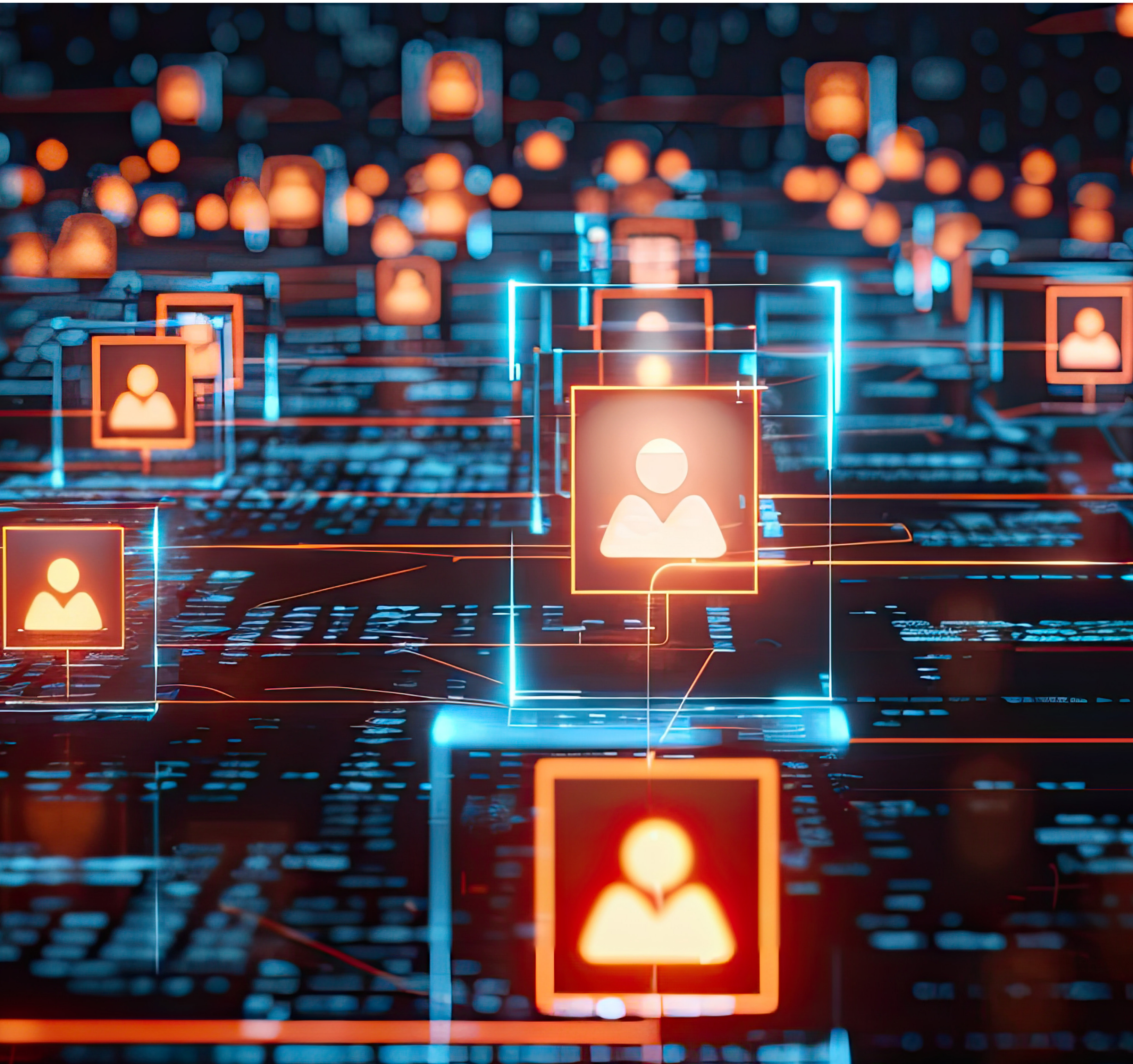
WHITE PAPER

Enabling Confidential Computing for Highly Secure Cloud Networking



Contents

Introduction

As enterprises continue to embrace cloud and virtualized environments to achieve scalability, cost efficiency and agility, the resiliency of their business depends on their networks maintaining continuous operations with high performance and secure delivery of data and applications from these locations, across the enterprise.

The flexibility and agility enabled by cloud heightens new threats that have grown in sophistication. Among these threats, malware targeting data-in-use has become a significant concern. IT security professionals and network engineers typically use traditional measures such as encryption during storage (data-at-rest) and transmission (data-in-transit), however this leaves a critical gap: the data in-use within the computing environment. Security concerns around this gap can prevent organizations from moving applications using sensitive data to the cloud to attain cloud computing benefits.

This white paper explores the necessity of protecting data-in-use and outlines how Riverbed RiOS 10 on SteelHead Cloud and SteelHead Virtual products enables confidential computing capabilities to address this challenge.

Resilient Networking

Resilient networking is the ability to maintain continuous, high-performance network operations even in the face of unexpected disruptions.
It involves:

- **Peak Performance:** Goes beyond just speed—it is about ensuring lightning-fast application responses and delivering critical data exactly where and when it is needed. By enhancing performance, it enables smooth, uninterrupted workflows, eliminates bottlenecks, and maximizes team productivity. Whether in the cloud, at the edge, or across your network, peak performance empowers real-time decision-making and keeps your business operating at its highest potential, no matter what the obstacles.
- **Secure Delivery:** Ensures secure data delivery from data storage—whether in the cloud or data center—straight to the edge. It safeguards data with encryption both at rest and in transit and makes possible near real-time data synchronization between central storage and the edge.
- **Visibility and AIOps:** Streamlines data management for rapid recovery and seamless restoration at the edge.

In essence, resilient networking solutions help businesses stay connected, secure, and efficient, no matter what challenges they face.

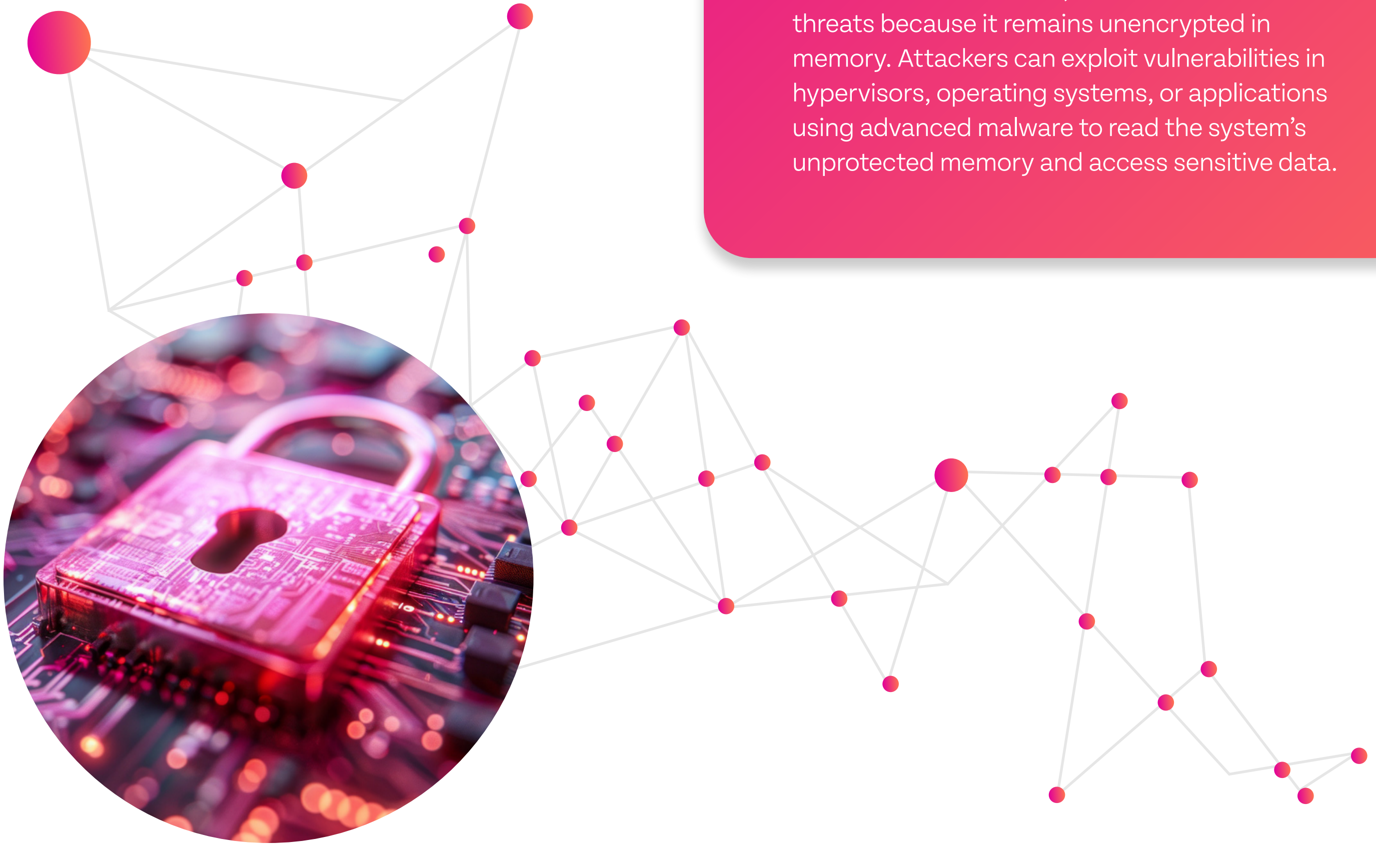
Data In-Use Vulnerabilities

The risk of unprotected data in-use is heightened in shared or multi-tenant cloud environments, where multiple virtual machines (VMs) share the same hardware infrastructure leveraging a hypervisor. The hypervisor is the software layer that enables virtualization, allowing multiple virtual machines to run on the same physical host. It sits between the physical hardware and the virtual machines, which means it is in a privileged position with direct access to the host's physical memory. VMs are logically isolated from one another. However, poor configurations, vulnerabilities in the hypervisor, or flaws in the memory management mechanisms can allow the hypervisor to access memory across VMs. If an attacker gains control of the hypervisor, they can potentially access the memory of any VM running on the host. These attacks are "hyperjacking." (See sidebar on page 5).

Where Is Data Vulnerable?

Data can be in one of three states: at-rest, in-transit, or in-use.

- **Data At-rest:** Refers to information that is not being accessed and is stored on some medium. Examples of data at-rest include files stored on servers, entries in databases, backup tapes, etc. Data at-rest is considered secure when it is properly encrypted.
- **Data In-transit:** refers to information that is traveling from a source to a destination over a communication channel. Examples of data in-transit include email exchanges, downloading/ uploading files, Cloud/SaaS applications, etc. Data in-transit is considered secure when it is transmitted over secured links for example, over TLS connections.
- **Data In-use:** refers to information actively processed in a system's memory. Unlike data-at-rest or data-in-transit, it is vulnerable to threats because it remains unencrypted in memory. Attackers can exploit vulnerabilities in hypervisors, operating systems, or applications using advanced malware to read the system's unprotected memory and access sensitive data.



Hyperjacking: VM Vulnerabilities

Hyperjacking is when a cyber attacker gains control over a VM's hypervisor; they can then control the entire VM server, allowing them to manipulate all aspects of the virtual machine and steal sensitive data. Malicious actors exploit vulnerabilities or misconfigurations in the hypervisor to gain unauthorized access and control over virtual machines (VMs).

Hyperjacking attacks are not just theoretical, in September 2022, Mandiant and VMware disclosed that a hacker group had successfully executed malware-based hyperjacking attacks, compromising the hypervisor to control virtual machines.

For example, memory scraping attacks and side-channel attacks allow malicious actors to extract sensitive information, such as encryption keys, personal data, or intellectual property, directly from the computing environment.

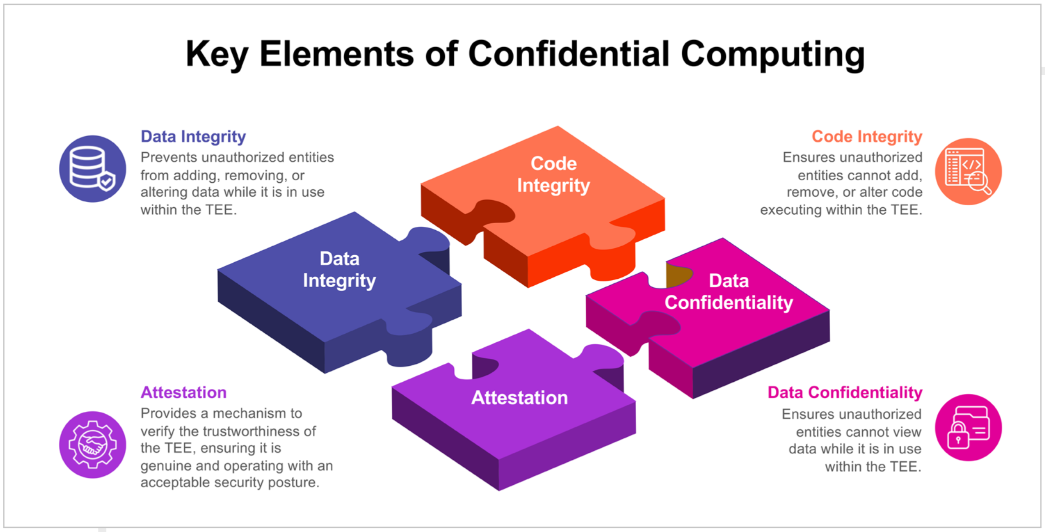
These risks underline the need for a robust mechanism to secure data during processing.

Confidential Computing

Confidential computing is an emerging paradigm designed to close the security gap for data-in-use. By enabling encryption of data while it is being processed, Confidential computing ensures that sensitive information remains protected even in the event of unauthorized access to system memory.

Key Elements of Confidential Computing

Confidential computing is built on several foundational technologies and principles that assure confidentiality of sensitive data.



Key Elements of Confidential Computing

Data Integrity
Prevents unauthorized entities from adding, removing, or altering data while it is in use within the TEE.

Code Integrity
Ensures unauthorized entities cannot add, remove, or alter code executing within the TEE.

Attestation
Provides a mechanism to verify the trustworthiness of the TEE, ensuring it is genuine and operating with an acceptable security posture.

Data Confidentiality
Ensures unauthorized entities cannot view data while it is in use within the TEE.

At its core, it relies on trusted execution environments (TEEs), which are secure areas within a processor or system, designed to safeguard data confidentiality via encryption even while it is being processed. By leveraging hardware-based isolation, TEEs are designed to offer strong protection against unauthorized access, even by privileged users such as system administrators, hypervisors, or malicious software, thus also guaranteeing data integrity. Last, but not least, attestation provides the mechanism to validate that the environment is secure and has not been tampered with before sensitive operations are executed.

Confidential Virtual Machines

A confidential virtual machine (CVM) is a type of virtual machine designed to protect the confidentiality and integrity of the data it processes, even when running on shared and potentially untrusted infrastructure. CVMs employ advanced hardware-based memory encryption and other security features to ensure that sensitive data remains protected throughout its lifecycle. This is achieved through a combination of TEEs, memory encryption technologies, and hardware isolation.

CVMs extend the concept of TEEs from individual applications or workloads to the entire virtual machine. This means that all components of the VM - its memory, CPU, and storage - are isolated from the underlying host system, hypervisor, and any other virtual machines running on the same physical hardware. This provides a secure environment where data and applications within the VM remain protected, even in multi-tenant scenarios such as public cloud environments. In these environments, a CVM ensures that sensitive workloads are shielded from the cloud provider and other tenants and maintains security even in the event of a hypervisor compromise.

Confidential virtual machines are supported by several leading cloud providers, including AWS, Microsoft Azure, Google Cloud Platform, and Oracle Cloud. These cloud platforms use various hardware technologies, such as Intel Trust Domain Extensions (Intel TDX), and AMD Secure Encrypted Virtualization (SEV), or cloud-specific technologies, such as Nitro, to provide memory encryption and isolation, protecting sensitive workloads even in multi-tenant environments. Additionally, popular hypervisors like KVM and VMware vSphere, also offer support for CVMs, making it possible to run confidential workloads across a variety of infrastructures.

Why Is Confidential Computing Essential for Resilient Networking?

Networking products such as accelerators, virtualized routers, firewalls, and SD-WAN appliances are critical components of modern infrastructure. These products often process sensitive data, including passwords, encryption keys, personal, or proprietary information. The exposure of such information can lead to severe consequences, including data breaches, compliance violations, service disruptions, and reputational damage.

RiOS 10: SteelHead Cloud and Virtual for Confidential Computing

Riverbed has introduced RiOS 10, an advancement of the RiOS software that has powered SteelHead Acceleration solutions across thousands of customers globally. RiOS 10 offers a comprehensive solution for enterprise application acceleration and high-scale data movement and powers SteelHead Acceleration solutions across thousands of customers globally. SteelHeads ensure resilient network connectivity, reduce costs, and improve user experience across distributed enterprise environments.

With RiOS 10, SteelHead Cloud and SteelHead Virtual products now provide support for confidential virtual machines offered by leading cloud providers and hypervisors, powered by Intel TDX to create trusted execution environments inside isolated memory regions called trust domains. RiOS 10 leverages attestation services to validate that the CPU is operating in a trusted state, and its provenance is confirmed, and that the confidentiality of the data is being upheld. Additionally, secure boot assures the system's software is legitimate and has not been tampered with. Together, these elements create a robust security model for managing sensitive data while it is being processed.

RiOS 10 provides enterprises with additional security measures to protect data-at-rest, supporting cyber security initiatives that enable them to comply with regulations such as GDPR, HIPAA, and other industry standards that mandate strict controls over the confidentiality and integrity of data.

In regulated industries, attestation allows organizations to prove to auditors, regulators, or third parties that their sensitive data is being processed in a secure environment, even when the infrastructure is managed by a third-party cloud provider.

Meet Compliance Requirements with Confidential Computing

As threats to data-in-use continue to rise, RiOS 10 provides a critical solution for securing sensitive operations in cloud and virtualized environments. By integrating confidential computing technologies, including confidential virtual machines and attestation services, RiOS 10 enables data confidentiality and integrity during processing.

By prioritizing the implementation of RiOS 10, organizations can confidently leverage the full potential of cloud and virtualized environments without compromising data security.

riverbed®

About Riverbed

Riverbed, the leader in AI observability, helps organizations optimize their users' experiences by leveraging AI automation for the prevention, identification, and resolution of IT issues. With over 20 years of experience in data collection and AI and machine learning, Riverbed's open and AI-powered observability platform and solutions optimize digital experiences and greatly improve IT efficiency. Riverbed also offers industry-leading Acceleration solutions that provide fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of market-leading customers globally – including 95% of the FORTUNE 100 – we are empowering next-generation digital experiences. Learn more at riverbed.com.