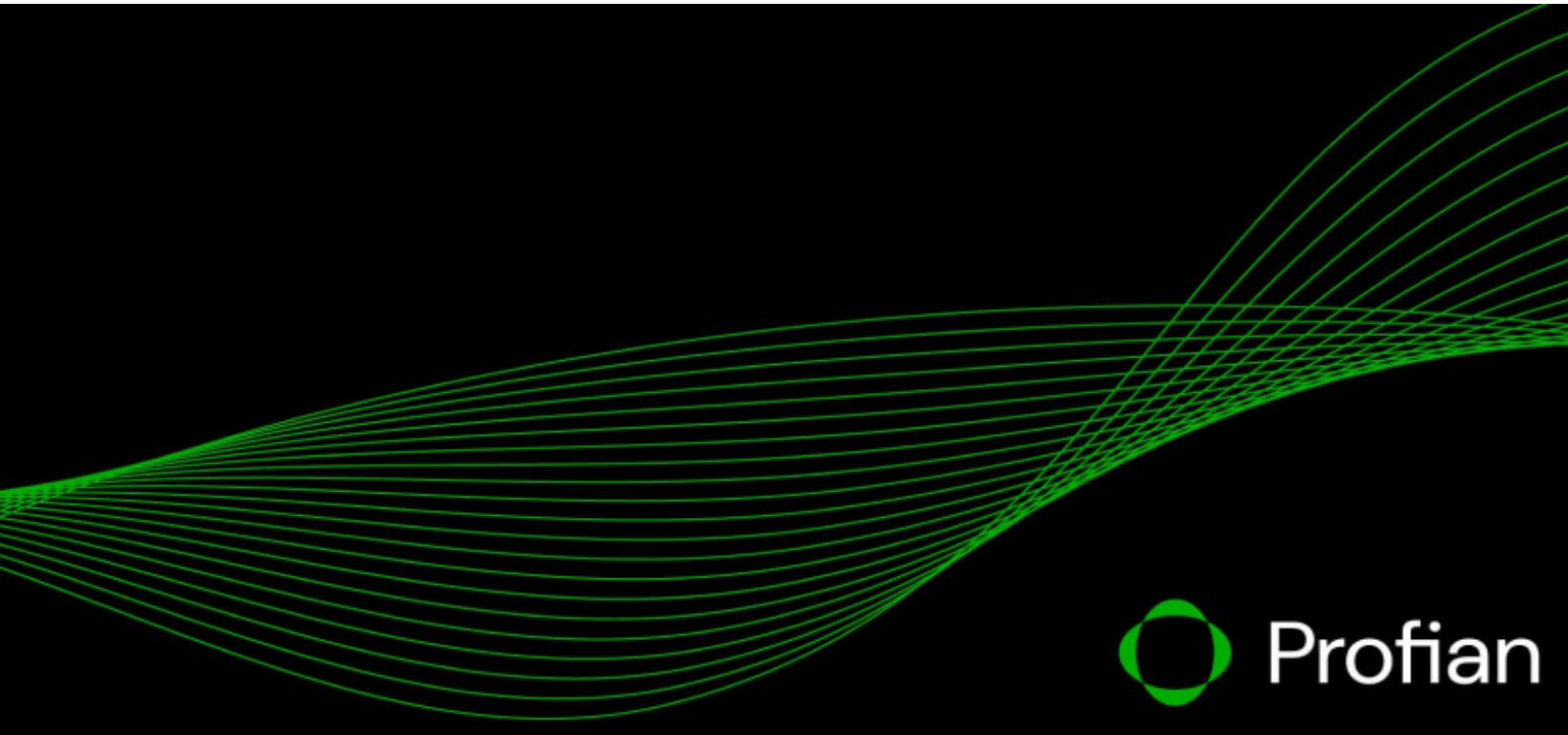
Profian

MANAGING INSIDER RISK WITH CONFIDENTIAL COMPUTING

Learn how to protect your data and applications in use.



Profian

The reality of insider threats

Companies reporting insider incidents now stand at 67%, up from 53% in 2018[1].

Insider risk is:

- associated with malicious or negligent employees or the loss of employee credentials
- difficult to address because of the requirement for legitimate access to machines and networks with sensitive data and applications

Organizations are made up of lots of parts – processes, intellectual property, buildings and facilities, legal agreements, computer software, computer hardware, customer data and more. But, one of the most important is people.

Whether those are full-time employees, part-time employees, consultants, contractors, on-site or hybrid, most will need access to the organization's computer systems in some way or other to perform their roles. Most people working for an organization are honest, but some are not. Some may be honest, but insufficiently careful with how they use or share data, and even when everybody is careful and honest, there still exists the danger of lost or stolen credentials (such as passwords or mobile devices) being used by external attackers to access applications or exfiltrate data for which they have no authorisation. All of these lead to insider threats and expose organizations to insider risk.

The problem with addressing insider risk is that data and applications run on machines to which many people within the organization have - and require - access to perform their roles, and these machines are networked to each other and the internet. Even with a zero trust architecture, which attempts to reduce unnecessary access to machines and applications, employees and contractors, any privileged

[1] 2022 Cost of Insider Threats Global Report

access to a machine on which sensitive data is being processed, or on which a sensitive application is running, allows an attacker to read or change that data or application. Sensitive data could include anything from customers' credit card data to patient health records, from financial predictions to cryptographic keys protecting the organization's website. Sensitive applications could include AI/ML models, risk assessment or trading models or the firewalls protecting the core business critical infrastructure.

Existing approaches[2] to mitigating insider risk concentrate on securing data in two states: data at rest (stored on disk or in a database) and data in transit (data on the network). Solutions for this are important, but cannot address the time when data is most at risk: **when it is in use.**

Data in use is the third, most vulnerable state: data being processed by an application, and the application itself. Beyond expensive and difficult to use Hardware Security Modules (HSMs), there have been no technologies which provide protection for data in use which provide protection in hardware until the recent advent of Confidential Computing.

What is Confidential Computing?

Confidential Computing:

- **uses hardware-based TEEs**
- **provides protection from malicious or compromised hosts**

[2] https://www.ncsc.gov.uk/guidance/reducing-data-exfiltration-by-malicious-insiders

"Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment" as defined by the Confidential Computing Consortium[3].

Today's modern data centers are built on the latest hardware which provide isolated areas – think built-in "mini-vaults" – inside each CPU. These vaults are called Trusted Execution Environments (TEEs) and they allow for hardware-based encryption of data in use. Taking advantage of TEEs to protect and encrypt data in use is the cutting-edge security technology known as Confidential Computing.

Confidential Computing, or encrypting data in use within a secure hardware environment, completes the data security triangle since data at rest (in storage) and in transit (across networks) are routinely encrypted.

For a deeper dive into Confidential Computing and Trusted Execution Environments, download our white paper.

How does Confidential Computing address insider risk?

Confidential Computing with Profian Assure:

- **Stops malicious insiders**
- **Stops attackers with compromised credentials**
- **Can be deployed on both public and on-premises systems**
- **Provides equal protection for data and applications**

[3] Confidential Computing Consortium, 2021, *A Technical Analysis of Confidential Computing, v1.2*, https://confidentialcomputing.io/wp-content/uploads/sites/85/2022/01/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.2.pdf

When an organization adopts Confidential Computing, they take the opportunity to protect their most valuable assets - sensitive data and applications - from unauthorized access. Confidential Computing allows organizations to manage and reduce their insider risk.

Standard computing, also known as classical computing, including bare-metal servers, containers and virtual machines (VMs) is how applications are normally run on servers, whether they are in the public or private cloud, in data centers, on-premises or on the Edge. In the standard computing model, anyone with access to a machine as an administrator, or with access to particular applications that privileged access, is able to look at and tamper with data and applications on that machine. It is this ability - to look at and tamper - that Confidential Computing blocks.

There are two main types of protection relevant to both data and applications:

- integrity protection (stopping unauthorized entities from making changes)
- confidentiality protection (stopping unauthorized entities from seeing or copying).

All true Confidential Computing implementations[4] provide at least three types of protection:

1. Data integrity
2. Data confidentiality
3. Application integrity

Our implementation provides a fourth type of protection, vital for many businesses: application confidentiality.

Profian Assure provides an added layer of security to your Confidential Computing environment through an automatic attestation process, which restricts the deployment of your workload to the secure environment until the attestation process is complete. Receive neutral,

[4] According to the Confidential Computing Consortium definition.

third-party validation that your “virtual vault” has been created properly to protect both your applications and data before they are deployed.

Profian

Profian delivers Confidential Computing solutions that solve for security of data in use, a well-known vulnerability of cloud computing. We help security teams seamlessly create private environments on public cloud hardware so organizations can enjoy the speed, scale and cost-saving benefits of cloud computing for even the most sensitive workloads. Profian's third-party attestation service helps meet regulatory standards and build trust with customers. Our solution builds on the open source project Enarx, of which Profian is the custodian.

Profian is a a member of the following organizations: