Google Cloud AMD EPYC Bullish

On the money: Digital asset exchange Bullish embraces Confidential Computing

Managing sensitive data in the cloud is a growing concern for organizations of all shapes and sizes. Privacy, security, and regulatory compliance are front stage center. One company that has faced critical technology choices is Bullish, a new global regulated exchange for cryptocurrency assets. It focuses on deep liquidity and automated market making primarily for institutional customers.

When Bullish began searching for a cloud technology platform to support its demanding business requirements, a few critical factors emerged. Performance couldn't be compromised. Dependability and availability were non-negotiable. Yet there was also a need for industry-leading security built on the latest authentication and verification protocols, including WebAuthn. Operating in a highly regulated industry and with its reputation squarely on the line, Bullish had to ensure that errors, glitches, and breaches wouldn't occur.

Top 3 benefits of confidential computing

- Privacy
- Security
- Regulatory compliance

As a result, Bullish turned to Confidential Computing from Google Cloud to be a part of its framework to deliver the demanding capabilities and features the financial services firm required. These included the ability to keep data encrypted while in memory, a highly secure collaboration framework, and maximum flexibility via Confidential virtual machines (VMs).

Bullish takes a stance for performance and strong security

Ensuring that data is available yet secure is an enormous challenge. For Bullish, this translated directly into a need for critical features, including always-on encryption, strong authentication and identity management, and the ability to track transactions and guarantee their integrity. Putting all these pieces in place from different vendors would have been incredibly difficult, costly, time consuming, and added significant complexity to Bullish's environment.

Bullish began searching for a platform that would deliver high flexibility and scalability along with a Defense in Depth and Zero Trust security framework.

Google Cloud AMD EPYC Bullish

"What sets us apart is that we look to combine the best of traditional exchange elements with decentralized finance (DeFi) innovation. An example of this is our automated market maker that allows Bullish to provide our customers with greater liquidity to trade along with the opportunity to earn a return on their digital assets," explains Matt Presson, lead security architect for Bullish.

When Bullish began defining its requirements, it recognized a need for a high-performance cloud environment capable of protecting personally identifiable information (PII) and transactional integrity throughout its blockchain-based platform. "Security had to be a critical part of every layer of our architecture, from the Web front end to our APIs and middleware along with all the infrastructure that supports our exchange," Presson explains.

What's more, these protections had to touch every workload, from deposit to withdrawal. They also had to support a demanding array of critical requirements, including always-on encryption, a fully verifiable execution stack, the ability for Bullish to provide and control its own images and verification keys, rollback protections, cryptographically verifiable software and services, and the ability to default to a fail-secure state.

Confidential Computing was a direct match. It could embed security within the entire product lifecycle—without the need to rewrite or rework software code. Among the key features that supported Bullish's needs was secure encrypted virtualization by an AMD EPYC™ CPU chip that doesn't allow data extraction from the hardware through rootkits and bootkits. In fact, this represented a level of security that wasn't available on any other cloud platform.

"We needed a solution that could go beyond conventional encryption at rest and encryption in transit. We needed to protect data in use," Presson notes. "This was a critical piece of the puzzle because when we took a close look at attacks on organizations that have a lot of sensitive data, especially those within the crypto space, it was apparent that if malware gets into the system, it could potentially extract sensitive data out of memory. For us, this could be our customers' KYC/AML data or transaction data that could allow someone to front-run the market."

> Security had to be a critical part of every layer of our architecture, from the Web front end to our APIs and middleware along with all the infrastructure that supports our exchange.
>
> — Matt Presson, lead security architect, Bullish

A new era of secure computing emerges

Google Cloud's Confidential Computing platform has delivered great value for Bullish. The company can now verify the security of its entire execution stack. "We not only wanted to protect our application within the execution environment, but also everything from the boot loader to the operating system and all of our code running on top of that," Presson explains.

As a result of Confidential Computing, Bullish gained a high level of confidence in the protections surrounding the digital assets in its custody.

"We have the ability to know and trust everything running in our environment, but we're also confident that nothing outside of what we know and trust can somehow execute. We have a verifiable, trusted boot state, a verifiable operating system and verified software. What's more, if one of these protections somehow failed to hold up to an attempted hack or attack—whether it's a piece of malware that somehow enters the system or a malicious insider—the computing environment will default to the secure state we require." Presson says.

These advanced security features—which include a variety of isolation and sandboxing techniques as well as data invisibility for everyone except the holder of the data—are baked into the Confidential Computing framework. The ability to encrypt the memory content of VMs in use and create Confidential GKE Nodes is critical. The end result is incredible security value.

"The environment delivers confidentiality, enhanced innovation and the ability to lift-and-shift workloads securely," Presson notes. "It's a critical piece of our overall security architecture."

To learn how Google Cloud, AMD and confidential computing can protect your sensitive data, visit us at cloud.google.com/confidential-computing