SPOTLIGHT

Sponsored by: Anjuna

With confidential computing, workloads are isolated and wrapped in additional security controls to ensure that the organization can manage which users or systems may access or modify application data code. The concept offers tremendous promise for data security and privacy.

Secure Innovation Requires Confidential Computing

July 2022

Written by: Jennifer Glenn, Research Director, Information Security

Digital Transformation Requires Data Protection at the Application Foundation

Privacy regulations and highly publicized data breaches have opened consumers' eyes to the significance (and value) of personal data. In this digital world, data is no longer just a technical word used to describe bits and bytes. Data is the digital version of what delineates us as humans, including health issues, financial status, and family situations. It's information about what we value, including purchase history, subscriptions, and political and/or religious affiliation. Having this data breached feels like a personal violation.

AT A GLANCE

WHAT'S IMPORTANT

Confidential computing is a significant leap forward in ensuring data security and privacy. Making confidential computing a simple and frictionless process for application developers is critical for advancing data protection throughout the business.

This level of awareness among consumers is forcing businesses to reimagine their digital experiences with a focus on building and maintaining trust. In fact, in IDC's *Future of Trust Survey* from February 2021, 36% of respondents cited securing personal data as a top driver for improving the practice of trust.

At the same time, rich customer experiences and engagement are a key pillar for creating a trusted brand. Businesses invest heavily in development teams and tools that pull data internally from multiple company sources and externally from partners to create integrated application and service experiences for their customers.

Trends in Application Development Drive Security Changes

The move to cloud infrastructure was a tremendous leap forward for creating these digital customer experiences. Data can be used in more places, and application development in the cloud offers continuous opportunity for improvement and innovation. However, as more applications and workloads move to the cloud, data security takes on new importance. What was once within the control of the organization and its employees is now housed in/hosted on an infrastructure owned and maintained (including security controls) by someone else. This presents a risk to the organization and the trust of its users as anyone with administrative access to the cloud infrastructure — including an attacker or a malicious insider — can access the applications, code, and data that sit on top. One of the ways the industry has sought to close this security gap is with confidential computing.

Protecting data by isolating it is not a new concept. Commercial credit card companies required protection for chip and pin information starting in 2015. Mobile providers also soon adopted this capability to ensure biometric log-in information could not be used by anyone other than the authorized user. The past two years have seen every major infrastructure vendor demonstrate/announce support for confidential computing capabilities.

IDC defines confidential computing as a process for protecting data in use with controls implemented at the hardware level of the infrastructure. This approach offers a high degree of technical assurance for security, privacy, and regulatory compliance in the cloud or any other collaborative infrastructure environment. With confidential computing, workloads are isolated and wrapped in additional security controls to ensure that the organization can manage which users or systems may access or modify application data code. Some of the tools used to provide this assurance are as follows:

- **Trusted execution environment (TEE):** A TEE is an isolated runtime environment within the infrastructure that uses hardware controls that require data confidentiality, data integrity, and code integrity. This means the environment must be protected from unauthorized access and modification of in-use applications and data, thereby increasing assurances that they remain secure.
- **Enclave:** While the term enclave is often used interchangeably with TEE, they are slightly different. An enclave is a security feature of the processor within TEE. It creates an enforceable barrier to prevent unauthorized users from gaining access to the memory, application code, or data. It allows IT professionals to do the jobs they need to do while still providing assurance that data is secure.

During digital transformation, it is essential for organizations to have confidence in the security of their cloud infrastructure. While cloud infrastructures provide a solid foundation for launching and delivering new services that drive customer engagement, organizations are responsible for ensuring that all data used in this experience is handled with integrity and with the proper security controls. This requires collaboration and balance between two of an organization's most influential departments: the development teams that create the products and services that bring in revenue and the security team that protects the interests (and assets) of the business. Some of the projects that these teams must execute together are as follows:

- **Securing workload migration to the cloud:** Regardless of where an application is built, organizations want to ensure that it is running in a secure, confidential environment. Moving existing applications to a secure, confidential computing client infrastructure requires rewriting the code, which requires extra time and possibly specialized developer resources (staff). This impacts the reliability aspect of trust in two ways. There is now an opportunity for new errors to creep into the application code and affect its performance. New vulnerabilities for compromise may also be introduced.
- **Protecting sensitive data:** Data is the building block for all applications. It must be portable and available to its fullest potential for use in multiple applications on various infrastructures. While data needs to be secure in each of these uses, security technologies often introduce time delays and extra barriers to get at the data. Enclaves make it possible to use data in real time while still preserving security and integrity.

- **Stopping insider threats:** In IDC's December 2020 *EDR and XDR Survey*, security professionals reported that the type of end-user error or oversight, such as "opened a document from an untrusted source" or "clicked on a link from an untrusted source," was a contributor in a quarter of security breaches. In that same survey, respondents reported that compromised credentials contributed to slightly fewer breaches than well-meaning mistakes (24%), but not much less. Regardless of how insider threats happen, the outcome is the same: Data may be viewed or compromised, putting the entire business at risk for privacy violations or worse. In both cases, it is important for organizations to make sure that data is secured against unauthorized access, whether it is in use with an application, stored, or in transit.

Benefits of Simplifying Secure Development Practices with Confidential Computing

Cybersecurity tools and practices are often seen as the responsibility of the security team. However, data security — as a pillar of customer trust — is an executive-level concern, which means it should be everyone's responsibility. Infusing data security into development practices in a way that is fast, frictionless, and easy has a number of positive impacts across the business, such as:

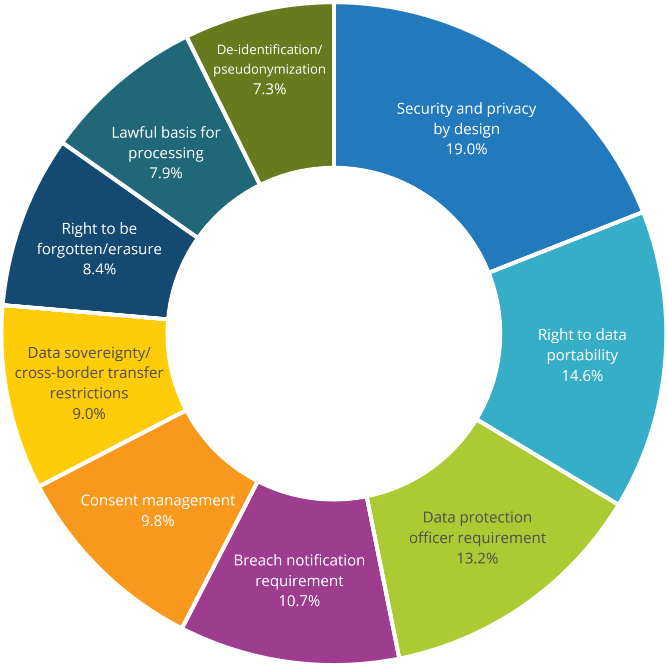
- **Adhering more easily to privacy and compliance guidelines:** Compliance and privacy regulations impact every department within an organization, from marketing to product development to everyday operations. They are also one of the biggest challenges to establishing trust. In IDC's *Future of Trust Survey* from February 2021, 28% of respondents cited complex regulatory requirements as one of the greatest challenges to establishing trust — second only to increasingly sophisticated cybersecurity attacks, which was cited by 31% of respondents. Regulations such as GDPR and CCPA are very clear about what organizations as a whole can and can't do with data. Without hardware-defined protections for data use in applications across the company, it can be difficult to meet these obligations. Confidential computing software that provides assured data protection makes it possible to enforce guidelines without needing to invest extra resources or take too much time.

- **Delivering innovative products and services faster:** Trust is more than just keeping data secure; it's also about delivering relevant, innovative applications to consumers. However, infusing security into the development process is often met with disdain because of the additional processes and time it takes as well as how it can disrupt the CI/CD process. In IDC's 2021 *Future of Trust Survey*, respondents were asked to rank their top 3 pain points caused by data privacy regulations: 44% of respondents indicated that security and privacy by design is one of their biggest pain points, with 19% of respondents highlighting it as their primary pain point (see Figure 1). By making confidential computing a part of the environment versus a part of the code, organizations can secure more applications in less time.

- **Demonstrating zero trust:** In May 2021, U.S. President Joe Biden issued an executive order that highlighted the need for zero trust security to help protect critical information from compromise. The order primarily targeted government agencies and the organizations that serve them, but many private enterprises are adopting zero trust strategies. Zero trust is all about layering security in the right way to ensure that data is accessed appropriately — under the right conditions by the right people. With confidential computing, a hardware root of trust is built into the environment, enabling zero trust protocols to be implemented simply and quickly.

FIGURE 1: ***Primary Pain Points Caused by Data Privacy Regulations***

Security and Privacy by Design Is a Significant Challenge



n = 507

Note: Percentages do not total 100% due to rounding.

Source: IDC's Future of Trust Survey, February 2021

Considering Anjuna Security

Anjuna Security is a Palo Alto, California-based company that offers a solution designed to enable organizations to run workloads securely. Anjuna Confidential Computing software operates transparently as an infrastructure software layer within the customer's public hosted cloud infrastructure. The solution automates an isolated, encrypted, and inaccessible hardware environment; even privileged users on operating systems can't access an organization's data or applications. This secure enclave is a TEE: Security is wrapped around the software and data and thus goes where the data goes, protecting data in memory, in use, and in motion.

Anjuna Confidential Computing software makes the public cloud secure by completely isolating existing data and workloads from insiders, bad actors, and malicious code. Its software deploys out of the box in seconds over AWS, Azure, and other public clouds. By employing secure enclave data protection, Anjuna effectively replaces complex legacy perimeter security without disrupting operations, applications, or IT.

Major cloud vendors have deployed these technologies, providing:

- Built-in high-speed hardware-grade encryption
- Hardware roots of trust

- Physical data isolation
- Key management

Anjuna's software combines, orchestrates, and abstracts these technologies to provide a secure, isolated, and virtually unbreachable environment around workloads and data. This isolation extends to data as it is processed, stored, and moved across cloud environments.

Anjuna Confidential Computing software requires no re-architecting of applications or kernel, and customers needn't concern themselves about the underlying TEE on the chip or cloud infrastructure level.

Challenges

While some vendors have been talking about confidential computing, it is still a relatively new concept. This means it is subject to abstract and conflicting definitions about what it means and who is responsible for making it a reality. IDC has stated that enabling confidential computing for applications in a cloud environment offers a variety of benefits for an organization. However, if the benefits are not substantial for any one group, there can be a lack of incentive to push confidential computing within the organization.

Conclusion

While every major infrastructure vendor has announced support for confidential computing, the concept is still gaining traction with the developer community. As the concept matures — and the organizations that will benefit from this approach also mature — it offers a tremendous amount of promise for data security and privacy. The challenges presented in this document may become moot when privacy concerns become a business driver.

Data security that is infused into the development cycle at the beginning offers several benefits to an organization's pursuit of trust.

About the Analyst

***Jennifer Glenn,** Research Director*

Jennifer Glenn is Research Director for the IDC Security and Trust Group and is responsible for the information and data security practice. Ms. Glenn's core coverage includes a broad range of technologies such as messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

Anjuna Security makes the public cloud secure for business. Confidential Computing software from Anjuna Security effortlessly enables enterprises to safely run even their most sensitive workloads in the public cloud. Unlike complex perimeter security solutions easily breached by insiders and malicious code, Anjuna leverages the strongest hardware-based secure computing technologies available to make the public cloud the safest computing resource available anywhere. Anjuna is based in Palo Alto, California.

To learn more, go to anjuna.io or experience a demo.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.