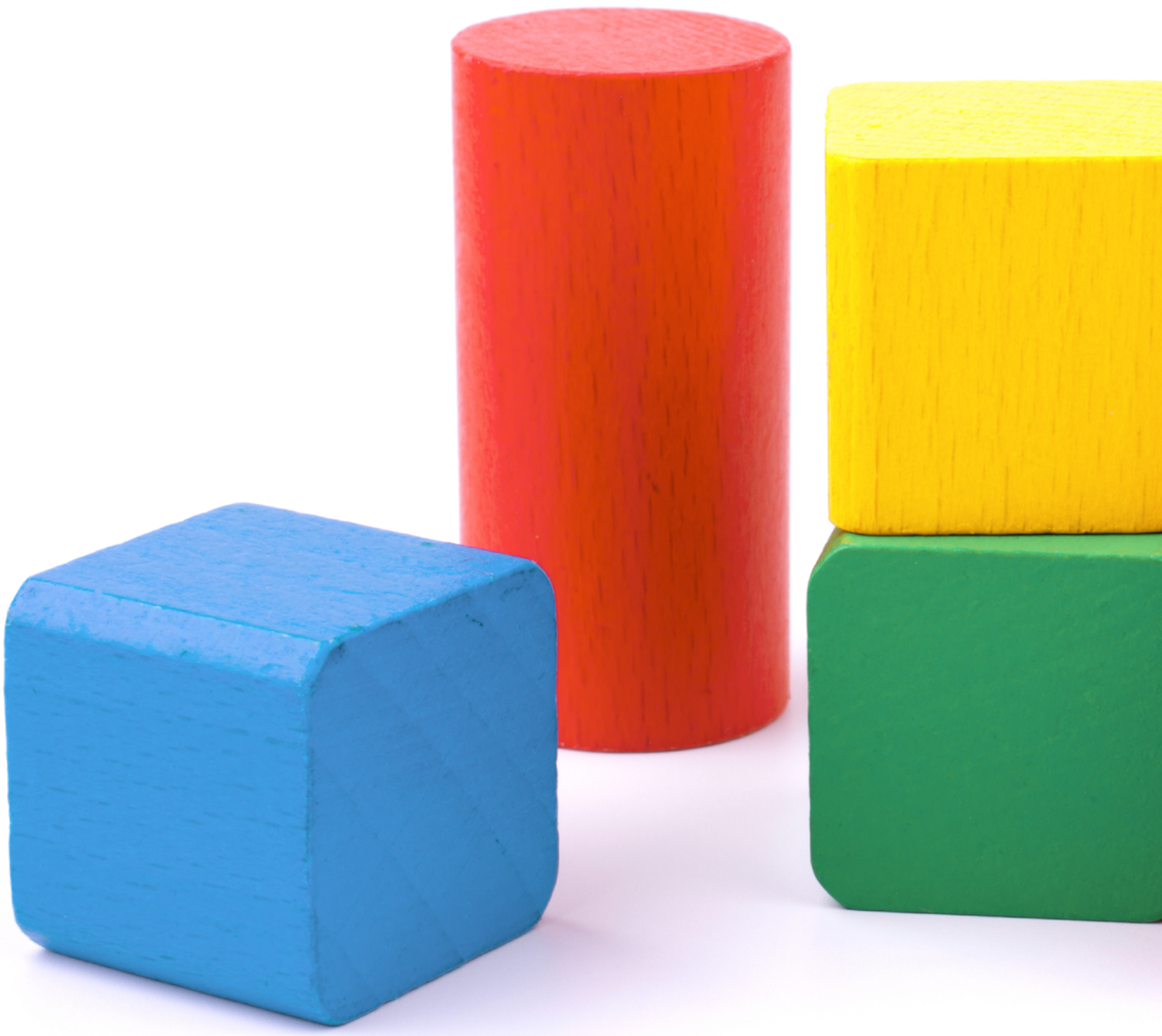
AMD

Google Cloud

Build bold: Innovate in the cloud with confidence

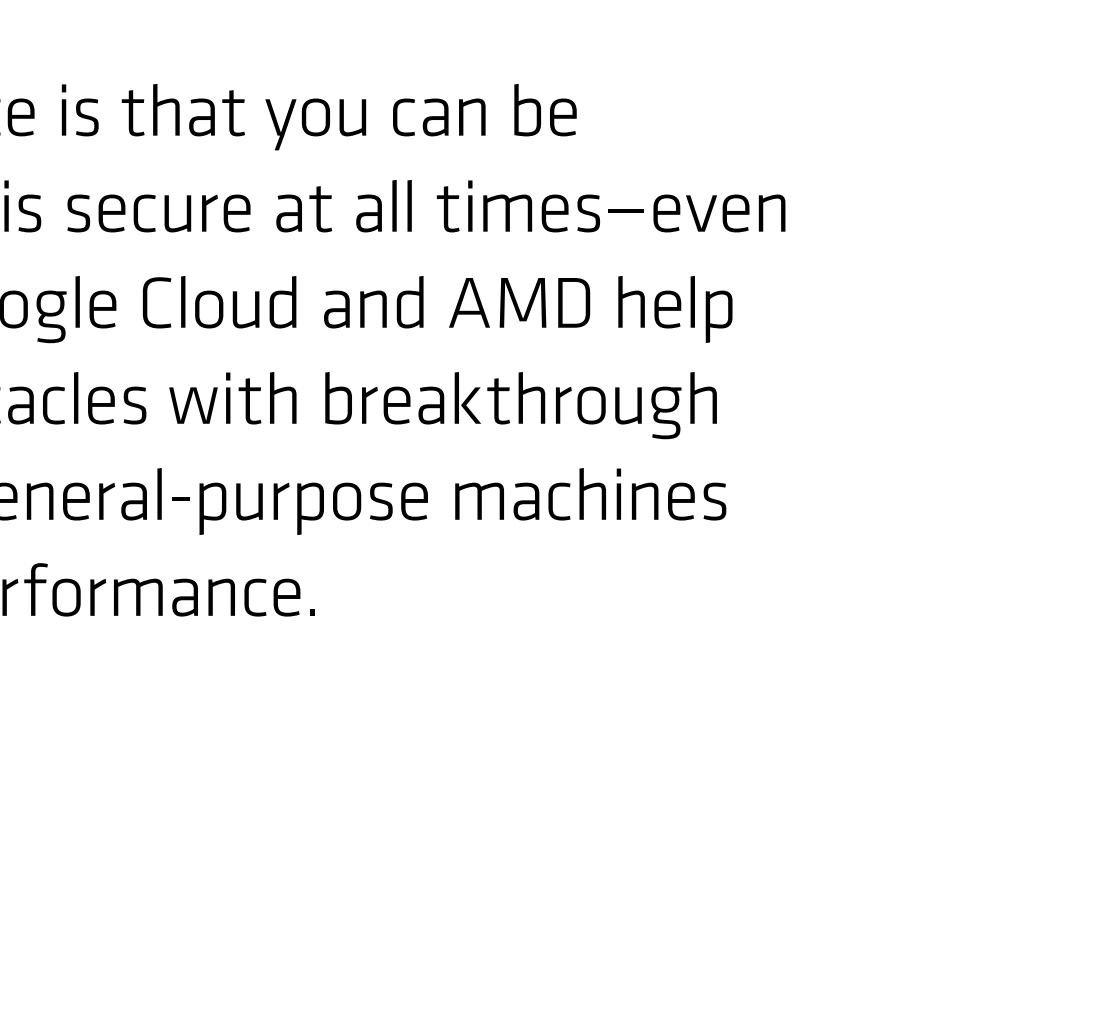
Get exceptional flexibility
and breakthrough data security
with Confidential VMs.



Challenges to building bold

Developing in the cloud hasn't been without its obstacles. Today's widely varied workloads—driven by digital innovation—demand a balance of performance and cost, without sacrificing flexibility.

Of the utmost importance is that you can be confident that your data is secure at all times—even when it's in use. Now, Google Cloud and AMD help you overcome those obstacles with breakthrough cloud capabilities using general-purpose machines that balance price and performance.



“Confidential Computing solves an issue that enterprises specifically have around trust in memory–namely that memory cannot be seen or used by a cloud provider. Three key use cases that can immediately benefit from this technology include edge computing, external key management, and in-memory secrets.”

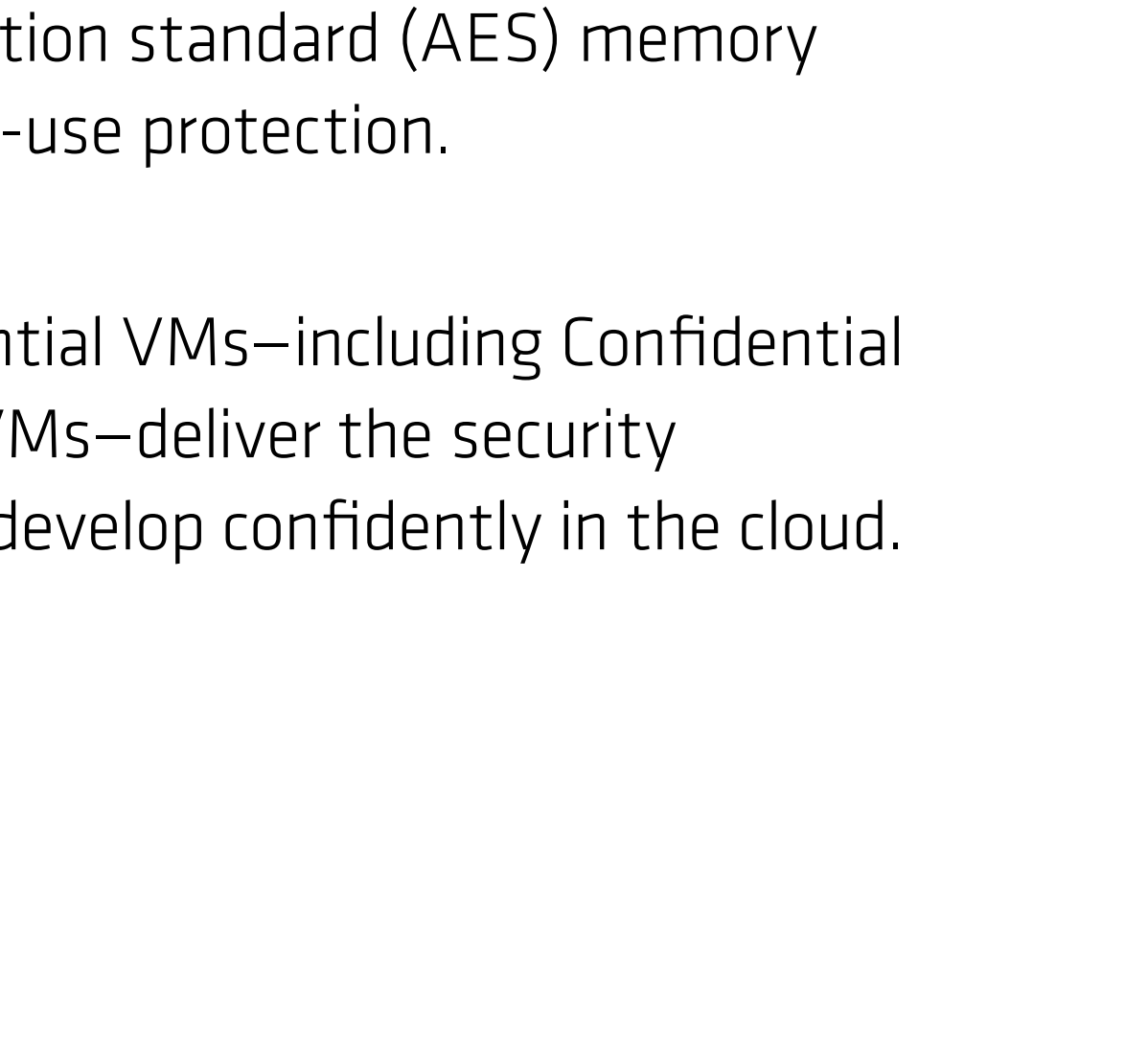
– Solomon Cates, Principal Technologist, CTO Office, Thales Cloud Security[1]

[1] Porter N, Lugani S, Better together: Expanding the Confidential Computing ecosystem, December 2020.

Open up new possibilities

Confidential VM (Virtual Machine) instances, powered by AMD EPYC™ processors, help secure your data in virtualized environments. AMD EPYC™ processors feature AMD Secure Encrypted Virtualization (SEV) with advanced encryption standard (AES) memory encryption for data-in-use protection.

Google Cloud Confidential VMs—including Confidential Computing and N2D VMs—deliver the security features you need to develop confidently in the cloud.



“Working closely with AMD, SUSE added upstream support for AMD EPYC™ SEV processors to the Linux kernel and was the first to announce Confidential VM support in SUSE Linux Enterprise Server 15 SP1, available in the Google Cloud Marketplace. These innovations allow our customers to take advantage of the scale and cost savings of Google Cloud Platform and the mission-critical manageability, compliance, and support from a world-class Linux support team, SUSE.”

– Dr. Thomas Di Giacomo,
Chief Technology and Product Officer, SUSE[2]

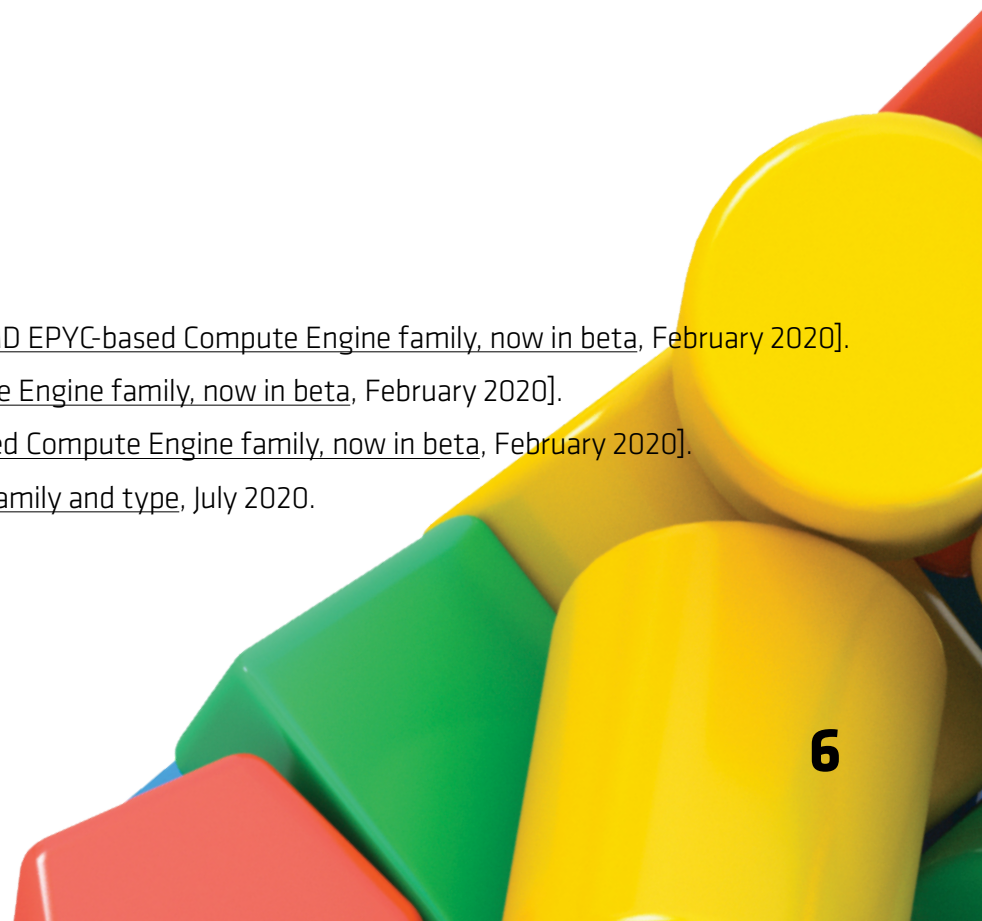
[2] Porter N, Lugani S, Better together: Expanding the Confidential Computing ecosystem, December 2020.

Get optimized performance *and* price

N2D VMs powered by AMD EPYC™ processors deliver:

- **Up to 39% better processing performance[3]**
- **Up to 13% lower costs[4]**
- **Up to 70% higher memory bandwidth for intensive workloads[5]**
- **100% performance improvement on a variety of representative benchmarks, including Gromacs and NAMD[6]**
- **The highest core count and memory of any general-purpose Compute Engine VM[7]**

That all adds up to cost-efficient, secure computing that helps you drive innovation and handle heavy workloads like crash analysis, financial modeling, reservoir analysis, and more.



[3-4] Compared to N1 and N2D non-confidential VMs [Vallejo C, New AMD EPYC-based Compute Engine family, now in beta, February 2020].

[5] Compared to N1 instances [Vallejo C, New AMD EPYC-based Compute Engine family, now in beta, February 2020].

[6] Compared to N1-standard-96 vCPUs [Vallejo C, New AMD EPYC-based Compute Engine family, now in beta, February 2020].

[7] Youssef H, Compute Engine explained: Choosing the right machine family and type, July 2020.

Breakthrough data security: Google Cloud Confidential VMs powered by AMD EPYC™ processors

More options, more flexibility

With Confidential VMs, you have more configuration choices—from handling everything from general-purpose workloads that require a balance of compute and memory to big compute workloads driven by memory bandwidth. That makes Confidential VMs a good fit for a wide range of use cases across many industries.

Confidential VMs also unlock computing scenarios that weren't previously possible. That includes helping your organization share confidential data sets and collaborate on research in the cloud, all while preserving confidentiality.

You can also use Confidential VMs to create custom machine types that best fit your workload. That helps you avoid unnecessary costs that come with stranding resources.

“

Confidential Computing is one key approach to extend security from on-premises deployments into the cloud. Google’s announcement of Confidential VMs is an example of how customers can further secure their applications and workloads.”

– Mike Bursell, Chief Security Architect, Red Hat[8]

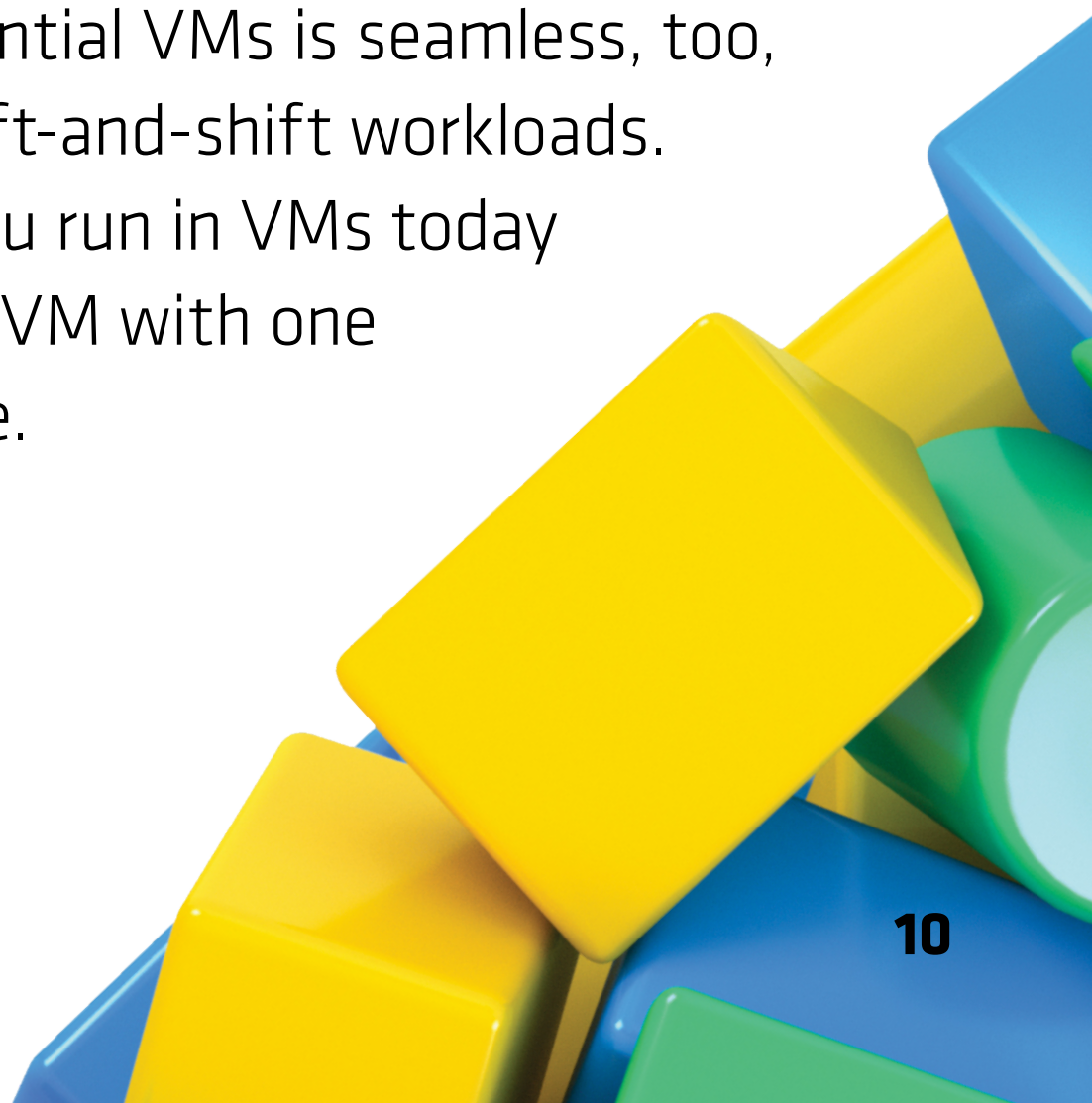
[8] Porter N, Lugani S, Better together: Expanding the Confidential Computing ecosystem, December 2020.

Experience next-level security features in the cloud

Confidential VMs help you protect your most sensitive data in the cloud—even while it's being processed—leveraging AMD SEV technology. That means your data stays encrypted, even while it's in use, indexed, queried, or trained on.

And, building on the protections offered by Shielded VMs against rootkits and bootkits, Google Cloud Platform (GCP) Confidential VMs also deliver protection against advanced persistent attacks. That helps ensure the integrity of the operating system you choose to run in your Confidential VM.

The transition to Confidential VMs is seamless, too, with confidentiality for lift-and-shift workloads. And all GCP workloads you run in VMs today can run as a Confidential VM with one checkbox—it's that simple.



“Confidential VMs will help tremendously accelerate our customer migrations to the cloud on their hybrid cloud digital transformation journey. This technology opens up new areas of migration opportunities for legacy on-premises workloads, custom applications, as well as Private and Government workloads that require the utmost security and compliance requirements once considered not cloud-ready in the past.”

– Dr. Thomas Di Giacomo,
Chief Technology and Product Officer, SUSE[9]

[9] Porter N, Lugani S, Better together: Expanding the Confidential Computing ecosystem, December 2020.

Empowering innovation across industries

Confidential VMs can deliver the flexibility and security that open the door to innovations that can change the world.

Analytics
Support intensive workloads with a wide range of high-performance compute and memory configurations that support data integration, data laking, and data warehousing.

Financial services
Innovate with data and adapt to evolving customer demands without sacrificing security and compliance.

Healthcare
Transform medicine by delivering a new level of patient care anywhere and accelerate genomics research to discover new treatments faster.

Manufacturing
Automate quality control processes and drive application modernization across on-premises and cloud infrastructures.

Media and entertainment
Deliver content to multiple streaming platforms with compute and memory configurations that support innovative broadcast modernization initiatives.

Retail
Apply artificial intelligence and machine learning for deeper insights and engaging customer experiences while helping ensure sensitive customer data in the cloud is always protected.

Ready to learn how Confidential VMs can help you innovate with confidence?

Schedule my call