Case Study

Intel® Xeon® Processors

Hypori Lets U.S. Military Personnel Use Their Own Mobile Devices in Compliance with Government Security Mandates

Supported by backend bare metal Amazon EC2 instances and 4th Gen Intel® Xeon® processors, Hypori provides a cost-effective solution to virtualize work devices, keeping work-related data protected.

Solution Ingredients

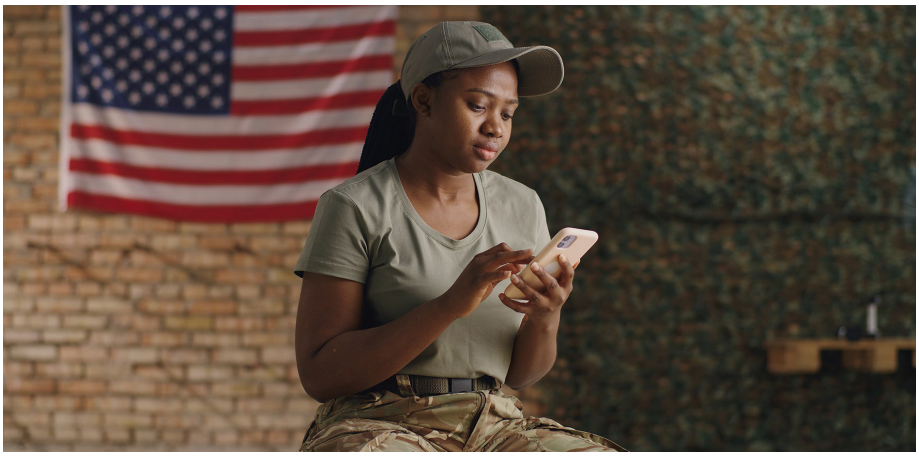
- Amazon EC2 R5 bare metal instances
- Intel® Xeon® processors
- Intel® QuickAssist Technology (Intel® QAT)

Executive Summary

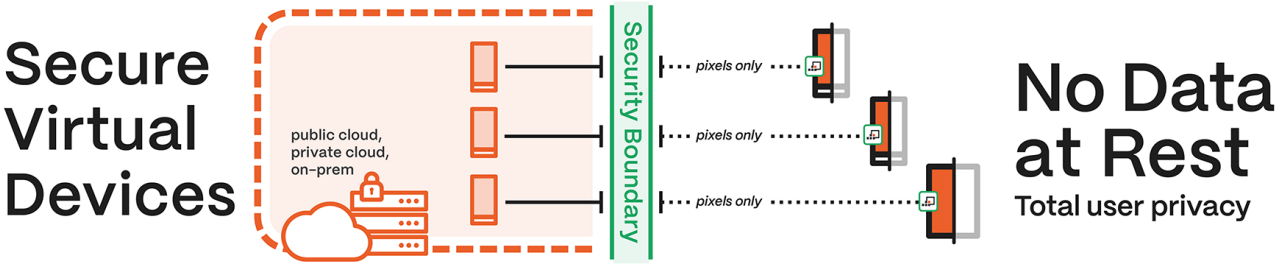
Government bodies and some private sector companies, like healthcare providers or defense contractors, must adhere to specific security mandates to protect sensitive or secret information. In the past, these regulations disqualified personal phones or Windows laptops from use in a work setting. Hypori changes that by providing a secure virtual workspace separate from the users' private information and content. User's personal data and applications are saved on the device, and employers cannot access that private information. Instead of storing work-related information on the device, however, Hypori transmits encrypted pixels that emulate a device's on-screen experience. All the work-related data remains secure in Amazon R5 bare metal instances supported by Intel® Xeon® processors. Hypori's benchmark testing found that 4th Gen Intel Xeon processors offered 2.5 times faster data compression and decompression compared to the previous generation. The solution also provided a 15 percent improvement in user capacity without increasing hosting costs.[1]

Challenge

Hypori customers, like branches of the U.S. Military, defense contractors, and healthcare providers like the Alliance Clinical Network, need to lock down



U.S. Military branches like the Army, Air Force, and Space Force, and healthcare companies like the Alliance Clinical Network (ACN) find multiple benefits from Hypori running on AWS instances featuring 4th Gen Intel® Xeon® processors.



job-related information and applications to ensure sensitive data remains secure. Applications and data stored on a physical device are at risk if the hardware is lost, stolen, or compromised. On the other hand, employees want to use their device of choice but not give their employer access to personal information. Hypori addresses both requirements.

> "Hypori makes personal device programs a reality without compromising security or user privacy, which is why it's the most widely deployed bring-your-own-device solution across the DoD. Leveraging Amazon bare metal instances and Intel technologies, Hypori delivers a secure, encrypted virtual workspace with minimal latency—striving to achieve the perfect balance between performance, privacy, and security."
>
> *—Jared Shepard, Hypori President & CEO*

Solution

The Hypori application addresses these challenges by creating a virtualized workspace that mimics the native user interface. Hypori continues to capture a device's touch and sensor data, so the device behaves like it would off-the-shelf. However, the device becomes a mere "window" for business use, so all work-related information remains secured in Amazon EC2 R5 bare metal instances supported by Intel Xeon processors.

A user's virtual workspace is encrypted on the backend to meet military and healthcare-related security standards. Built on a zero-trust architecture, Hypori is IL4/IL5 certified, HIPAA and GDPR compliant, NIAP Common Criteria certified, and meets FedRAMP High "In Process." Hypori also adheres to DFARS for protecting CUI based on NIST 800-171.

When a user accesses job-related content through the virtual workspace, Hypori sends and receives encrypted pixel data that visually simulates a device's interface. Hypori provides a near-native user experience while maintaining complete separation between work-related information and personal device data.

Working closely with Amazon and Intel, Hypori optimized Amazon C5 bare metal instances to maximize performance and minimize user latency. Intel® QuickAssist Technology (Intel® QAT), built into Intel Xeon processors, provides an integrated workload accelerator that offloads resource-intensive processes like data compression and encryption from the CPU cores. In doing so, Intel QAT helps minimize latency and maximize Hypori's virtual workspace performance.

Hypori allows employers to cut off access to the virtual workspace so no work-related information is compromised if a user's phone is damaged, lost, or stolen. Administrators can also use Hypori to configure a new virtual workspace that is accessible from any mobile device in minutes.

Results

U.S. Military branches like the Army, Air Force, and Space Force, and healthcare companies like the Alliance Clinical Network (ACN) see multiple benefits from Hypori with gen-over-gen upgrades. For example, after moving from 3rd to 4th Gen Intel Xeon processors, benchmark tests showed 2.5 times faster data compression and decompression and a 15 percent increase in user capacity without increasing hosting costs.[1]

As a proven solution running on trusted hardware from Amazon and Intel, the Hypori solution can be implemented rapidly by government and private companies without requiring extensive prototyping and testing before use in production.

Another benefit is Hypori's cost-effectiveness. Since employees can use personal devices for work, Hypori customers do not need to supply their staff with secondary devices or an associated telecommunications plan. Backend systems management and fast provisioning can also reduce the volume of user support services yearly.

Key Takeaways

- The Hypori app allows public and private sector employees to use their devices and keep personal information private while enabling secure virtual access to work-related apps and data in the cloud.
- Virtualizing users' mobile devices using backend Amazon bare metal instances and Intel Xeon processors removes risks associated with locally stored, job-related information without altering the familiar device interface.

- Hypori mimics a fully functional handheld device by transmitting encrypted pixels—thereby generating screen images—rather than moving actual data that could be intercepted or stolen.
- The complete separation of the virtual workspace means malware from a compromised physical device cannot infiltrate the virtual device. This separation also protects against data spillage and breach.
- Hypori is easy to implement at scale with simple QR-code provisioning. It relieves IT-admin work and reduces costs by eliminating the need for secondary work phones and associated data plans.

For more information

Learn more about Hypori.

Explore Intel Xeon Processors.

Check out Amazon EC2 R5 bare metal instances.

intel + aws

[1] Benchmarks performed by Hypori comparing performance on their current AWS instance with 4th Gen Intel Xeon processors and their previous AWS instance with 3rd Gen Intel Xeon processors.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.
For workloads and configurations visit www.Intel.com/PerformanceIndex. Results may vary.
Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.
Your costs and results may vary.
Intel technologies may require enabled hardware, software or service activation.
© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

102024/RJMJ/JS/PDF PleaseRecycle 362531-001US