LEARNING MADE EASY

Anjuna Security Special Edition

Secure Enclaves

for dummies®
A Wiley Brand

Make data secure by default

Migrate safely to the cloud

Eliminate risk of insider breaches

Compliments of

anjuna

Ayal Yogev

Yan Michalevsky

Secure Enclaves

Secure Enclaves

Anjuna Security Special Edition

by Ayal Yogev and Yan Michalevsky

for dummies®
A Wiley Brand

Secure Enclaves For Dummies®, Anjuna Security Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-76759-6 (pbk); 978-1-119-76760-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz or visit www.wiley.com/go/custompub. For details on licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Contributing Writers: Jeff T. Parker, Linda Popky

Project Manager: Martin V. Minner

Acquisitions Editor: Ashley Coffey

Senior Managing Editor: Rev Mengle

Business Development Representative: Matt Cox

Production Editor: Mohammed Zafar Ali

Special Thanks: Michael Cartsonis

Table of Contents

INTRODUCTION 1
About This Book 1
Icons Used in This Book 2

CHAPTER 1: **Understanding the Fundamental Flaw in Computing** 3
Understanding the Fundamental Data Security Flaw 4
Recognizing the Impact on the Enterprise 5
Overexposing Data to Insiders 5
Recognizing Security Tool Fatigue 6
Avoiding the Cloud 6
Limiting Global Reach 7
Creating Data Insecurity for the CISO 7

CHAPTER 2: **Introducing Secure Enclave Technologies** 9
Defining Secure Enclave Technologies 9
Understanding Barriers to Enclave Technology Adoption 11
Discovering Broad Industry Support And Cooperation 12
CPU manufacturers 12
Cloud service providers (CSPs) 12
Confidential Computing Consortium 13

CHAPTER 3: **Looking at Enclave Benefits for the Enterprise** 15
Virtually Eliminating Risk of Data Breach 15
Securing All Data and Applications by Default 16
Protecting Data Everywhere It's Used 16
Isolating Insiders From Data 17
Simplifying Data And Operational Compliance 17
Assuring Customer Data Privacy 18
Establishing Zero Trust Infrastructure 18
Mitigating Vulnerabilities En Masse 19
Eliminating Costly Security Software Layers 19

CHAPTER 4: **Making Secure Enclaves Real for the Enterprise** 21
Putting Enclave Technology to Work for the Enterprise 21
Introducing Secure Enterprise Enclaves 22

Building a Secure Enclave Solution for Enterprises 22
Adoption should be as simple as "lift and shift" 23
Enclave protection should extend full stack 23
Support should be platform and cloud agnostic 24
Enterprise-class management 24
Integrating with the enterprise IT ecosystem 24
Easily Deploying Data Security by Default 25

CHAPTER 5: **Going Where No Enclave Has Gone Before: The Enterprise** 27
Migrating to the Cloud with Confidence 27
Executing Workloads Safely Anywhere 28
Securing databases 28
Implementing infrastructure micro-segmentation 29
Streamlining and Securing Key Management 29
Protecting Deployed Intellectual Property 30
Opening up New Possibilities With Secure Data Everywhere 30
Multi-Party Analytics 31
Personal Data Privacy 31

CHAPTER 6: **Ten Questions About Secure Enterprise Enclaves** 33
What Is a Secure Enterprise Enclave? 33
Why Should I Consider Secure Enclaves Now? 34
How Safe Are Secure Enclaves — Really? 34
How Difficult Are Secure Enterprise Enclaves to Implement? 35
How Do Secure Enclaves Work in the Cloud? 35
How Will My Organization Be Affected by Implementing Secure Enclaves? 35
What Is the Performance Impact on Applications That Run in a Secure Enclave? 36
What New Opportunities Might Be Available With Secure Enclaves? 36
What Benefits Will My Organization See by Implementing Secure Enclaves? 37
How Will This Affect My Developer Operations and Software Development Processes? 37
Bonus Question: What Should I Do Now to Get the Process Started? 38

GLOSSARY 39

Introduction

Keeping data secure is the ultimate goal of all enterprise cybersecurity efforts. Yet data insecurity remains at the heart of the many data breaches that continue to plague businesses and IT organizations.

Why should it be that so many resources are spent protecting data, while the data itself remains vulnerable and insecure?

Because today, thanks to a fundamental flaw in computing, data can't ever be really secured. As a result, access to a system — whether physical or remote — can also result in unimpeded access to data, even if the data is encrypted.

What if there was a way to secure data — including customer data and applications — by default, from creation to disposal? What if you could control all access anywhere data lives? What net new opportunities might arise in your organization if data security and privacy simply became part of IT infrastructure?

This book examines these questions through the lens of *secure enclave technology.* Don't feel bad if it's your first time hearing about it. You aren't alone. We often say this may be the best kept secret in the world of enterprise cybersecurity.

This book sets out to change that.

About This Book

This book introduces and explains secure enclave technology, a data security technology now present in modern CPUs and clouds from Amazon AWS, AMD, Intel, Microsoft Azure, and many others. The book then helps you plan a path to take full advantage of this powerful capability, which promises to simplify IT and security.

It's time you took a few minutes to read up on the implications of secure enclave technology, which can virtually eliminate data insecurity. Here's an overview of what this book covers:

» **Chapter 1:** "Understanding the Fundamental Flaw in Computing"

- **Chapter 2:** "Introducing Secure Enclave Technologies"
- **Chapter 3:** "Looking at Enclave Benefits for the Enterprise"
- **Chapter 4:** "Making Secure Enclaves Real for the Enterprise"
- **Chapter 5:** "Going Where No Enclave Has Gone Before: The Enterprise"
- **Chapter 6:** "Ten Questions About Secure Enterprise Enclaves"

A glossary ends the book with keywords and terms.

Icons Used in This Book

Throughout the book, a few icons will grab your attention. The icons offer more than a distraction from the normal text. What they offer may be a valuable detail, additional technical context, or maybe some helpful information.

TIP

This icon offers a juicy tidbit or recommendation related to the text. Collect these suggestions for easy reference later.

REMEMBER

This icon points out something important to remember, or something to recall from the last time you heard it.

IN THIS CHAPTER

- Raising awareness of the fundamental data security problem
- Recognizing the negative impact on the enterprise
- Creating data insecurity for the CISO

Chapter 1
Understanding the Fundamental Flaw in Computing

Putting private data to work while keeping it secure has been an ongoing challenge for businesses since the beginning of modern computing. In fact, it's been kind of like the quest for the Holy Grail: The ability to control data and maximize how it is used is always just out of reach. Over the years, plenty of vendors have been ready with products that don't quite resolve the problem.

The move to cloud-based computing only exacerbates this issue. Sending data to a remote site and out of an organization's immediate control brings data exposure to bad actors or, worse, the possibility of a data breach. Indeed, fear of data loss is often highlighted as the last barrier to cloud migration.

In this chapter, you learn why data is fundamentally insecure everywhere and the effects this data exposure has on information technology (IT) organizations, business agility, and the psychological well-being of chief information security officers (CISOs) everywhere.

Understanding the Fundamental Data Security Flaw

From the time computing systems were first able to store large amounts of data, individuals with no right to that data have been exposed to it. This overexposure to data has resulted in breaches and data loss, by both bad actors and trusted insiders. Entire cybersecurity industries have sprung up to help organizations keep their data safe and secure and to keep companies out of the courtroom. Yet, despite the layers of security and processes implemented by IT, hackers and unauthorized insiders have been persistently successful in gaining access to sensitive data to which they should never have had access, such as personally identifiable information (PII).

That's because all data — and software security solutions that try to protect that data — are subject to a fundamental flaw persisting in today's computing infrastructure:

Data cannot be simultaneously used and secured.

The reason is simple to understand. All data, including applications, algorithms, and cryptographic keys, must sit exposed and unencrypted in memory for the CPU to use them. Anyone or any process that can get access to the host, including administrators, bad actors, or malware, implicitly gains access to user data exposed in memory and in storage.

This unencrypted memory, which often holds decrypted encryption keys and certificates, can be easily dumped undetected, using commonly available tools. With keys revealed, encryption can no longer protect data or applications. This means malicious insiders, unauthorized third parties, or other bad actors gain easy and unfettered access.

The implications of this flaw can be terrifying. Anyone exposed to host infrastructure can breach the data it manages — regardless of where it is, including in encrypted storage.

No amount of security software or IT process can completely stop them — this data security flaw is at the root of virtually every data breach. Because data is fundamentally defenseless and insecure,

data overexposure, breaches, and incursions are bound to happen, sooner or later. Layers of security might make it harder, but data exposure is still inevitable.

Recognizing the Impact on the Enterprise

As one might expect, this data vulnerability has a significant impact on enterprises, enterprise IT organizations, and the CISOs responsible for enterprise security. Most of these impacts are simply accepted as part of IT. But these issues cost companies dearly in time, money, and lost opportunity. You might recognize some of these challenges in your own organization.

Overexposing Data to Insiders

Today, too many workers have access to too much data by default. In fact, from a security and compliance standpoint, everyone who can access IT infrastructure must be assumed to also be exposed to the data involved. Although some business users have a legitimate need to see data to properly do their jobs, virtually all IT operations staff — including system administrators, site reliability engineers, IT operations personnel, and others — do not.

Employees of third-party partners or cloud service providers are also needlessly exposed to customer data running in a cloud environment. Anyone who can access IT infrastructure can also access data — whether they need this access or not. This is commonly known as *data overexposure.*

In an ideal world, data would be protected everywhere it's used, stored, or moved across a network. Instead of being *exposed* by default (as is the case in memory), data would be *secured* by default starting from a *zero trust data posture.* In such a world, access to infrastructure would no longer include implicit exposure to data.

REMEMBER

What is zero trust? In this case, it means starting with the position that no one is trustworthy enough to receive any access to data. Only those who are explicitly given permission can see any piece of data. All use of that data is controlled by least privileged policies, monitored, and recorded. Think of this like your medical records.

No one has permission to see this data (including family members, other medical providers, and insurance companies) unless you explicitly give them permission. Even then, permission is usually limited to specific information for a specific length of time.

Recognizing Security Tool Fatigue

The effort to keep data and applications as secure as possible results in a cat-and-mouse game where IT organizations have implemented layer upon layer of complex security software and processes, and over time, hackers have found ways around them. These security options include encryption, privileged access management (PAM) solutions, firewalls, storage encryption products, and micro-segmentation. Rest assured, even more are coming.

Adding these complex software security layers and processes is costly to organizations in terms of money, resources to implement and integrate the solutions, and strain on productivity. Yet all these solutions eventually fall to the same data insecurity flaw. Solution after solution may delay a breach, but they can't stop one from eventually happening.

In an ideal world, data would intrinsically have strong protection that reduces the need for much of the accumulated layers of software, process, and complexity.

Avoiding the Cloud

Many businesses aspire to move much, if not all, of their IT infrastructure to the cloud. Data insecurity is often said to be the last major barrier to cloud migration, and this is for good reason; data stored in the cloud is vulnerable to anyone who can gain access to the cloud infrastructure — including insiders employed by the cloud service provider or authorized third parties who work with that provider.

In spite of the cost savings, many companies still maintain their own servers and data centers because they simply can't move their most sensitive data and applications, such as payroll or consumer financial portals, to the cloud.

In an ideal world, businesses could move all relevant IT to the cloud in complete confidence that their data would be measurably more secure there than it is on their own site. Cloud service

providers could then provide assurances that would protect themselves and their clients from insiders and liability.

Limiting Global Reach

Data security concerns may also limit global expansion. Enterprises often want to transact business, process data, or efficiently reach customers around the globe. Some of these locations are untrusted. Lax physical security, for example, means infrastructure may be compromised. There is also the risk that governments may expropriate proprietary data. Because businesses won't take on these risks, they often end up serving potential customers less effectively, or in some cases, not at all.

Compliance with government privacy initiatives, such as the European Union's General Data Privacy Regulation (GDPR) framework or the California Consumer Privacy Act (CCPA), further limits where and how data can be stored. Achieving compliance often means duplicating all or parts of a company's IT infrastructure to achieve data security requirements for personal data. Proving compliance can be even more complex, requiring even more layers of software and complicating processes.

In an ideal world, workloads and data could be processed anywhere with full confidentiality — even if the underlying infrastructure is known to be compromised. With these assurances, businesses would be free and safe to serve their customers in any location, and given simple and reliable data controls, compliance would be easy to prove.

Creating Data Insecurity for the CISO

Because of this fundamental flaw in data security, CISOs must assume that all data will eventually be exposed and become public: It's just a matter of time until a breach or incursion occurs. To be held accountable for protecting data assets that cannot be secured is a frightening prospect. This feeling of *data insecurity* can be paralyzing even as significant time, effort, and money are spent in a futile effort to minimize risk. Many CISOs simply retire early or become consultants in an effort to avoid the stress of not being in control.

In an ideal world, CISOs wouldn't have to think about data protection and privacy at all. Data would inherently be created with its own protections. IT would be in full control over data throughout its entire life cycle — from the time data is created, any time it is used, and, finally, when it is definitively destroyed. That control would extend to anywhere data is used or stored.

Until now, that ideal world has been just a vision.

IN THIS CHAPTER

- Defining secure enclave technologies
- Understanding barriers to enclave technology adoption
- Discovering broad industry support and cooperation

Chapter 2
Introducing Secure Enclave Technologies

Data insecurity is more than an uncomfortable feeling of eventual data loss — it leaves businesses persistently vulnerable to economic loss as well. To reduce these risks and protect their data, most organizations implement complex multi-layered security defenses. None of these address the fundamental data security flaw — at best, they only obscure it. Even elaborate encryption schemes fall short of solving the problem — because the keys they depend on (and the data they protect) end up exposed and unencrypted in memory.

This chapter shows how new CPU-level security features present in modern processors fix this data insecurity flaw and enable a new kind of secure and trusted computing environment.

Defining Secure Enclave Technologies

Researchers have known for years that the ultimate solution to the data insecurity flaw is to create trusted execution, storage, and network environments rooted in trusted hardware. Research has shown that correctly implemented, hardware-based security is virtually impossible to break.

Hardware-rooted solutions have already been implemented within cell phones and some Apple laptops. They work with specialized chips designed to store cryptographic keys that support highly effective disk encryption and private payment functionality. They're so well integrated and perform so well that most users don't even know they're there.

It wasn't until 2015 that Intel introduced Software Guard Extensions (SGX) — a set of proprietary, security-related, silicon-level modifications and machine-level instructions built into the company's new CPUs. AMD quickly followed with its own proprietary instruction set, called Secure Encrypted Virtualization (SEV), for AMD CPUs. Both of these silicon-level machine-language command sets enable the creation of encrypted and isolated segments of memory that can only be decrypted inside the CPU itself. This finally resolves the data in use security flaw with minimal impact on overall CPU performance.

These CPU security features can be used to create what is commonly known as a *secure enclave*, which isolates data in memory, including executable code, from all users and processes on the host computer in such a way that they may be completely unaware of enclave's existence. Even if they are aware, the enclave can't be accessed, even by users and processes with privileged "root" access. The data remains protected even in the event of a physical breach of the host.

With additional software, secure enclaves can even be extended to protect storage and network data for "full stack" coverage for virtually any application. Figure 2-1 shows the architecture of a memory-only secure enclave.


TIP

Full stack has several meanings in the computer industry. Sometimes it refers to the complete set of basic functions that enable modern software to run. This includes CPU, memory, all types of storage, and network communications. Other definitions are broader and include operating systems, virtual machines, and other types of software (including security software) that support the final application. For the purposes of this book, we are using the more encompassing definition.

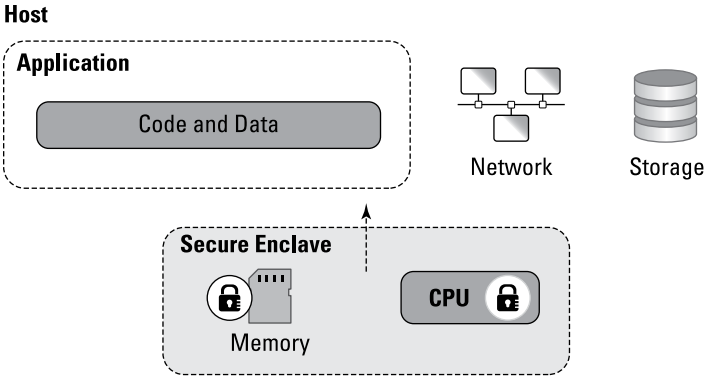

FIGURE 2-1: Secure enclave technology protects running applications in memory.

Understanding Barriers to Enclave Technology Adoption

The power of secure enclave technologies is easy to appreciate but difficult to put to practical use.

All the elements for creating enclaves are present in the CPU silicon. But actually creating enclaved applications requires considerable technical expertise to make them work.

Application programmers need to work with software developer kits (SDKs) to manually rewrite and recompile existing applications so that they run within an enclave. This requires significant time and effort. Most organizations don't have the programming expertise or time required to integrate their applications, which often need protection at the storage and network levels, in addition to memory.

This is aggravated by the fact that standards for enclave technology have not been defined. If an organization were operating machines from three different CPU suppliers and wanted to enclave a specific application, it would likely need to rewrite and recompile that application three times — once for each enclave technology architecture.

It isn't reasonable to expect enterprises to do this development work once, let alone make the changes to operations and

processes that would be required for a typical enterprise IT installation. Many organizations also run legacy or off-the-shelf applications that simply can't be modified at all.

Before enterprises can adopt secure enclave technology, they need a way to avoid the long, tedious process of rewriting and recompiling applications. Other critical capabilities and requirements must also be met to make secure enclaves ready for the enterprise. Chapter 4 examines these requirements in greater detail. The good news is the industry is focused on breaking down these barriers to make enclave technology accessible and practical.

Discovering Broad Industry Support And Cooperation

Key industry players and several startups understand that without broad market support, use of this powerful technology in the market will be limited. A broad group of players is focused on building the bridging layers of software that will ease the widespread adoption of secure enclaves.

CPU manufacturers

Most major CPU manufacturers already include enclave enabling instruction sets coded in their chip architectures. These include Amazon Web Services (AWS), AMD, Arm, and Intel. Amazon has branded its secure enclave technology as AWS Nitro Enclaves.

Cloud service providers (CSPs)

Nearly all companies today embrace cloud computing to some degree. But very few have moved their entire IT operations to the cloud. Cloud Service Providers, and many enterprises, have a clear economic interest in achieving 100 percent cloud adoption. Data security remains the last hurdle to making that happen.

Secure enclave technologies remove obstacles from that path by assuring that customer data is never accessible to cloud service provider insiders. This promises to make public cloud computing at least as secure as private IT infrastructure — in some cases even more so, paving the way for full cloud migration.

That's why Microsoft recently announced the availability of Azure confidential computing platform, based on the Intel CPUs that support Intel SGX enclave enabling technology. Google Cloud has chosen to do the same, leveraging AMD SEV technology. Amazon has delivered AWS Nitro Enclaves, a proprietary enclave technology built into EC2. Chinese hosting companies, including Baidu and Alibaba, have also announced the availability of Intel SGX-enabled hosts that assure confidential computing capabilities within mainland China.

REMEMBER

Cloud clients are not alone in wanting to secure data and applications. CSPs want a level of confidentiality that will protect them from exposure to customer data. They want to minimize liability from incompetent or malicious employees, espionage, and even government warrants. In other words, enclaves protect both service providers and customers.

Confidential Computing Consortium

In 2019, a group of leading cloud and software vendors came together under the auspices of the Linux Foundation to create the Confidential Computing Consortium. The charter of the consortium is to define and promote the adoption of confidential computing. The group is working to bring to market the tools and ecosystems needed to ease the use of enclave technologies.

More than 20 industry leaders have joined the group, including chip manufacturers like AMD, Arm, and Intel; cloud service providers such as Google Cloud, Microsoft Azure, and VMware; and secure enclave software providers such as Anjuna Security.

Table 2-1 lists some of the cloud, software, and hardware vendors supporting secure enclaves.

TABLE 2-1 Wide Industry Support for Secure Enclaves

Sector	Secure Enclave Support
Cloud	Alibaba Cloud, AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud
Operating Systems/Virtual Machine Managers	CentOS, Docker, KVM, Red Hat, VMware, Xen Project
CPU	AMD, ARM, Intel

IN THIS CHAPTER

- Virtually eliminating the risk of data breach
- Securing all data and applications by default everywhere it is used
- Simplifying data security and operational compliance
- Establishing zero-trust infrastructure

Chapter 3
Looking at Enclave Benefits for the Enterprise

In this chapter, we talk about the broad, positive impacts and implications secure enclave technologies can have on IT organizations and the business itself. Perhaps as important, we discuss how this may ease the "data insecure" state-of-mind of the chief information security officer (CISO).

Virtually Eliminating Risk of Data Breach

We'll start with perhaps the most obvious benefit. Think of enclave technologies as creating a cloaking device around data. No one outside the enclave can see the data inside — not even if the host is compromised. This assures that even if bad actors manage to get a hold of data on disk or on the network, they can't see or manipulate the data unless explicitly authorized.

With data protected at this fundamental level, the risk of a data breach is virtually eliminated.

Securing All Data and Applications by Default

Enclave technologies potentially provide inexpensive and simple building blocks for data and application protection as part of the IT infrastructure. This can enable all existing applications and data to be secured by default.

Today, because of cost, complexity, and performance degradation, data protection is generally applied only to a company's most sensitive data. Unfortunately, this selectivity tells hackers *exactly* where to focus their efforts.

When costs and performance impacts are low enough, cloaking all data and applications in a secure enclave improves an organization's overall security posture by eliminating this signaling. All data — whether stored, used, or transmitted — will be secure by default.

As enclave protection becomes ubiquitous, enterprises will no longer have to worry about "shadow IT." Data never escapes the enclave, and thus enterprises retain full control.

Protecting Data Everywhere It's Used

With enclaves, applications and data have the same hardware-grade protection wherever they run — on premises, in the cloud, and even in hostile and untrusted environments. Alibaba, Amazon AWS, Baidu, Microsoft Azure, and other cloud services already support enclave technologies. This means that with the right infrastructure now in place, it's now possible to securely execute workloads or store data in even untrusted locations. It no longer matters where enclaved data and applications are stored or replicated. What matters is where the *keys* to that data and applications are held.

Isolating Insiders From Data

Guarding your data against insiders has become one of the hardest risks to mitigate. In some cases, privileged users — most often attackers impersonating employees — gain unauthorized access to data. Other times, data may be left exposed inadvertently. Today, simply by doing their jobs, IT insiders are implicitly overexposed by default to data they don't need or want to see.

This is because access to infrastructure today implies access to host memory. Once an insider gains access to a physical (or virtual) machine, they can dump unencrypted memory to get the cryptographic keys they need to execute catastrophic data storage breaches.

Enclave technology mitigates this risk because, even if an insider (or a bad actor impersonating an insider) gains physical access to a machine, it's nearly impossible for them to gain access to the actual enclave. And even if they could somehow get to the data, it would still be encrypted and useless outside the perimeter of the enclave.

Simplifying Data And Operational Compliance

The same data overexposure issues make compliance a complex physical and IT security challenge. In today's insecure hardware environments, many IT staff can be caught in the data compliance dragnet. To reduce staff exposure, complex layers of security product and process need to be implemented as a control to counter data exposure.

That complexity is potentially eliminated with secure enclave protections. Data within a secure enclave is only accessible within the enclave itself. That means users, processes, and all software running on the same physical server can't see the enclave itself or the data it contains. Access to the enclave and the application must be explicitly granted, and thus, can be regulated,

monitored, documented, and audited. This simplifies compliance dramatically, with the enclave acting as a powerful data access control.

Assuring Customer Data Privacy

Companies today manage the private information of their customers by gathering large "lakes" of data. Though analysis of this data is critical to the business, no one in the company ever actually needs to see the actual data.

With enclave technology, data privacy is assured wherever it flows and however it's processed. Customer data, for example, can be collected, moved, and processed all within the secure confines of the enclave without ever compromising customer privacy. This is a significant competitive advantage for companies because they can now certify that their employees won't have access to customer data.

Establishing Zero Trust Infrastructure

As Chapter 1 explains, *zero trust* is a security model based on the principle of maintaining strict access controls and not trusting anyone, anywhere, at any time. Although great in concept, implementing zero trust in software is vulnerable to the same data security flaws as any other software: Though access to data by users may be controlled, data remains exposed and free to access through memory — whether or not it's encrypted, as in storage, for example.

Enclave technology has the potential to be a simple-to-implement zero trust infrastructure that isolates data from all users. With enclaves, data access is only allowed through explicit policy. Any access or use of data can be vigilantly controlled, monitored, and recorded. Even more, secure enclaves create a hardware root of trust from which all software and data can be verified, trusted, and identified as genuine, further assuring integrity.

Mitigating Vulnerabilities En Masse

Most companies have hundreds of thousands, if not millions, of cyber-related vulnerabilities throughout their IT infrastructure. Enclaves establish a tight hardware-grade secure perimeter around data and applications that renders many host, operating system, container, and network vulnerabilities irrelevant.

With application and data enclaving, there is less of an urgency to patch infrastructure vulnerabilities to protect data. Even in the event of a physical breach of hardware, the data inside remains protected. This mitigates many vulnerabilities, resulting in a substantial reduction in cyber risk.

Eliminating Costly Security Software Layers

Over the last 30 years, industry analysts have been fairly uniform in their cybersecurity advice: A relatively secure data posture can be achieved by layering physical, network, system, endpoint, and application security protections.

Purchasing and maintaining this complex array of security solutions is expensive. Installing and integrating them into an enterprise IT organization requires significant manpower. The overwhelming complexity of integrating, maintaining, and configuring growing layers of security software itself creates a security risk — as multiple software packages overlap, conflict, or create undetected gaps in the organization's IT armor.

When enclave-based data protection is introduced, these software layers can be dramatically rationalized. Privileged access management (PAM), data classification systems, network security products, as well as other host, network, perimeter, and physical security solutions become redundant and unnecessary. With the risk of data exposure eliminated, the organization no longer needs to maintain a costly, complex security infrastructure or the complicated processes that impede IT productivity, as shown in Figure 3-1.

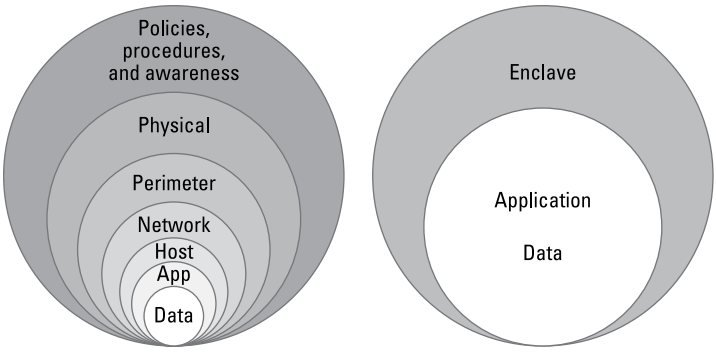

FIGURE 3-1: Because data is implicitly secured by hardware within the enclave, additional layers of data security can be reduced or eliminated.

IN THIS CHAPTER

- Putting enclave technology to work
- Introducing secure enterprise enclaves
- Building a secure enclave solution for enterprises
- Easily deploying data security by default

Chapter 4
Making Secure Enclaves Real for the Enterprise

This chapter examines the specific requirements that must be met for secure enclaves to be widely deployed in the enterprise.

Putting Enclave Technology to Work for the Enterprise

Fixing the data insecurity flaw opens the door to solving a host of long-standing security challenges in a variety of industries. It's likely that specialized enclaves will be created for Internet of Things (IoT) devices, real-time applications, machine learning applications, secure storage, and other areas.

Most important to enterprise chief information security officers (CISOs) is a general-purpose software solution called a *secure enterprise enclave* that focuses on solving enterprise data security challenges and opening up new business opportunities.

The focus in this chapter is to examine the specific requirements for implementing enclave technologies in the enterprise.

Introducing Secure Enterprise Enclaves

Secure enterprise enclaves are designed to enable businesses to deliver data security, maintain the privacy of customer data, and enable confidential computing on premises, and in public, private, and hybrid clouds.

Think of secure enterprise enclaves as similar to a secure virtual machine that establishes an isolated, encrypted, and validated environment in which applications and data securely reside and operate.

Like all enclaves, a secure enterprise enclave is isolated. No process other than the enclave itself can access its protected resources, which now extend beyond memory to storage and network communications. All data — including applications and data in use and at rest — are encrypted. Decryption only happens within the CPU, which is validated genuine before it is used.

Secure enterprise enclave technologies add a layer of software immediately above the CPU that enables the creation, extension, and management of the enterprise enclave. This enables full-stack data encryption security with no additional development cost or process changes. Software developer kits (SDKs) are not required, so this approach delivers data security while remaining transparent to applications, data, and IT operations.

The result is a fully confidential and secure execution environment that is suitable for protecting everything from databases to human resources (HR) applications to customer data — anywhere they're run or stored — without modification.

Building a Secure Enclave Solution for Enterprises

Before enterprises can adopt secure enclave technology on a wide scale, they need a way to address the issue of rewriting and recompiling applications multiple times. But other key criteria should also be met to make secure enclaves enterprise-ready.

Adoption should be as simple as "lift and shift"

Enterprises often have hundreds of applications. Some are bought off the shelf, and many are legacy applications. Others are under continuous development. Ideally, an enterprise enclave solution needs to make enclaving any application as smooth as possible. Such an ideal solution would require no changes to the application, no recompiling, and no programming. Enclaving an application shouldn't modify or slow the software development life cycle or demand major changes from operations.


TIP

Every application and process being run within a secure enterprise enclave should simply run as is, regardless of the underlying hardware architecture on which it is run.

Enclave protection should extend full stack

Protecting data in memory is critical to maintaining data security, but that alone is not enough to support even the simplest enterprise applications. Data protections must extend beyond memory to protect storage and communications as well. Figure 4-1 shows how full stack protection secures applications from compromised operating systems, virtual machines, containers, and more, while also encrypting memory, storage, and network communication to protect all elements of an application and data with the smallest possible attack surface.

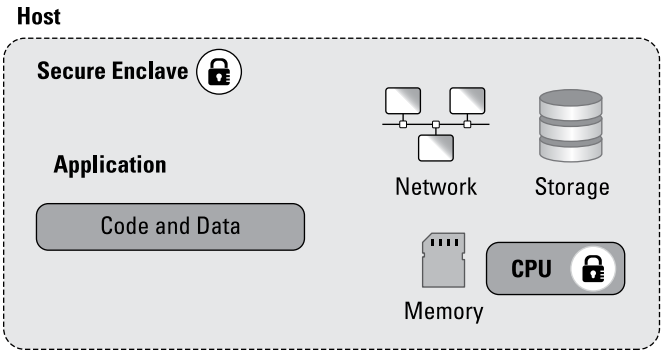

FIGURE 4-1: Enterprise enclaves cover the entire application and data.

Support should be platform and cloud agnostic

No enterprise today can afford to be locked into one hardware platform or a single cloud service. Nor can they afford to develop software for multiple enclave technologies. Secure enterprise enclave solutions must offer transparent support across multiple enclave technology platforms, enabling applications to run on any confidential cloud or system without modification.

Enterprise-class management

Shifting applications into an enclave means gaining full control over your applications and data lifecycle. Secure enterprise enclaves should provide centralized enclave lifecycle and management capabilities. They should also support disaster recovery and redundancy capabilities that enable an enterprise to scale enclaves to be reliably deployed across an enterprise's entire application and data portfolio.

Integrating with the enterprise IT ecosystem

In the course of normal IT business, applications are developed and deployed, infrastructure is built, and operations are continuously managed. Secure enterprise enclaves need to integrate with the delivery processes and management systems that make up today's enterprise IT ecosystem.

Secure enterprise enclaves should secure and scale transparently with container infrastructure and operations systems, such as Kubernetes, with minimal configuration needed. They should work smoothly — without having to alter existing software development delivery processes — to facilitate, if not accelerate, the continuous delivery of application features.

Once deployed, enclave technologies will require some degree of operational monitoring and reporting. An enterprise-ready solution should be able to report on enclave-related activities through enterprise secure information and event management (SIEM) and security operations, automation, and response (SOAR) systems for centralized monitoring, reporting, and forensics.

Other enterprise information system integrations may be required and will vary from organization to organization. It's important to carefully consider the additional management and infrastructure integrations required. Confirm that the chosen secure enterprise enclave solution has open application programming interfaces (APIs) or purpose-built connectors to facilitate building integrated and automated processes and workflows.


TIP

Kubernetes is an open-source system for automating application deployment, scaling, and management. Originally designed by Google, it is now maintained by the Cloud Native Computing Foundation. Many cloud services such as Microsoft Azure confidential computing offer Kubernetes-based services that work with secure enclave technologies.

Easily Deploying Data Security by Default

The less visible a cybersecurity solution is to business operations, the more effective it will be. Enterprise enclave solutions offer the promise of both transparency and efficacy without compromise. Unlike higher-layer software security tools, enclave technology exists as part of the underlying physical infrastructure. With secure enterprise enclave software to bridge vendor and technology gaps, data security itself becomes part of the enterprise infrastructure on which applications are deployed. This will secure all applications and data that run within an enclave *by default*.


TIP

When the question arises, "Should we run securely or not run securely?," the correct answer is always "Run securely," of course.

IN THIS CHAPTER

- Migrating to the cloud with confidence
- Executing workloads safely anywhere
- Opening up new possibilities with secure data everywhere

Chapter 5
Going Where No Enclave Has Gone Before: The Enterprise

Secure enterprise enclaves allow enterprises to reduce risk, improve security, and resolve the data security challenges that have dogged businesses for decades. But there's more. They also open up new ways to reduce costs, increase productivity, and win new business.

This chapter explores some of the new opportunities that may be available to your business and security operations.

Migrating to the Cloud with Confidence

The last great barrier to migrating IT to the cloud is addressing the understandable fears of the chief information security officer (CISO) regarding data security. There's good reason to be concerned. Workloads and data executed and stored in the public cloud expose data to too many people — good and bad.

CISOs want to ensure that data protections in the cloud are at least as good as those on premises. With secure enclaves, workloads and data sent to the cloud are inaccessible to service provider insiders, even to those that have direct and privileged access to the infrastructure. This allows enterprises to finally migrate even the most sensitive applications to the cloud with confidence. The result is dramatically reduced costs associated with maintaining private compute, storage and networking equipment, facilities, and layers of security software — while upgrading security and reducing risk and complexity.

With application "lift and shift," secure enterprise enclaves make this move especially simple, eliminating reprogramming and not limiting the ability to choose multiple cloud and hardware vendors.

Executing Workloads Safely Anywhere

Enterprises often operate on a multinational level, with sales and marketing offices, development centers, and data operations located offshore to more effectively penetrate new markets.

This puts data at risk. In many locations, data intrusions are executed by nation-states, who have already infiltrated seemingly independent data centers. In such countries where industrial espionage efforts are the norm, using technology such as secure enterprise enclaves will defeat efforts to access critical data.

Secure enclaves also make it much easier for IT organizations to effectively establish secure data residency in a remote location. That means they can safely store data in a geographical location of choice, which is often desirable for regulatory, tax, or policy reasons.

Securing databases

Securing database operations and communications presents another excellent opportunity for applying secure enclaves. Redis, an open-source, in-memory database that's surging in popularity, stores chunks of potentially sensitive data in memory as plaintext. Without enclave protections, that data is easily accessible to an insider or bad actor who can gain access to servers,

operating systems, and containers. That same database, enclaved and running without modification within the confines of a secure enterprise enclave, is protected from that in-memory vulnerability. The result is one of the most secure database solutions available.


TIP

An enterprise-ready application of secure enclaves can protect the data in a Redis database from unauthorized incursion — even by authorized personnel. This protection happens without changes to application code, processes, or the use of SDKs.

Implementing infrastructure micro-segmentation

Improving security is one of the many advantages of micro-segmentation, which breaks a network into explicit policy-driven communications. This helps companies better control networks that are open and insecure by default.

Secure enterprise enclaves offer a more complete implementation of micro-segmentation that extends beyond the network. Like network micro-segmentation, communication relationships between entities must be explicitly allowed through policy. But unlike network segmentation where segmentation starts and ends with the network, enclave-enabled micro-segmentation encompasses hosts, memory, CPU, storage, and network — a far more complete and secure implementation of the concept.

The implications: An open and insecure infrastructure can be transformed into a logically segmented and extremely private business-class resource at any scale over any geography.

Streamlining and Securing Key Management

Cryptographic encryption is the superior method of ensuring that data or software cannot be accessed by unauthorized users (unless, of course, keys are exposed in memory). A simple way to look at cryptographic encryption is as a series of locks and keys, which must be safe.

With secure enclave technology, keys are hard-coded in the processor — embedded in the CPU as part of the manufacturing process. That means there's no ability to access or compromise this key — regardless of the privileges of the person attempting to open the lock.

In an enclaved infrastructure, key management and encryption becomes a default, implicit, and invisible function of the infrastructure, rather than part of an elaborate (and insecure) software scheme implemented over layers of software. IT may still need to understand security key management, but the team won't have to spend time managing this function as a separate software system because it becomes a service of the underlying hardware.

Protecting Deployed Intellectual Property

Sometimes an organization needs to protect more than just raw data. Intellectual property (IP), including proprietary software, machine learning models, and results of other analyses can easily be replicated across the world at the speed of the Internet. Any remote use of these software assets, even in unsecure environments, comes with the risk of losing commercial control. This is because modern software, like all data, is exposed and enabled to run on *any* computer.

Enterprise enclave technologies can give software asset owners the control they need to protect their IP. They can even leverage policies to restrict usage of that software to specific hosts, or, if needed, for specific durations. Secure enterprise enclaves give intellectual property owners complete control over who uses their software as well as if, how, where, and when their software and data can be used.

Opening up New Possibilities With Secure Data Everywhere

Imagine a world where data security is universal across the enterprise, the cloud, and the world by default. Better still, imagine your complete confidence that data security in the cloud is just as

strong — if not stronger — than it is within an enterprise data center.

With that knowledge, now imagine what new applications may arise that would not even be conceivable without this higher level of data security.

Multi-Party Analytics

Secure enterprise enclaves enable data to be securely shared across multiple parties for analytics without exposing it. Applications might include financial or healthcare records, where confidentiality and integrity must be preserved even while shared for analysis across organizations. Sensitive data can be combined and analyzed within the secure enterprise enclave with only specific analytical results exposed.

Personal Data Privacy

Contact tracing has received much attention throughout the fight to control the COVID-19 pandemic.

The fastest, most efficient, and untrusted implementation of contact tracing involves the timely and automated collection and processing of real-time geolocation data from mobile devices. That data is processed to determine who had contact with an infected individual and when.

As you can imagine, this data is extremely personal. In today's computing environments, such data would be exposed in multiple clouds. In many geographies, such as the United States and the European Union, this kind of potential exposure is legally unacceptable. Yet manual contact tracing is slow and ineffective — putting more lives at risk.

But what if mobile device-based tracing could be implemented without exposing data to anyone? What if data privacy concerns and risks could be completely mitigated?

With secure enterprise enclaves, contract tracing systems could potentially collect, store, process, and expose private tracing results without exposing the raw data itself to anyone. This would optimize both efficacy and data privacy. It would also save lives.

These are just two examples of what may be beyond the horizon when business is freed from data privacy risks. From an enterprise perspective, moving beyond today's security limitations will usher in a new era of secure computing and IT. It will also allow the CISO to finally move beyond the current mental stress of data insecurity, knowing all data is finally secure by default.

IN THIS CHAPTER

- Understanding key points about secure enclave management
- Overcoming data insecurity

Chapter 6
Ten Questions About Secure Enterprise Enclaves

As security technology goes, the hardware-based secure enclave may be one of the most underrated options available. Even with enormous support by CPU and cloud vendors, implementation of secure enclaves is just beginning to take off. This chapter offers ten questions you're likely to ask about secure enclaves — plus the answers!

What Is a Secure Enterprise Enclave?

Secure enterprise enclaves enable applications and their data to execute securely with hardware-level protection from secure computing hardware. All data is encrypted in isolated segments of memory and decrypted only inside the CPU when it's used. The enclaved memory segments and data remain completely protected, even if the operating system, hypervisor, or root user are compromised. With the addition of enterprise enclave software, data can be fully protected across its full life cycle — at rest, in motion, and in use — from creation to retirement.

Why Should I Consider Secure Enclaves Now?

There are three key reasons to start using secure enclaves now:

- Enclaves are already being adopted throughout the industry and will be an integral part of enterprise IT strategy in the next few years. Your security contracts come up for renewal all the time. You'll need to decide if you want to continue to invest in legacy technologies or position yourself for a more secure and cost-effective enclave-enabled future.
- You can start right now with low-cost, low-risk proof of concept (POC) projects to understand how secure enclaves will fit in your organization.
- Adopting any new technology takes time. If secure enclaves are a fit for your organization, you'll need to start planning for an enterprise-wide rollout now. This is likely similar to the process you underwent when implementing server virtualization.

How Safe Are Secure Enclaves — Really?

Hardware-based enclave technology is far more secure than the software solutions you are currently using. Secure enclaves are so hard to crack that security researchers are spending an enormous amount of time trying to make a name for themselves by attempting to compromise them, with little success. This is great news for enterprises because hardware vendors are now five years into this cycle, making enclave technology, if not unbreakable, certainly miles ahead of existing security approaches. As of this printing, the few vulnerabilities that have been discovered have been patched. Even these required physical access to a chip, sometimes using a probe, and thus will not pose a realistic threat to most enterprises or cloud providers.

How Difficult Are Secure Enterprise Enclaves to Implement?

The adoption of secure enclaves is similar to the adoption of virtualization technologies. Implementing virtualization at the chip instruction level is difficult, requiring software development kits (SDKs) and custom application software modifications. With secure enterprise enclaves, just as with common virtualization systems, enclaving can be implemented transparently for applications, end-users, and operations staff using commercial software that does the heavy lifting. Evaluating enclave software solutions against the critical capabilities outlined in this book is the key action enterprises need to take today to find the simplest and most effective path.

How Do Secure Enclaves Work in the Cloud?

Secure enclaves work extremely well in cloud environments — whether public, private, or hybrid clouds. All major cloud vendors, including AWS, Microsoft Azure, Google, and other global providers, support secure enclave technologies today, usually as a simple option or add-on to their existing hosts or virtual machines (VMs).

How Will My Organization Be Affected by Implementing Secure Enclaves?

With the proper software, secure enclaves will result in few costs and many benefits for your organization. Applications need not be rewritten or re-compiled. There will be only a small impact on operations because you will need to ensure your hardware and VMs will support secure enclave technology. In some cases, you

may need to integrate enclaving capabilities into your management and monitoring systems. Your enclave vendor's out-of-the-box integrations and APIs should minimize the integration effort.

Once you have implemented enclaves, the benefits are tremendous — in terms of moving secure workloads to the cloud, protecting data from insiders and external bad actors, safeguarding customer privacy, and reducing the costs of maintaining layers of security software and processes.

What Is the Performance Impact on Applications That Run in a Secure Enclave?

The performance impact will vary, depending on your application and the secure enclave implementation. However, because all encryption and decryption are done efficiently inside a chip, performance, especially compared to software-based solutions, is dramatically improved. Enclave performance impacts are similar to those of virtualization. As software, hardware, and firmware improve, performance impacts should diminish.

Here's a rule of thumb. If your application can run virtualized with acceptable performance, it should run fully secured with similar performance within a secure enclave.

What New Opportunities Might Be Available With Secure Enclaves?

As hardware enclave-enabling technologies become ubiquitous in hardware and in the cloud, computing will move into a new era where the persistent issues of data security are solved and new powerful applications can be built. The largest and most important opportunity will be to allow sensitive applications to safely move to the cloud. Confidential multi-party data sharing

will enable new classes of powerful secure applications, such as contact tracing, medical record management, and election solutions. These are possible because of new levels of personal data and application security, privacy, and integrity.

What Benefits Will My Organization See by Implementing Secure Enclaves?

Your organization will see several immediate benefits. First, you'll see a potential dramatic reduction in your attack surface. Access to enclaved data can only come from explicit permissions granted remotely from a computing host. With attack surfaces minimized, you'll be able to run sensitive applications securely anywhere, on premises, in the cloud, or in hybrid configurations. Data security and privacy will be enhanced transparently, as the number of people and credentials that can access data are both dramatically reduced. You'll be able to safely run applications in untrusted or even hostile environments. All of this will simplify your security cost by reducing the need for redundant software, people, and process.

How Will This Affect My Developer Operations and Software Development Processes?

This depends on your enclave strategy and software. With secure enterprise enclaves, there should only be a minor impact on these processes. With the right software, there should be no change to the development process. However, at some point, you will want to integrate secure enclave hardware and software into your continuous integration and continuous delivery (CI/CD) processes. This can be as simple as adding another server and replacing a few commands to the test and production environments.

Bonus Question: What Should I Do Now to Get the Process Started?

There is no substitute for diving in and learning more about secure enclaves with a proof-of-concept project (POC). Pick an application and the associated data that you'd like to secure, either on premises or in the cloud. Next, contact a software vendor, such as Anjuna Security, who can help you quickly implement a secure enterprise enclave POC to demonstrate how simple integrating secure enclaves into your enterprise can be.

Glossary

AMD SEV (Secure Encrypted Virtualization): An enclave-enabling technology developed by Advanced Micro Devices (AMD) to protect Linux KVM virtual machines by transparently encrypting the memory of each VM with a unique key.

Anjuna Security: A provider of enterprise secure enclave software solutions.

AWS Nitro enclaves: The secure enclave-enabling technology developed by Amazon Web Services (AWS), which enables customers to create isolated compute environments to further protect and securely process highly sensitive data within EC2 instances.

cloud services provider (CSP): An organization that maintains a network of remote servers hosted on the Internet to store, manage, and process data. Sample providers are Microsoft Azure, Amazon AWS, and Google Cloud.

confidential computing: A term promoted by the Confidential Computing Consortium and others, it refers to the protection and encryption of data on public clouds utilizing a hardware-based secure enclave or trusted execution environment (TEE).

continuous integration/deployment (CI/CD): The process by which developers send software to be integrated into larger systems for testing multiple times per day (or more). After being tested, the system is deployed at increasing scale by automated tools.

data residency: Data residency is the process where an organization specifies that certain data must be stored in a specific geographical location, usually for regulatory, tax, or policy reasons. By contrast, **data localization** is implemented when it is legally required that data created within a certain territory remain within that territory. The degree of data control afforded by secure enterprise enclaves enables highly reliable data residency and localization.

enterprise enclave (or secure enterprise enclave): A secure enclave solution designed to address the specific needs and requirements of enterprise IT organizations.

full stack: Refers to the complete set of basic components and functions that enable modern software to run: CPU, memory, all kinds of storage, and network communications. The "full software stack" also includes operating systems, virtual machines, and other applications (including security software) that support the final application.

hardware encryption: Using hardware to cryptographically transform usable data into something not useful to those without the proper credentials or keys.

intellectual property: Creative works or inventions that should be protected from theft, such as data, application code, and algorithms.

Intel SGX (Software Guard Extensions): A set of security-related instruction codes that are built into some modern Intel central processing units (CPUs) that enable the creation of secure enclaves.

Kubernetes: Kubernetes is an open source platform that allows you to cluster together groups of hosts running Linux containers and easily and efficiently manage those clusters at scale.

"lift and shift:" The ability to place an application within a secure enclave without the need to rewrite or recompile the application.

Microsoft Azure confidential computing: Microsoft's implementation of a secure computing platform that leverages secure enclave technologies, including Intel SGX-enabled CPUs.

on-premises ("on-prem") computing: Storing, managing, and processing data and applications at an organization's own IT facility, rather than remotely.

proof of concept (POC): A small pilot project to demonstrate that a technology solution is feasible.

hardware root of trust: A system element that verifies data integrity and confidentiality between trusted devices or software in a system or network. It assures that all components of an IT system (hardware, firmware, software, and so on) are secured.

security ecosystem: The diverse set of security solutions implemented by an organization, and the interdependencies among components.

secure enclave technology: A set of technologies that enable the creation of a trusted execution environment**.** This includes encryption/decryption within the CPUs, memory and data isolation, and other security features that vary by vendor.

shadow IT: Information systems and data deployed by groups other than the central IT department, to work around the perceived shortcomings of the main IT function.

software development kit (SDK): A set of tools to allow developers to build software on top of a particular technology. Typically, these are unique to a particular hardware architecture.

trusted execution environment (TEE): An isolated execution environment providing security features, such as isolated execution and integrity of applications executing within the TEE, along with encryption of data. Often used interchangeably with *secure enclave.*

virtual machine (VM): An emulation of a computer system, based on computer architectures, that provides the functionality of a physical computer.

zero trust security: A security approach where no entity is trusted by default when accessing a resource such as networks, hosts, and data. Even when access is granted, it is continuously monitored and verified against least-privileged access policies. Zero trust is meant to counter the open nature of IT infrastructure, which until now has led data, for example, to be exposed by default.

Simple. Strong. Secure.

Enterprise Enclaves from Anjuna.

For data to be used, it must be exposed and unencrypted. That makes it vulnerable to data breaches, incursions by bad actors, and overall overexposure.

No matter how good your security software, it can't overcome this fundamental weakness. But now there's a way to keep your data secure by default. In memory, on disk, or on the network. On premises or in the cloud.

Secure enclave technology isolates data and applications from every other process or user. Anjuna makes the process of adopting enclaves for the enterprise amazingly simple.

Come as You Are

Easily protect all data and applications with no recoding or recompiling.

Go Anywhere You Want

Available for Microsoft Azure, AWS Nitro Enclaves, Intel SGX, and AMD SEV.

Be Ready For Anything

High availability, disaster recovery, scaling in the cloud, integration with key management solutions, and more.

Tired of living with the threat of data insecurity?

Contact us. We make it simple to be secure and strong.

anjuna

Keeping data secure by default.

Anjuna.io
info@anjuna.io

Secure enterprise enclaves — the standard for cloud data security

Now there's a way to make data secure by default — no matter where it's used or stored. Industry leaders are implementing this powerful new capability with AMD SEV, AWS Nitro Enclaves, Google Confidential VMs, Intel SGX, and Microsoft Azure to enable virtually unbreakable data protection in the enterprise data center and the cloud. This book helps you plan a path to take full advantage of this powerful capability to lock down data security and save money, while facilitating safe data, confidential computing, and application migration to the cloud.

Inside...

- The fundamental flaw exposing all data
- The enclave technology solution
- How enclaves improve data security
- Realizing opportunities now available
- Enclaving enterprise applications simply
- Addressing enterprise requirements
- Bringing cloud computing to all apps

anjuna

Ayal Yogev is the CEO and co-founder of Anjuna Security. Anjuna's products enable enterprises to simply implement secure enclaves across all major platforms. **Dr. Yan Michalevsky** is the CTO and co-founder of Anjuna Security. An expert in cryptography and computer security, Yan has a PhD from Stanford University.

ISBN: 978-1-119-76759-6
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.