is broad enough to include a variety of data types, from social media posts to credit card information collected while booking an airline. Since the definition of personal data encompasses such a broad variety of data, companies are often confused about whether the GDPR applies to their data collection. The leads to many companies being unaware of their applicability of the GDPR to them, and their resulting need to comply with this law.

Stage 2: Companies that are using manual compliance processes

Companies in this stage of the data privacy journey are organizations who were aware of the applicability of the GDPR and have perhaps achieved compliance by manual processes. Depending on the type of organization, this leads to an excess of IT, legal, support and engineering resources being exhausted on compliance and pain from manually configuring different systems. According to Forbes, GDPR costs have eclipsed $8 billion dollars in the US and UK, with these resources being spent on hiring legal teams, consultants, and data protection officers. As requests (like right to be forgotten) pile up at companies, IT admins and helpdesk representatives will spend more cycles on this edge task to keep compliant, rather than working on their core functionalities.

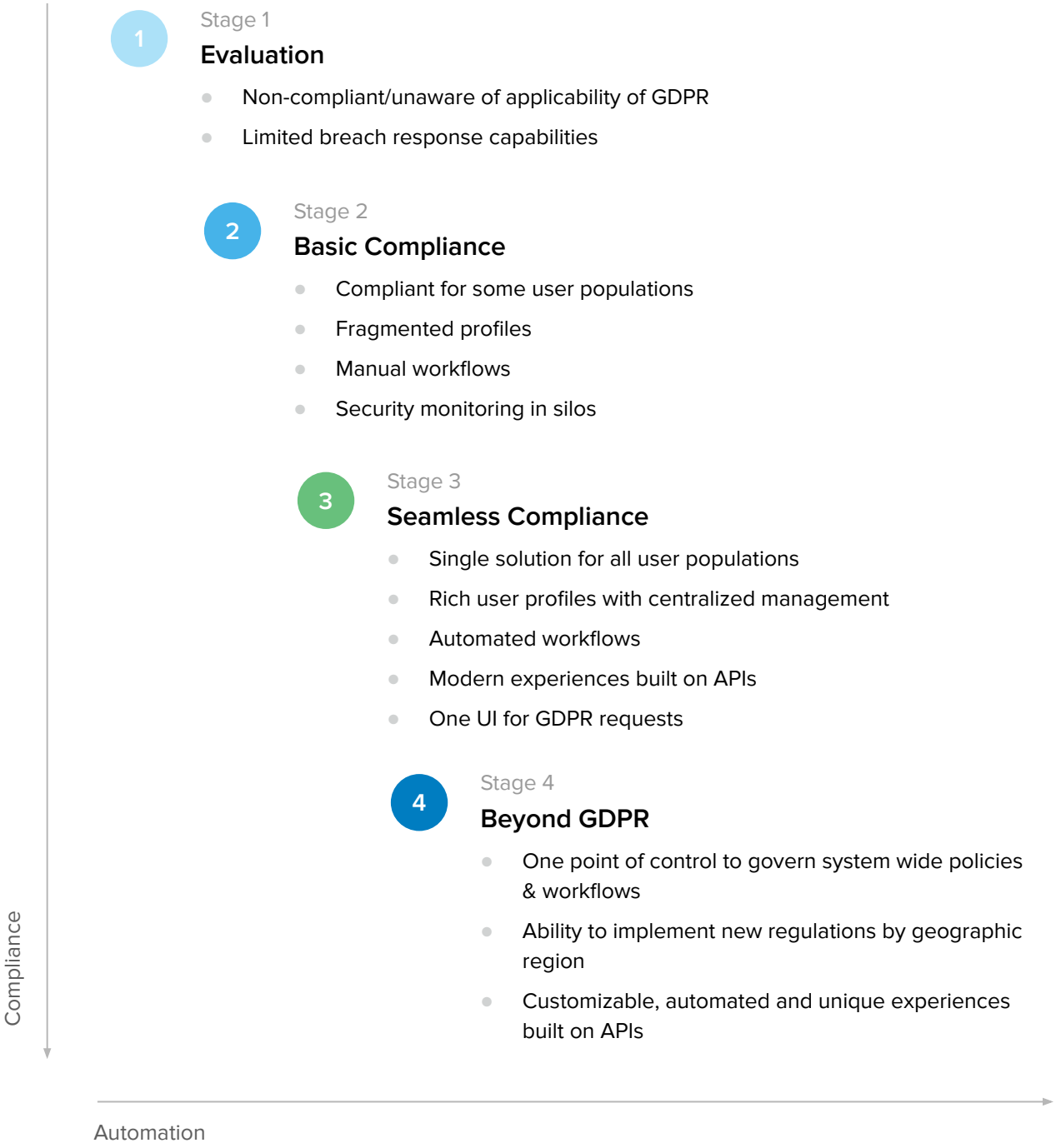
Some companies in this stage also might have only thought about their own employees in compliance, but have not addressed compliance processes that need to be put in place for consumers. This is a growing problem, with companies like Google receiving 2.4 million requests to be forgotten and only achieving answering 43% of the requests. Also, 89% of these requests came from private individuals which suggests a growing concern for consumer privacy.

Stage 3: Companies using Software for GDPR Compliance in line with Digital Transformation

Companies in this stage utilize software for compliance, including a modern identity solution to automate repetitive workflows. By approaching parts of the GDPR like right of erasure and right of access requests as provisioning and deprovisioning problems, companies can use products like Lifecycle Management to ease IT administrator workloads. Functionalities are further extended by utilizing identity and access concepts like downstream app mastery and security policies to achieve compliance.

Stage 4: Companies that adopt a platform identity solution that adapts to dynamic data protection laws

GDPR Maturity Curve



From the European Union's GDPR, to the Privacy Act in Australia, and the CCPA in California, we are seeing a global wave of regulations. Privacy is increasingly becoming an explicit concern for IT organizations worldwide as they think about how to comply with a constant stream of privacy regulations. In addition, as larger enterprises become more globalized, companies should consider an adaptable and flexible identity solution for continued compliance to meet unique regulations in different locales. As illustrated in Figure 1, we see that customers around the world are subject to differing levels of regulation, with each country having their unique approach to privacy.

But more than using various tools to achieve a modern identity solution, transition to an identity platform is inevitable. The next step of managing compliance is having a single point of control necessary to govern system wide policies and workflows.

Part III:

Customer Identity & Compliance

By automating through a modern identity solution, organizations will be able to better manage their GDPR compliance obligations through having customer identity at the core. By approaching the GDPR as an identity-based problem, we can use a corresponding set of products that can help solve the problems posed by compliance. Let's look at the tools we can use and the corresponding requirements of the GDPR.

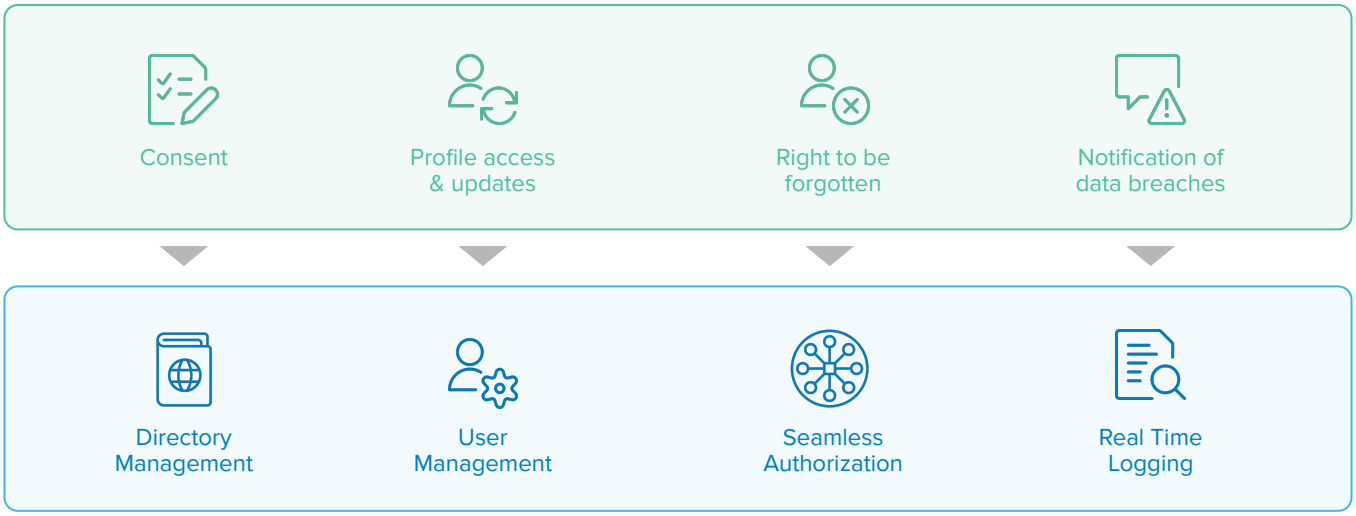


Figure 2

From Figure 2, we see that GDPR can be addressed with 4 products:

- Universal Directory – a centralized store of all users; can store profile and consent attributes.
- Lifecycle Management – automate downstream actions once a customer has acted.
- API Access Management – manage consent and scopes to downstream applications.
- Real time Logging – utilize a syslog to provide an audit trail for compliance.

Which map to four important GDPR requirements:

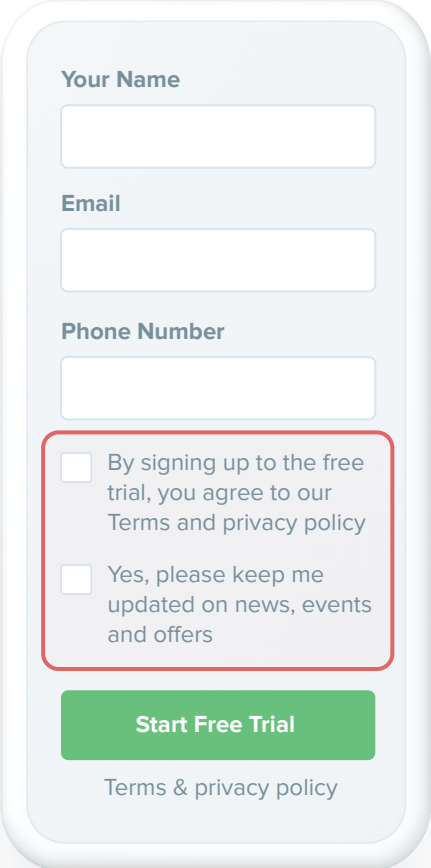
Consent	Articles 6 & 7 of the GDPR
Profile Access and Updates	Articles 15, 20 & 40 of the GDPR
Right to be Forgotten	Article 17 of the GDPR
Data Breach Notifications	Articles 33 & 34 of the GDPR

By dissecting each requirement and mapping product functionalities to compliance obligations, organizations can take the first steps to leveraging an identity solution to help fulfill their compliance needs. In the following sections, we will take a deeper look into specific articles of the GDPR and describe how to use Okta's suite of products to help manage compliance needs.

How Okta Can Be Leveraged for Managing Consent

Article 6 of the GDPR lays out the situations, or legal bases, that allow companies to process personal data. One legal basis to process personal data is consent for specific purposes. The specific conditions for valid consent are described in Article 7. A common scenario for which companies may need to collect consent is for the registration of a mobile calendar application. At Okta, we store consent as an attribute on Universal Directory. In the next section, we will go through a sample registration for a calendar application to show how Okta helps with consent management.

Calendar App Registration



Build user profile in UD with Attributes:

- Name
- Email
- Phone
- Terms of Service (Date)
- Terms of Service (Version)
- Email Updates (Date)
- Email Updates (Version)

Registration

In a calendar registration flow, a business is not only collecting attributes like name, email, and phone number, but also business requirements that are pushed to IT administrators. Those business requirements might define collecting consent for terms of service and email updates as shown to the left.

When an individual opts in to email updates, the form collects the given consent as an attribute from the individual to allow for email marketing and comply with data privacy regulation.

Storing Consent as an Attribute

Okta's universal directory can store all of these responses as attributes, including consent to terms of service as shown in Figure 3 (TOS).

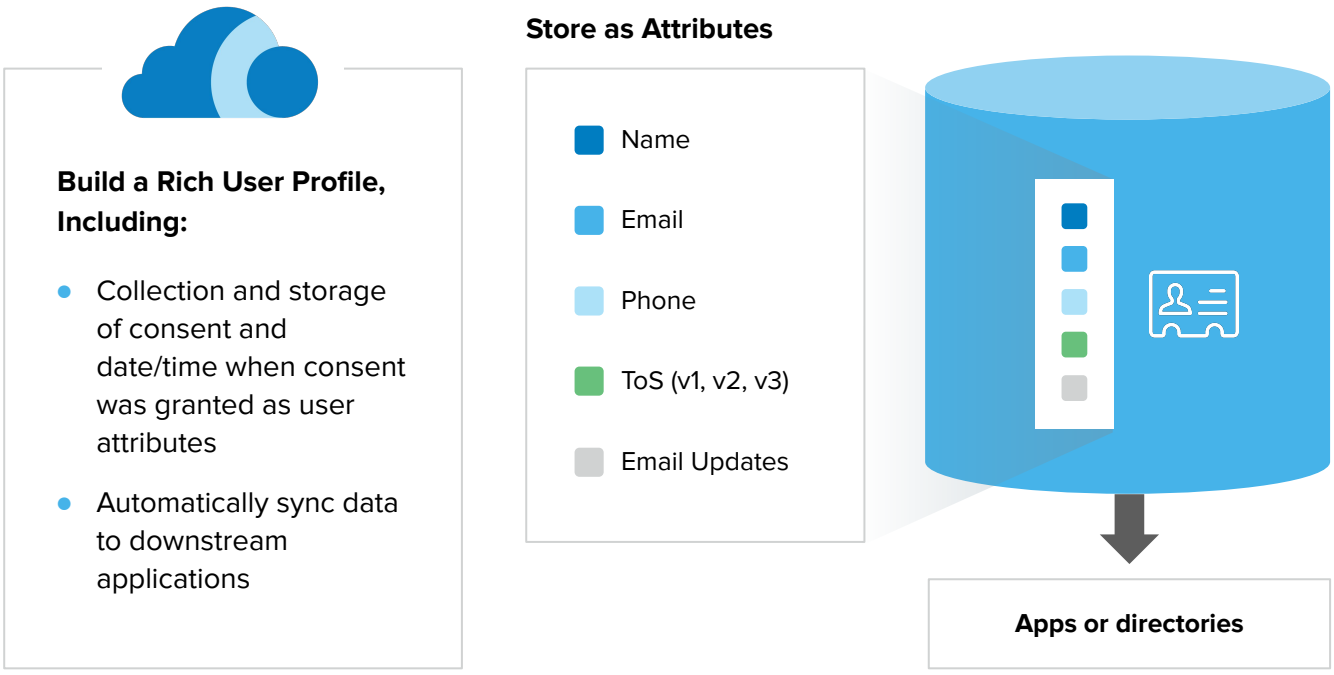


Figure 3

Optional Consent

If an individual did not want to receive marketing emails, but still wanted to use the application, you could also store that as an attribute. By using scoping to dictate which individuals get marketing, IT Administrator overhead is reduced by presenting an out of the box UI as shown in Figure 4.

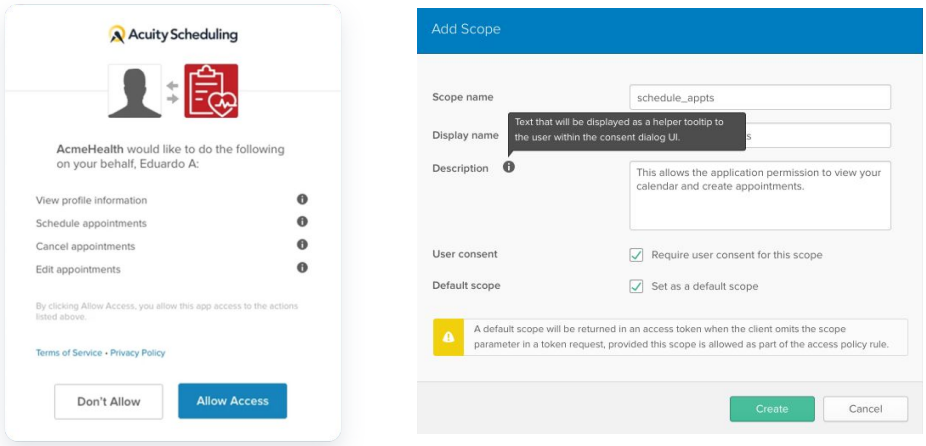


Figure 4

Downstream apps

Another example of collecting consent is the scenario of downstream applications, and collecting consent to share information.

For example, if a user wants to sync their Google Calendar to their custom calendar app, collecting consent is necessary to comply with the GDPR. In this case, consent for the calendar application being able to access Google Calendar is required from the user. Scopes that might be required would be your profile, and contacts that could be stored as attributes.

A functionality that API Access management offers is an out of the box UI for collecting consent or the option to customize your own UI through APIs shown in Figure 4. This makes the developer's life easier by providing an easy to use interface to present to the end user. As a point of clarification when sending a request to downstream applications, Okta can only help with automating the request downstream but cannot control the privacy practices or data uses by a downstream application.

Consent over Time

As mentioned before, consent can be stored as an attribute in Universal Directory and can automatically be updated if the use cases for consent change over time. Some example scenarios of this would be an update to a term of service, privacy policy, or marketing preferences. By storing a separate date attribute in conjunction to the consent attribute, IT administrators can review compliance with consent over periods of time, and different consent requirements.

A common example for distinct consent requirements could be in the form of disparate privacy policies across applications. For example, some web applications might collect cookie information, while other apps might collect personal data such as email. With all these disparate requirements, this means unique policy settings and differing types of consent.

How Okta Addresses Profile Access and Updates

The GDPR includes the rights of access (Article 15) and rectification (Article 16) for data subjects. The right of access allows individuals to have access to the personal data collected about them. The right to data portability allows an individual to request a company to share that personal data collected about them in a machine readable format so that they may transmit it to another company. Companies can address these two rights for individuals through an Okta platform-based solution (Universal Directory, SysLog API) which allows an individual to review and access profile information.

Creating a Consolidated Profile

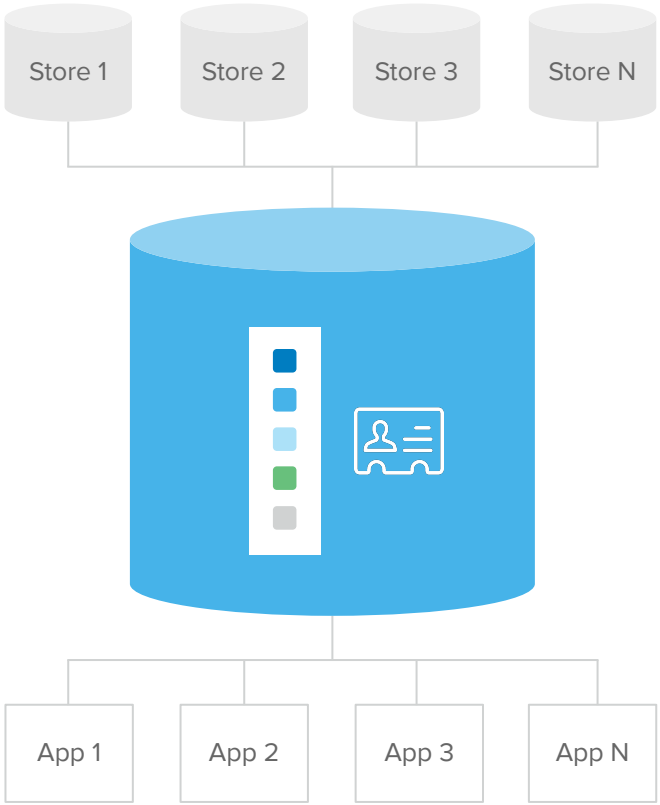
As described above for consent management, Okta's universal directory sits at the core of addressing profile access and updates.

Oftentimes individuals' data is scattered through disparate identity store silos, making it difficult to bubble up a single source of truth and accurately display what data is collected on an individual in the event of an access request by a data subject. This problem is solved through directory integrations which allow Okta to connect to various identity stores and present a single pane of glass showing individuals' information. Legacy directories such as AD and LDAP can also be integrated via an On-Prem-Provisioning agent which is integrated to Okta through HTTPS.

Give users control over personal data

Consolidate Customer Data for a Single Source Of Truth

- Admins or helpdesk can access and edit profile data in an intuitive UI
- Automatically sync updates to apps and directories
- Export data via CSV or API
- Audit trail showing who, how and when profile updates were made in Sys Log



Once all individual information is imported, Okta has specifically scoped access admin and helpdesk roles. If an individual chooses to exercise his or her rights of access, data portability, or rectification under the GDPR, the scoped roles allow an admin to access and export that data for the individual or change the profile information when requested by the individual. When utilizing this functionality with Okta's capability for Real Time Logging, companies can maintain an audit trail of the data access, changes, and export by the admin to share if needed in the event that a regulatory authority requests compliance records.

Let's take a look at an example for profile updates to downstream apps and making sure these changes are done through the Okta UI. We can see in image 2 that once a profile attribute is changed (first name) in the profile section, these changes are then pushed to an external application to reflect the change.

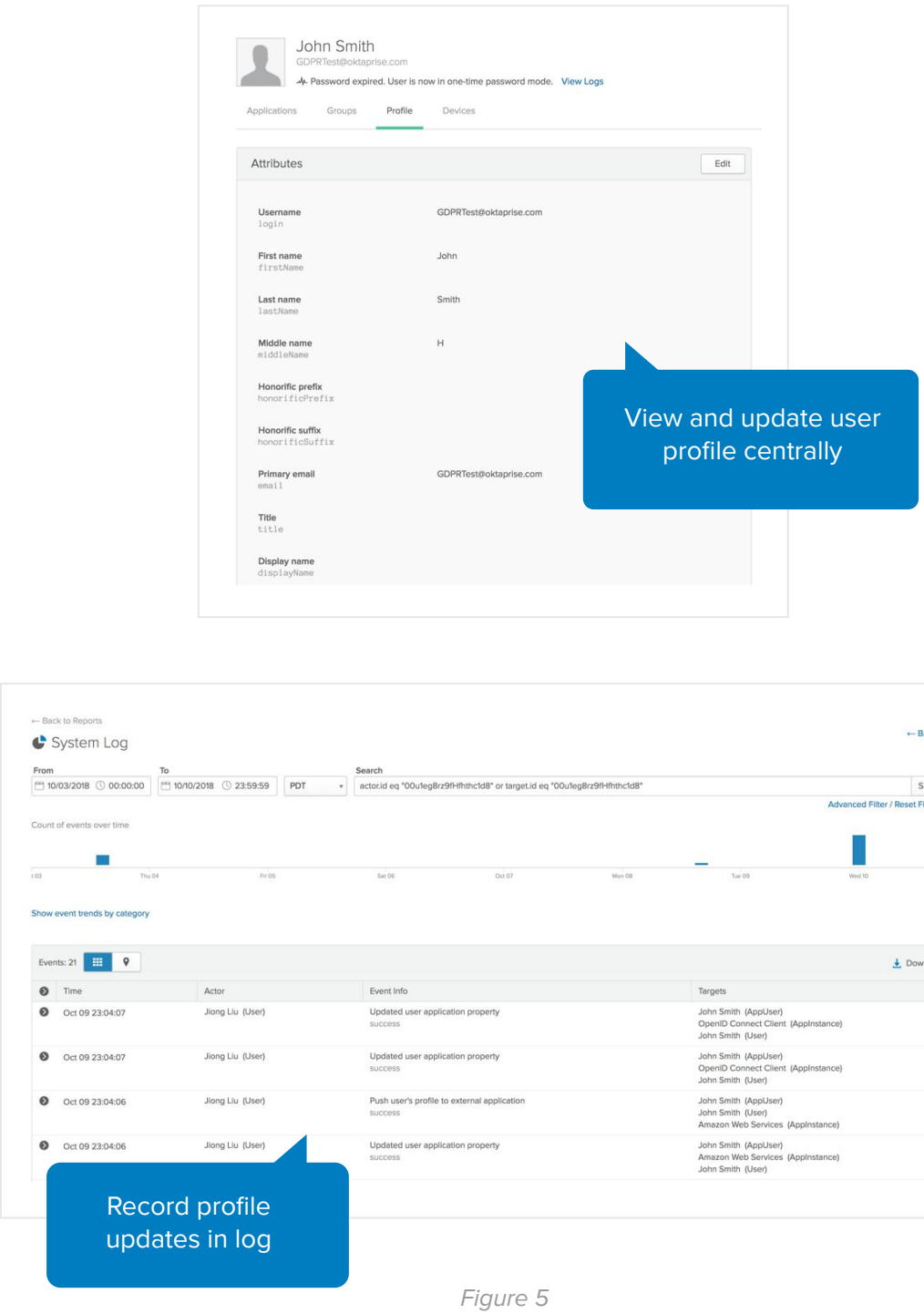


Figure 5

To aid companies with fulfilling data portability requirements, or the right to receive data collected on the individual in machine-readable format, Okta's user interface also has the functionality to download a CSV file which can then be passed to the individual. Developers can also build out a custom branded UI by calling Okta's APIs and delivering the data in an automated fashion, while maintaining the customer experience.

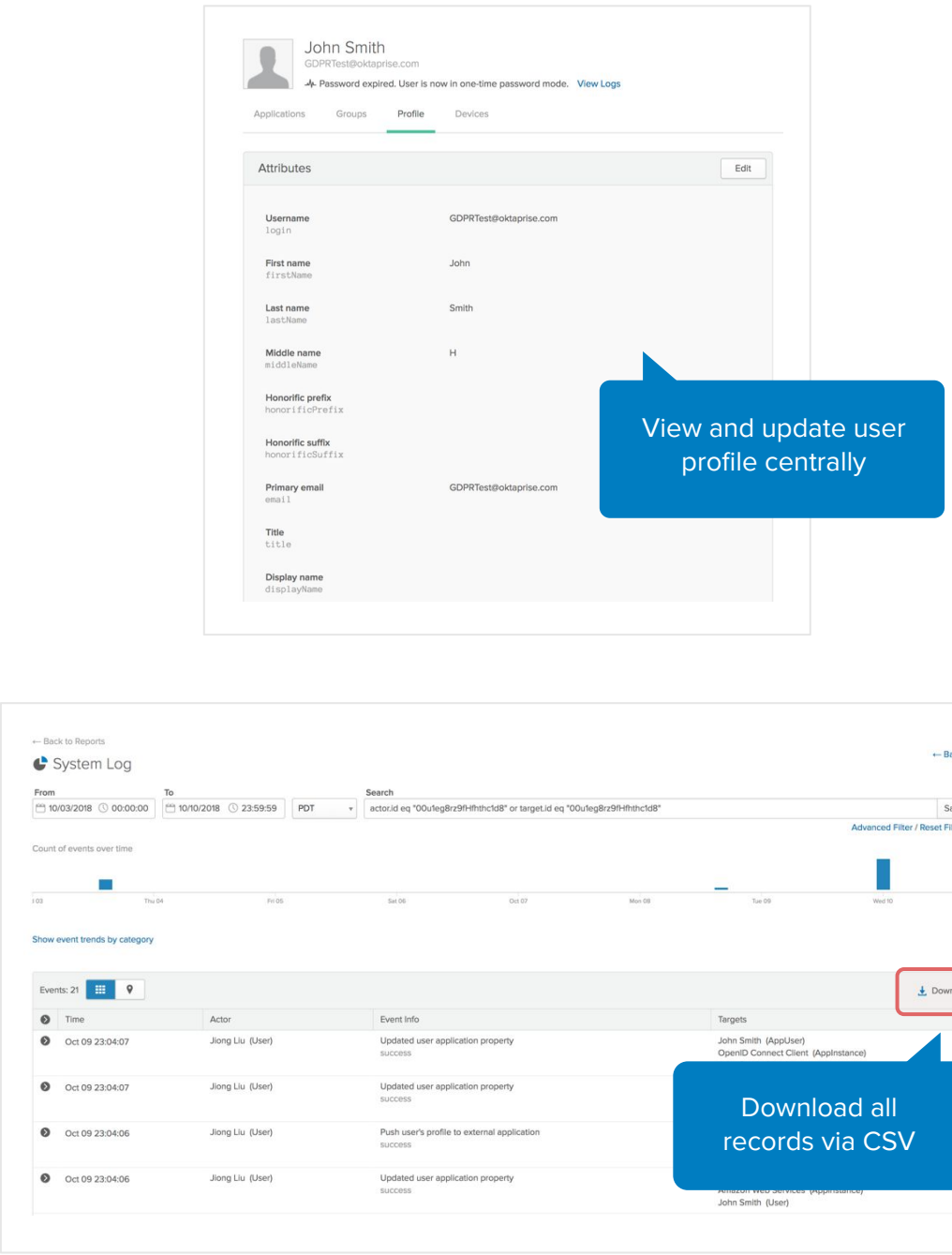
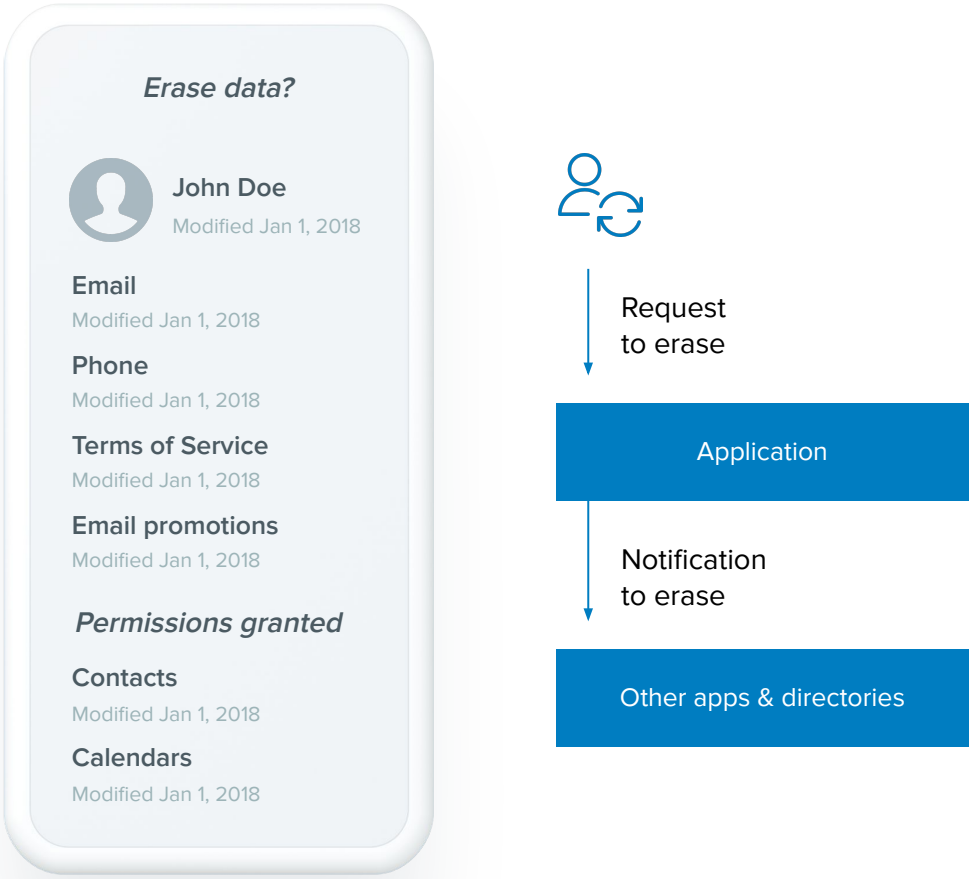


Figure 6

How Okta Manages for Right to be Forgotten (Erasure)

Article 17 of the GDPR outlines the right to the erasure of personal data by a data subject. This means that modern enterprises have a responsibility to delete personal data without undue delay upon receipt of an individual's request.



For IT Admins, this translates to a requirement to delete the personal information collected on an individual, which may include consent preferences, email marketing preferences, as well as profile information in addition to the requirement to make sure that any downstream applications and data stores that contain any personal information of the requesting individual also delete the personal information under the request.

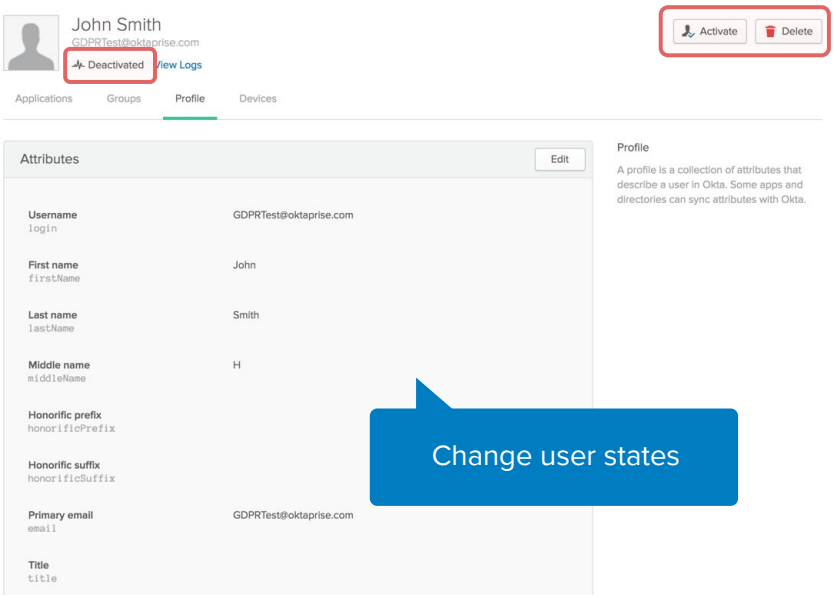
The product used to facilitate this process in this instance would be the Lifecycle Management tool which manages the provisioning and deprovisioning of user accounts from Okta. LCM has 3 lifecycle states: Suspend, deactivate/activate, and delete user states.

The powerful part comes into play by connecting to this tool via API and building an automated workflow to manage individuals who exercise their right to be forgotten. The deletion request can be pushed to downstream applications to help IT admins make sure that all identity store instances do not contain the said user's personal information. These requests are documented through the system log, allowing companies to maintain an audit trail of steps taken in furtherance of Compliance.

Automated deletion from a central location

Manage Requests With A Centralized Identity

- Suspent, deactivate/reactivate, and delete user states
- Automated worlows and self service capabilities available through API
- Auditable record trail



How Okta Helps With Notification of Data Breaches

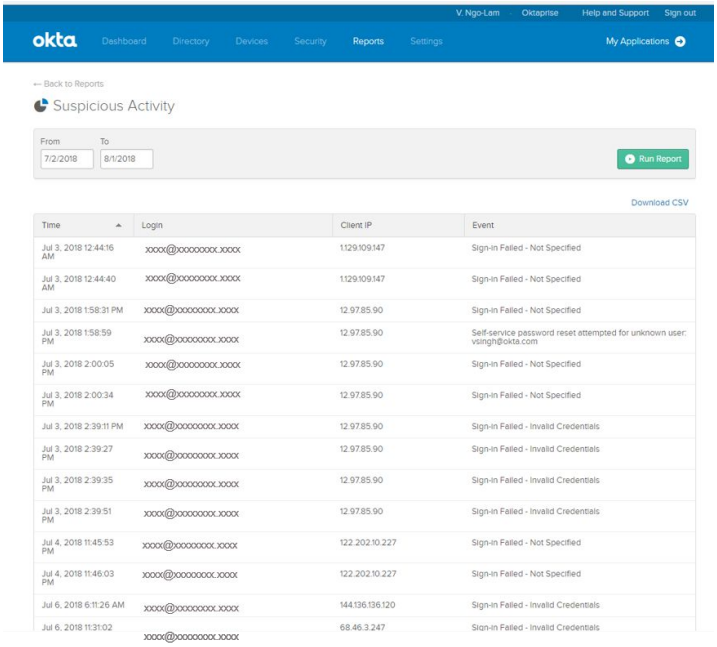
Articles 33 & 34 of the GDPR require companies that act as data controllers to notify a supervisory authority without undue delay, and when feasible, no later than 72 hours of becoming aware of a personal data breach. This notification must include the following information:

- Nature of personal data breach
- Consequences of personal data breach
- Measures to be taken to mitigate effects
- Contact details of Data Protection Officer

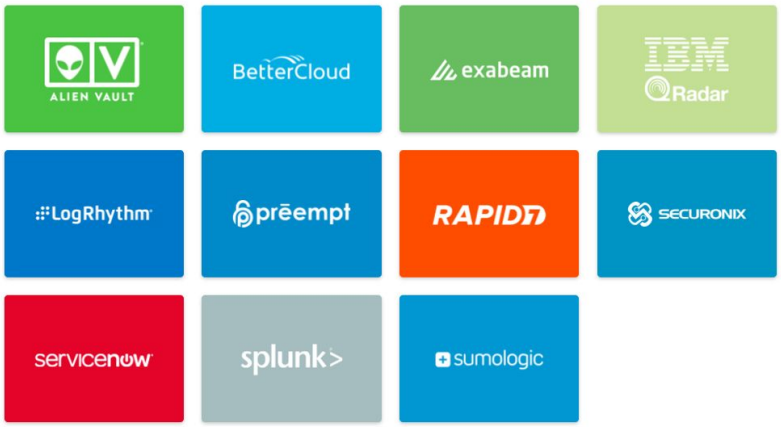
Breach report

- Identify what was breached
- Investigate causes
- Contain further damage

Okta can help incident response teams manage their data breach related obligations. By utilizing the System Log, incident response teams can review a detailed log of all login activities. Further, the Sys Log API provides developers with out of the box UIs/reports drawing from all apps (cloud, mobile, etc.), which in turn can be used by companies as part of an investigation of the data breach to provide some of the necessary details required by the GDPR, thereby minimizing manual processes and making IT admins happy.



If Okta is connected to all your apps, syslog can also surface who has access to applications, as well as the login attempts to those applications in the form of canned reports. One example of a report would be the suspicious activity report which highlights a suspicious user's login, IP, and time of activity. Reports like this provide an insight into the bad actors that could be potentially trying to infiltrate your IT infrastructure. For deeper use cases and a more holistic view of the account activity environment, Okta also has integrations with the largest SIEM providers. Services like Splunk and Rapid 7 can provide security analytics at a deeper level.



Integrations

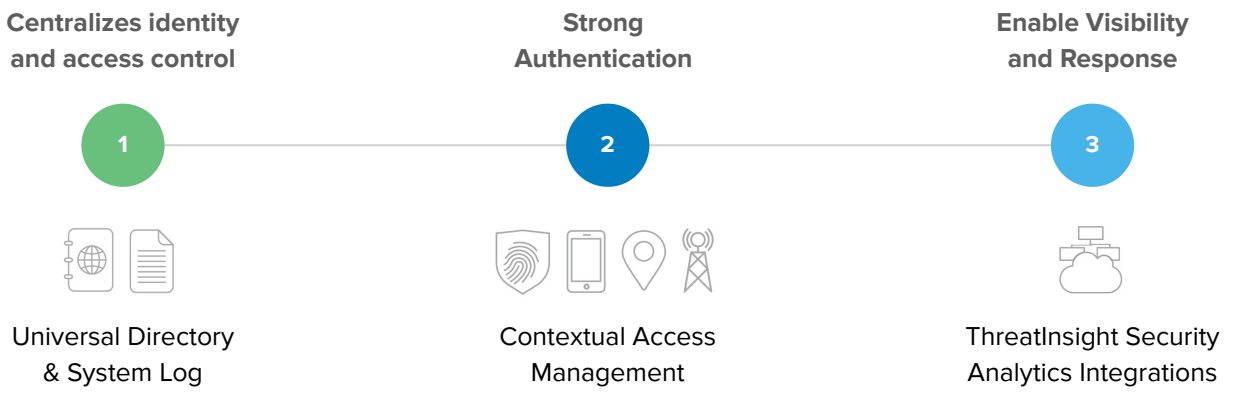
Part VI:

Proactively Prevent Data Breaches

While we at Okta understand that customers have obligations to notify the correct parties in the event of a data breach, it would be best if no data breach happened in the first place. This is where the broader suite of Okta products come into play, and where approaching security as an identity-centric problem is prudent.

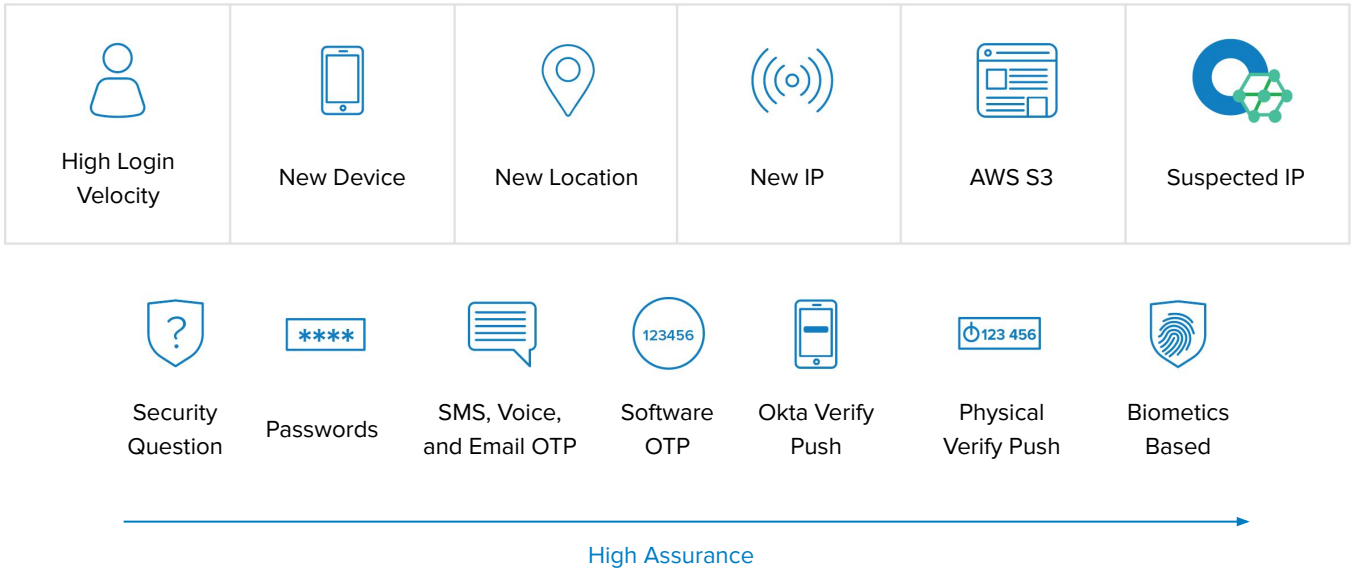
With the proliferation of IoT devices, the attack surface of enterprises has expanded to outside the simple firewall perimeter.

Okta's platform for identity-based security works in 3 ways:

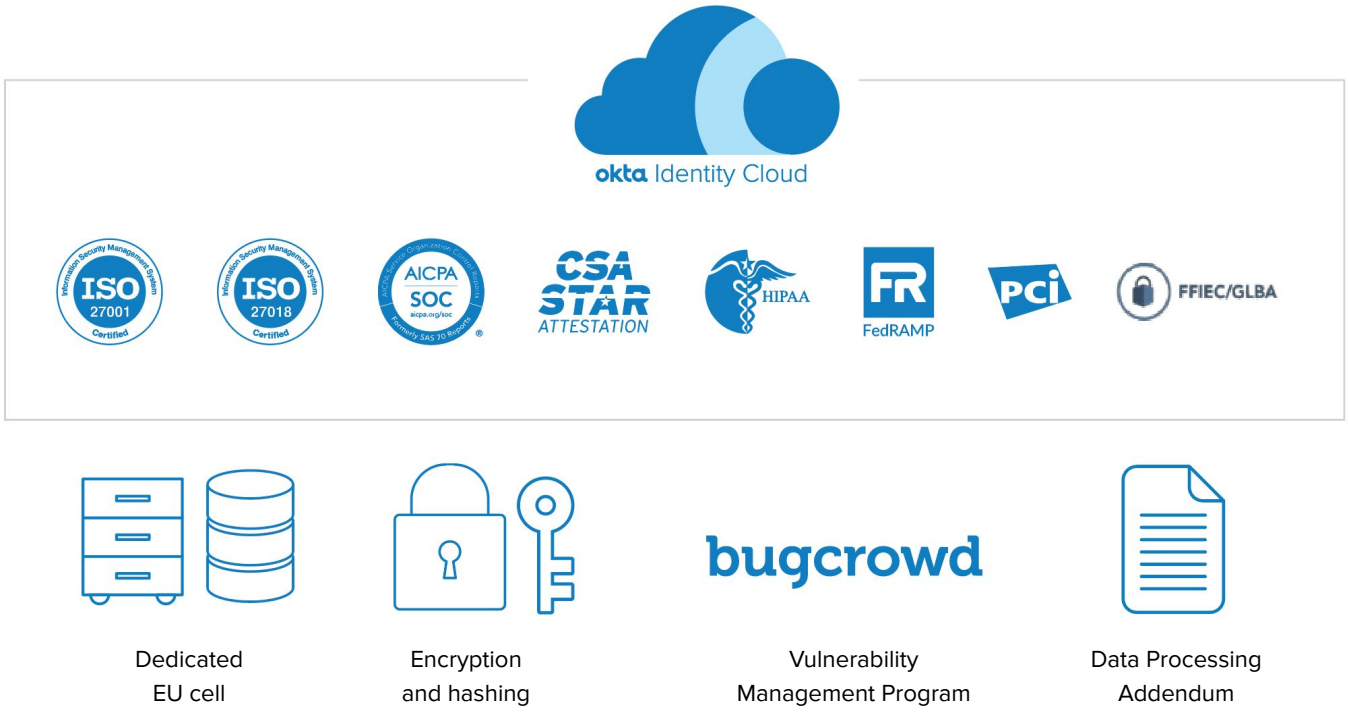


Centralizes identity and access control – By creating a source of truth and a window to the backend of account activity using Universal Directory and Syslog, identity & access can be controlled in a pre-built UI or be custom-built using Okta's API. This was shown earlier in Profile Access and Updates.

Strengthening authentication – SFA and 2FA are so last year - Modern security requires the use of contextual access management. With contextual access, these scenarios can be governed with customizable security policies that IT Administrators can easily implement through the Okta UI. By analyzing things like network characteristics, type of device, location, and biometrics details, our adaptive MFA product (AMFA) is the gold standard in achieving superior enterprise security while balancing usability.



Enable visibility and response – As the leading identity provider, customers can take identity-based security to the next level by incorporating curated intelligence from SIEM providers from the Okta Integration Network. With over 4300 customers and 5000 partners, Okta has a unique value proposition by providing a set of best practices in regard to suspicious access requests. When a request is seen as less than 100% certainty of user's identity, Okta feeds the authentication request to a Risk Scoring mechanism which can be used to dictate customer's access policies. Okta can further be configured to adapt for network zones and frequency of access for step-up MFA.



Part V:

Built with Privacy in Mind

The Okta Identity Cloud was built in the cloud and designed with security and privacy in mind. With numerous certifications across a gamut of industries and several external attestations, Okta has been proven to be the leading identity provider through.

Some other functionalities that Okta offer:

- Dedicated EU Cell for GDPR
- Encryption and hashing
- Vulnerability Management Program
- Data Processing Addendum

At the end of the day, Okta's approach to data privacy is to respect that customers own their own data. We only use data to provide our services and do not sell customer data and with the Okta Identity Cloud, and we take measures described in our Trust and Security Documentation to keep our customers' data safe and secure.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 6,100 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

www.okta.com