WHITE PAPER

Digital Identity Security Assurance:

How to Keep Your Customer Data Secure

Executive Summary

Digital identity and customer profile management are central to every company's digital transformation. Customer identities, and the personal data associated with them, are among the most critical and valuable assets of any organization. Securing these digital identities from registration to later stages of the customer relationship — and ensuring ongoing business value from the associated data — are crucial for business success.

In managing digital identities and building consumer trust, companies need to apply the highest security measures to protect themselves and their customers. In the worst-case scenario, customers could become victims of identity theft, with potentially significant impact on their financial, professional, and personal safety. All of which have the potential to lead not only to the loss of trust, but also to liability charges and class-action lawsuits against the business.

In addition, companies must implement strict identity privacy measures to comply with international privacy regulations, including the European Union's General Data Protection Regulation (GDPR),[1] the California Consumer Privacy Act (CCPA),[2] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA),[3] and other industry-specific regulations, such as privacy laws addressing the security of medical information.

This paper discusses:

- *The need to protect consumer identities with customer identity and access management (CIAM) and secure, robust infrastructure*
- *The need for advanced, flexible security functionality, such as scoped access*
- *The importance of edge network protection*
- *Growing international privacy regulations*
- *How to build consumer trust*
- *The advantages of cloud-based CIAM*

The paper concludes with a brief, real-world example of a leading global pharmaceutical company that deployed a secure, best-in-class CIAM solution to empower its healthcare providers amid data privacy regulations.

Secure Customer Identities

Digital customer identities are valuable assets. Businesses increasingly use identity data to personalize customer experiences based on preferences, behavior, and demographics. While collecting identity data to personalize experiences has benefited both businesses and consumers, it has also increased the risk of expensive, brand-damaging data breaches.

The 2019 Cost of a Data Breach Report, conducted by IBM Security and Ponemon Institute, found that 48% of the organizations represented identified the root cause of a data breach as a malicious or criminal attack, with an average cost of approximately $157 per breached identity record.[4] As personal information security breaches frequently involve hundreds of thousands — or even millions — of customer records, the resulting cost can severely harm a company. And that's before potential revenue loss from reputational damage and lost customer trust is calculated.

Taking and storing customer data — holding and processing customer credentials and personal information — is a duty of care that businesses and organizations cannot afford to breach or compromise. As an added mandate, governments have introduced legislation to protect customers' personally identifiable information (PII). The European Union's GDPR, California's CCPA, and Canada's PIPEDA are just a few of the many data privacy regulations being enacted globally.

For a global brand to adhere to the nuances of different regional data privacy regulations, it must implement a strategy that granularly collects, processes, and stores PII in accordance with the appropriate law, or choose to overhaul its data privacy strategy for global compliance.

Beyond protecting individual customer identities, the underlying IT infrastructure itself must be protected against threats, such as distributed denial-of-service (DDoS) attacks that could otherwise result in downtime, performance degradation, loss in consumer trust, and potential financial losses. Collection of certain customer data can actually aid in securing infrastructure. For example, the IP address used by a customer can be recorded and checked against a blacklist in order to prevent fraudulent activity. Many of the newer privacy regulations, such as GDPR, consider IP addresses to be personal information, but allow for collecting and processing such data as long as it only occurs for security purposes.

Protecting Customer Data

To protect customer data and maintain consumer trust, companies should start with a best-in-class CIAM solution to secure user data and credentials with strong encryption and scoped access control. Whether building a CIAM solution in-house or deploying a professional-grade commercial solution, organizations must ensure their identity management solution is able to:

- *Secure customer data with strong encryption of data in transit and at rest*

- *Provide scoped access control for both data and applications; access control should be possible down to the level of individual data record fields (as opposed to systems that only allow "nothing or everything"), and by role and/or attribute*
- *Protect customer accounts against abuse with strong user authentication methods, such as step-up and one-time password (OTP) authentication, and CAPTCHA challenge-response support*
- *Stop attack traffic before it can reach critical applications and cause outages, degrade performance, or drive up computing costs*
- *Adhere to security protection certifications and attestations, such as International Organization for Standardization (ISO) 27001:2013 and 27018:2014, Service Organization Control (SOC) 2 Type II, and Cloud Security Alliance (CSA) STAR Level 2*
- *Allow full compliance with different regional data privacy regulations, including GDPR, CCPA, PIPEDA, and numerous other industry-specific and healthcare regulations*

Scoped Access Control

To protect customer identity information, CIAM solutions should provide highly granular permission levels to ensure full control of which individuals and applications can access and manipulate information — all based on roles and responsibilities.

Fine-grained access control should be applied all the way down to data columns, rows, and fields. For example, it should be possible to define roles that allow developers to perform application administration tasks without allowing them to gain access to any customer data.

Furthermore, a CIAM solution should offer a set of predefined roles based on typical administrative duties that support the principle of least privilege — for example, roles specifically for customer service representatives that need to access customer data without further administrative permissions.

Such scoped access should be available for company employees and contractors, as well as the organization's sales and marketing applications. This capability can be very helpful in preventing the spread of toxic data. For example, if a user opts out of receiving email communication, a CIAM solution with scoped access can automatically block marketing automation systems and other facilities from accessing the email addresses of those individuals.

Protection at the Edge

An important component of digital identity security is edge network protection. Enterprise-grade CIAM solutions should protect registration endpoints against increasingly complex and sophisticated threats ranging from opportunistic and sophisticated breach attempts to DDoS attacks and malicious application programming interface (API) calls.

By having protection layers reside in and protect the identity endpoints at the network edge, malicious activities and bad actors can be detected and fended off before they (and the potentially massive attack traffic they cause) can reach the actual sites and applications.

To boost the performance of the identity experiences, enterprise solutions should also apply intelligent caching technology to ensure data and user experiences are held close to the end user.

Privacy Regulations and Trust

Closely associated with the concept of digital identity security is the concept of consumer privacy assurance. As discussed in the companion white paper "GDPR, CCPA, and Beyond: How Identity Governance Helps Companies Comply and Improve Customer Trust," growing privacy regulations such as GDPR and CCPA are being enacted across the globe at a rapid pace, fueled by well-publicized data breaches, ID theft, and related scandals.[5] In the U.S. alone, 10 states have introduced or passed bills imposing far-reaching business obligations to provide consumers with more transparency and better control over PII.[6]

Businesses cannot afford to ignore these new privacy laws and regulations. From a financial standpoint alone, moderate fines that were levied during the first 12 months of GDPR have now given way to much larger fines. The recent fine of $123 million against a global hospitality company due to the hacking of the personal information of 380 million hotel guests is a prime example.[7] And these fines are destined to increase in size – up to the staggering GDPR statutory cap of 4% of the annual global turnover.

But the cost to global businesses is much more than financial. At risk is consumer trust. Businesses today need explicit consent in order to process personal data. And consent requires trust. Without trust, there is no consent. Without consent, there is no data. And that results in ineffective sales and marketing campaigns.

Honoring security and privacy is not just a compliance question, but also a core business advantage. Security, privacy, and identity governance help businesses form deep relationships with users and customers, resulting in higher loyalty and the potential for higher business revenue.

The Requirement for State-of-the-Art CIAM

According to GDPR and other privacy legislations, organizations that process personal data must secure the data against unauthorized access. Being able to demonstrate that "appropriate" and "state-of-the-art" security measures are effectively protecting the data is essential under GDPR.

But what is an "appropriate security measure," and what required evidence is expected? According to GDPR, appropriate security measures are those that take into account the "state of the art," the cost

of implementation, and the scope, context, and purposes of processing — and balance these against the risks and impacts to the rights and freedoms of individuals. So an organization needs to determine what is appropriate or in balance, and will therefore have to refer to industry best practice as a guide.

One tool to determine the right balance is the data protection impact assessment (DPIA),[8] a process required in some cases under GDPR to determine the potential impact of data processing operations. When conducting a DPIA, an organization must document in detail a number of factors, including:

- *Envisioned data processing operations*
- *The necessity and proportionality of these operations*
- *An assessment of the risks of data breach associated with the operations*
- *The measures envisioned to address these risks, including safeguards and security measures, and mechanisms to ensure the protection of personal data*

GDPR and other regulations mandate a risk-based approach to data protection. Data security obligations are not stated in a vacuum, but rather are to be developed on the basis of a thorough analysis and understanding of the risks that each processing operation may have for the data subjects.

While this approach offers the flexibility for organizations to apply reasonable measures in light of costs, system architecture, and related factors, it still requires a rigorous cost-benefit/risk review of everything the organization does with personal data.

How successfully an organization can provide sufficient evidence of effective risk mitigation will depend on its understanding of the relevant privacy risks as well as the strengths of the "state-of-the-art" data management and security measures it chooses to implement in response to perceived risks.

The Advantages of the Cloud

To implement the digital identity security concepts, processes, and technologies discussed in this paper, companies have two basic choices: developing in-house or buying an enterprise-grade solution from a vendor specializing in CIAM.

As analyzed extensively in the white paper "Build vs. Buy: A Guide for Customer Identity and Access Management," cloud-based, commercial, off-the-shelf solutions are usually a better choice for most companies' goals, needs, and resources.[9] This is particularly the case for the initial implementation, as well as the level of effort it takes to operate and maintain a solution in the long

From ongoing R&D to guaranteed SLAs, commercial CIAM solutions have several significant advantages over in-house IT departments. Cloud solutions add elastic scale, multi-region failover and disaster recovery, plus security levels in-house teams would be hard-pressed to match.

term with continuously changing requirements dictated by technology, consumers, markets, and regulators. In particular, the state-of-the-art clauses of regulatory legislation such as GDPR are best met by professional-grade, third-party solutions.

Commercial CIAM solutions have several significant advantages over in-house IT departments that attempt to build their own. From global availability and scale to guaranteed service-level agreements (SLAs) to security certifications, commercial CIAM solutions have the competency, resources, and ongoing research and development that come with third-party vendors, which means that internal IT teams can focus efforts on other key business initiatives.

CIAM solutions that are architected to utilize the capabilities of a modern cloud to share resources, provide elastic scale, ensure security, and enable multi-region failover and disaster recovery offer identity-as-a-service (IDaaS) capabilities with a wealth of features — and at security levels that are frequently hard to match with in-house developments. At the same time, they eliminate the need to own and operate data center facilities and hardware.

While do-it-yourself identity management might seem doable, there is substantial risk of underestimating effort, underfunding, and a lack of long-term internal resources and expertise to support, maintain, and evolve the solution to meet changing market requirements and consumer expectations.

Commercial CIAM vendors are in a better position to keep up with changes dictated by technology, consumers, markets, and regulators, simply because solution vendors need to evolve their services to keep their offerings competitive, relevant, and in compliance. As they develop their solutions not just for one but for many clients, they can realize economy-of-scale benefits that are simply not available when developing in-house solutions.

Global Pharmaceutical Company Deploys Secure Identity Management Solution to Empower Healthcare Providers

The Challenge

A leading global pharmaceutical company collaborates with healthcare professionals (HCPs), governments, and local communities to support and expand access to reliable, affordable health care around the world. However, multiple compliance regulations for promoting products and services to HCPs affected the company's goals to bring therapies to market quickly. The company needed an identity management solution that would give HCPs secure and seamless access to its professional website to take advantage of prescription drug promotions, while remaining in compliance with country-specific regulations. To meet these needs, the company required an enterprise-grade, state-of-the-art CIAM solution.

The Solution

The company selected Akamai Identity Cloud to provide secure and fully branded account registration for its professional website with login workflows, single sign-on, authentication, password management, account creation flows, field validation, and more. Profile management features enable easy editing of profile information, while profile data storage automatically collects and stores HCP data in a secure, flexible, unified cloud database.

The Identity Cloud platform is nine times faster than the company's previous solution. It grants HCPs across the globe secure and equal access to regulated medical resources, while meeting geographically diverse security and compliance standards. HCPs can now obtain drug samples in days rather than weeks through the secure website, thereby improving patient care and enhancing quality of life for patients. Company representatives now experience productivity gains, with fewer required visits to HCP offices to deliver drug samples and other resources.

Additionally, Identity Cloud's integrations with existing marketing technology platforms enable the pharmaceutical company to personalize its marketing efforts to HCPs worldwide.

Akamai Identity Cloud

Identity Cloud is Akamai's solution for CIAM. The platform provides everything companies need to empower their customers to create personal accounts and securely log in to websites, mobile apps, or IoT-based applications. Identity Cloud provides tools that can be used to significantly reduce privacy compliance efforts, while still providing companies with a highly secure customer profile repository and enabling a 360-degree view of the customer.

Identity Cloud offers specific capabilities and user experiences that can help companies address security and regulatory requirements. Identity Cloud privacy and protection features include client registration, login, authentication, single sign-on, scoped access control, preference and consent management, and numerous other capabilities needed to collect, manage, and secure personal data.

By deploying Identity Cloud, businesses and organizations can implement enterprise-grade identity management in a fast, flexible way. Engineered with a cloud-native architecture, the solution intelligently scales with application capacity needs to accommodate spikes in traffic and deliver scalability to hundreds of millions of users, as well as the security, performance, and availability to satisfy business-critical applications. Akamai Identity Cloud is designed to help organizations comply with international security and privacy regulations, build trust in their brand, manage client data, and mitigate risks by making the data securely available across all regions and applications.

Conclusion

Beyond expanding data privacy regulations, customer identity security and privacy are crucial for organizations that want to build deep and trusted digital relationships with their customers. Consumers have increasingly high expectations that their personal data should be kept private and secure. The many publicized cases of data abuse, breaches, and identity theft have massively raised the bar for enterprises to be considered trustworthy keepers of personal data. When customers store data with an organization, they are entering into a trust contract. If that trust is breached, it tends to be very difficult to restore.

SOURCES

1) European Union Data Protection Rules, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2) California Legislative Information: AB-375 Privacy, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
3) The Personal Information Protection and Electronic Documents Act (PIPEDA), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
4) IBM 2019 Cost of a Data Breach Report, https://www.ibm.com/security/data-breach
5) Akamai white paper: GDPR, CCPA, and Beyond: How Identity Governance Helps Companies Comply and Improve Customer Trust, <insert white paper link>
6) Davis Wright Tremaine: "Copycat CCPA" Bills Introduced in States Across Country, https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) ZDNet: Marriott Faces $123 Million GDPR Fine in the UK for Last Year's Data Breach, https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
8) Data Protection Impact Assessment (DPIA): How to Conduct a Data Protection Impact Assessment, https://gdpr.eu/data-protection-impact-assessment-template/
9) Akamai white paper: Build vs. Buy: A Guide for Customer Identity and Access Management, https://www.akamai.com/us/en/multimedia/documents/white-paper/build-vs-buy-a-guide-for-customer-identity-and-access-management.pdf

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 11/19.