Trusted Computing: Hardware Security and Confidential Computing For Server Platforms

MARCH 2023

Authors
Ralf Helkenberg
Research Manager, European Privacy & Data Security, IDC

IDC

An IDC Infobite, sponsored by AMD

The Cyber Resilience Imperative

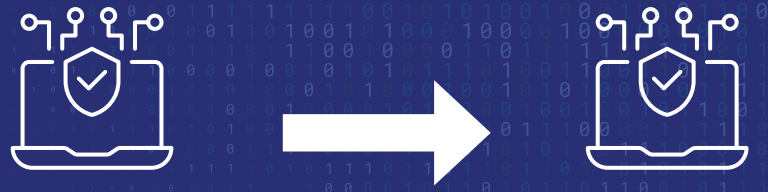
Cyber attacks are growing in volume, variety, and precision, and are a cause of significant business disruption.

Ransomeware | Supply Chain | Malware | Identity Theft | Host Software and Firmware Threats

54% of organizations have experienced an increase in cyber attacks in the past 12 months.

Source: IDC European Security Survey, 2022

2022 **CEO View: No1 Business Risk** **2024**



Cybersecurity Threats → **Cybersecurity Threats**

CEOs' Perspective:

- Cybersecurity threats the foremost business risk over the next two years.
- Recognize that security must keep pace with digital infrastructure investment.

Source: IDC WW CEO Sentiment Survey, 2022

For more information visit: www.amd.com/en/technologies/infinity-guard | www.amd.com/security

Protecting IT Infrastructure is a Priority

The shift to a digital-first strategy is driving strong IT infrastructure investment.

79%

of companies are looking to increase their spend on IT infrastructure through 2022 and into 2023.

Top 2022–2023 IT Infrastructure Priorities

1. improved security and compliance

2. enhanced agility and flexibility

3. Better automation and orchestration

Source: IDC Digital Infrastructure Survey, 2022

For more information visit: www.amd.com/en/technologies/infinity-guard www.amd.com/security

Cloud Adoption Accelerators and Road Bumps

84% of European organizations operating a combination of on-premises IT and public cloud infrastructure.

2022: How Cloud Technology is Supporting Organizations

1. Cost reduction
2. Modernization of applications
3. Platform to develop new products and services

2022: Top Trust Concerns Impacting Cloud Strategy

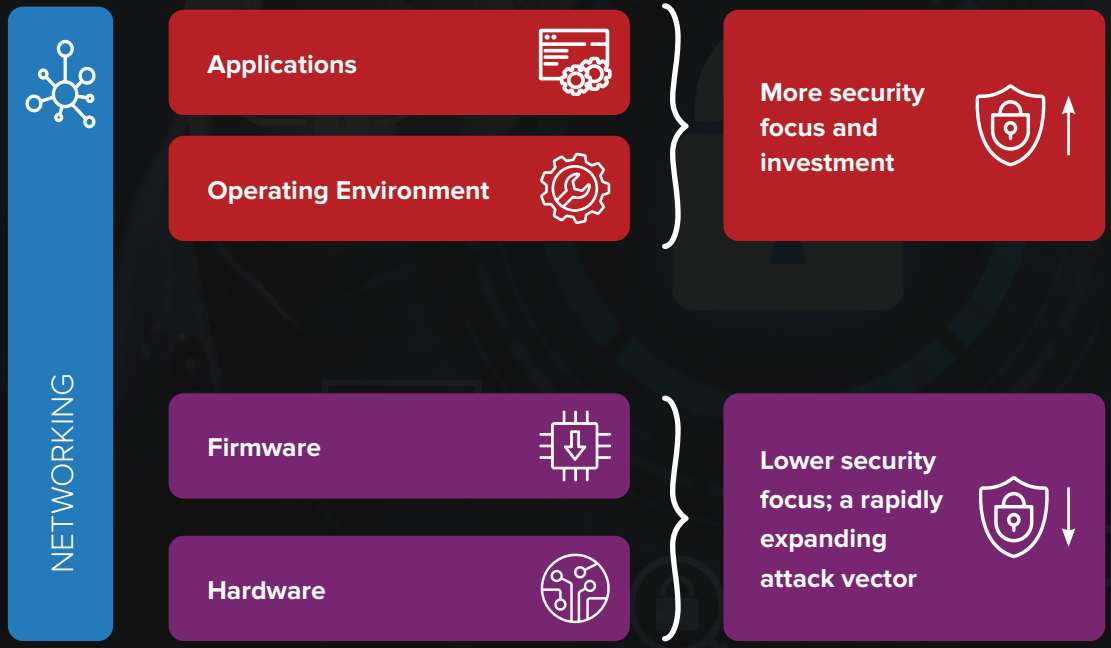
1. Security of data
2. Privacy compliance
3. Data sovereignty (Cloud Act/Schrems II)

Source: IDC European Multicloud Survey, 2022

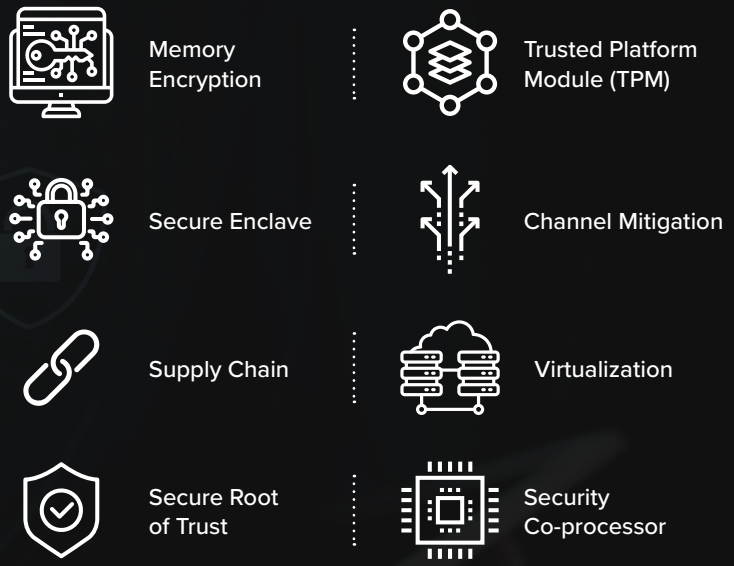
For more information visit: www.amd.com/en/technologies/infinity-guard www.amd.com/security

Trusted Computing: Hardware Platform Security

Protecting IT infrastructure requires a holistic approach that builds security from the processor to the cloud across hardware, firmware, and the operating system.



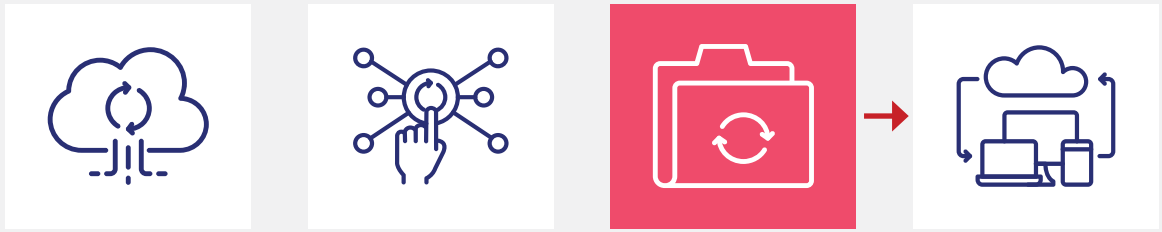
The right hardware security can help harden IT service delivery



For more information visit: www.amd.com/en/technologies/infinity-guard www.amd.com/security

Confidential Computing — Data-in-Use Hardware Protection

Closing the data security gap

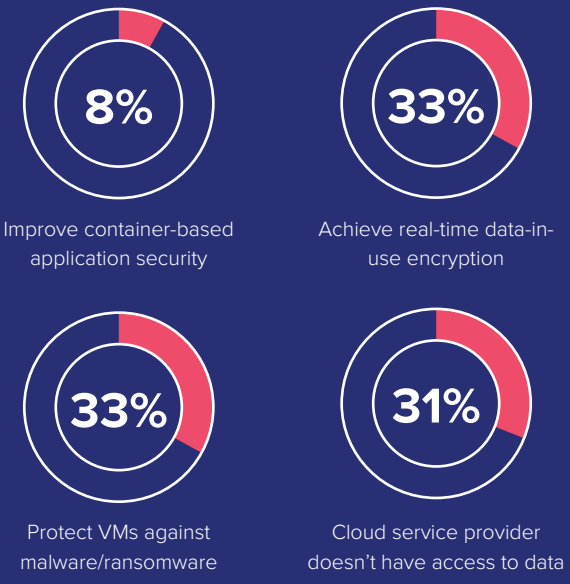


Traditional data encryption

End-to-end data encryption

Confidential Computing: Secure hardware-based computing environment that allows data and applications to be protected while being processed. The secure processor protects the encryption keys and ensures their secure use.

Top factors for adopting confidential computing in the cloud



Data and application inaccessible to third party hosting the CPU.

Source: IDC WW Cloud Survey, 2021

For more information visit: www.amd.com/en/technologies/infinity-guard www.amd.com/security