EU data protection and the data economy

Improve your ability to meet and exceed core security and data privacy compliance requirements within the European Union.

Contents

Introduction

Protecting data is our ongoing commitment to EU customers

AWS is here to support Europe's digital future. We understand that your most critical and sensitive assets are your data. Earning your trust to protect those assets is the foundation of our business.

We offer the most comprehensive set of services, tooling, and resources to help you to protect, use, and – when appropriate – share your data. We provide technical, operational, and contractual measures needed to protect that data. You create and manage your data, control how your data is used, determine who has access, and how it is encrypted. AWS delivers all these capabilities with the most flexible and secure cloud computing environment available today.

We continually monitor the evolving privacy, regulatory, and legislative landscape. Coupled with active conversations with our customers, we identify changes and determine what tools you may require to meet your compliance needs.

Maintaining customer trust is an ongoing commitment and we will always inform you of the privacy and data security policies, practices, and technologies that we've put in place as they evolve.

At AWS, we work hard to prepare for the future and we want you to be well-prepared, too.

AWS has achieved internationally-recognised certifications and accreditations that demonstrate compliance with rigorous international standards, including: ISO 27017, ISO 27018, ISO27701, SOC 2, Cloud Computing Compliance Controls Catalog (C5, Germany), and Hébergement de Données de Santé (HDS, France).

Learn more ›

The global data economy

In the European Union (EU) and across the world, we work with our customers to bring their most sensitive and regulated data securely to the cloud. Thousands of the EU's fastest growing start-ups, largest enterprises, and governments are using AWS to innovate faster and to better serve their customers and EU citizens. The ability to collect, improve, learn from, and share data is a critical part of this.

You can facilitate this through both private and commercial data via AWS Data Exchange and also with open data via the Registry of Open Data. With data exchange, healthcare providers, for example, can better plan clinical trials and research new drugs that have the potential to improve patient lives.

> **"Pressing population health problems of today require not only modern analytic techniques, but also access to new trustworthy sources of data. Working with AWS Data Exchange enabled us to apply our advanced machine learning and comparative effectiveness techniques to contemporary sources of data our clinical researchers have not used before. These innovations have led to several novel studies and grant applications with new partners."**
>
> **Dr. Michael Pencina PhD**
> *Vice Dean for Data Science*
> *and Information Technology,*
> *Duke University School of Medicine*

Collaborate and share

Our experience has taught us that all stakeholders want to share and consume the same accurate data as a single source of truth. They want to be able to query live views of the data concurrently, without any performance degradation, and access the right information exactly when it's needed. For example, Amazon Redshift, the first data warehouse built for the cloud, has become the go to data warehouse component for many of our customers' data management architecture.

Amazon Redshift users can share data with users in an AWS account, but to share data and collaborate with other AWS accounts, they would previously have needed to extract it from one system and load it into another. But not anymore. We recently introduced cross-account data sharing to do exactly this, making it possible for you to share data across organisations and collaborate with external parties while still meeting compliance and security requirements.

Get insights from your data

AWS also provides the broadest and most cost-effective set of analytics services to help you gain data insights even faster. Each analytics service is purpose-built for a wide range of use cases including interactive analysis, big data processing, data warehousing, real-time analytics, operational analytics, dashboards, and visualisations.

Scalability and availability

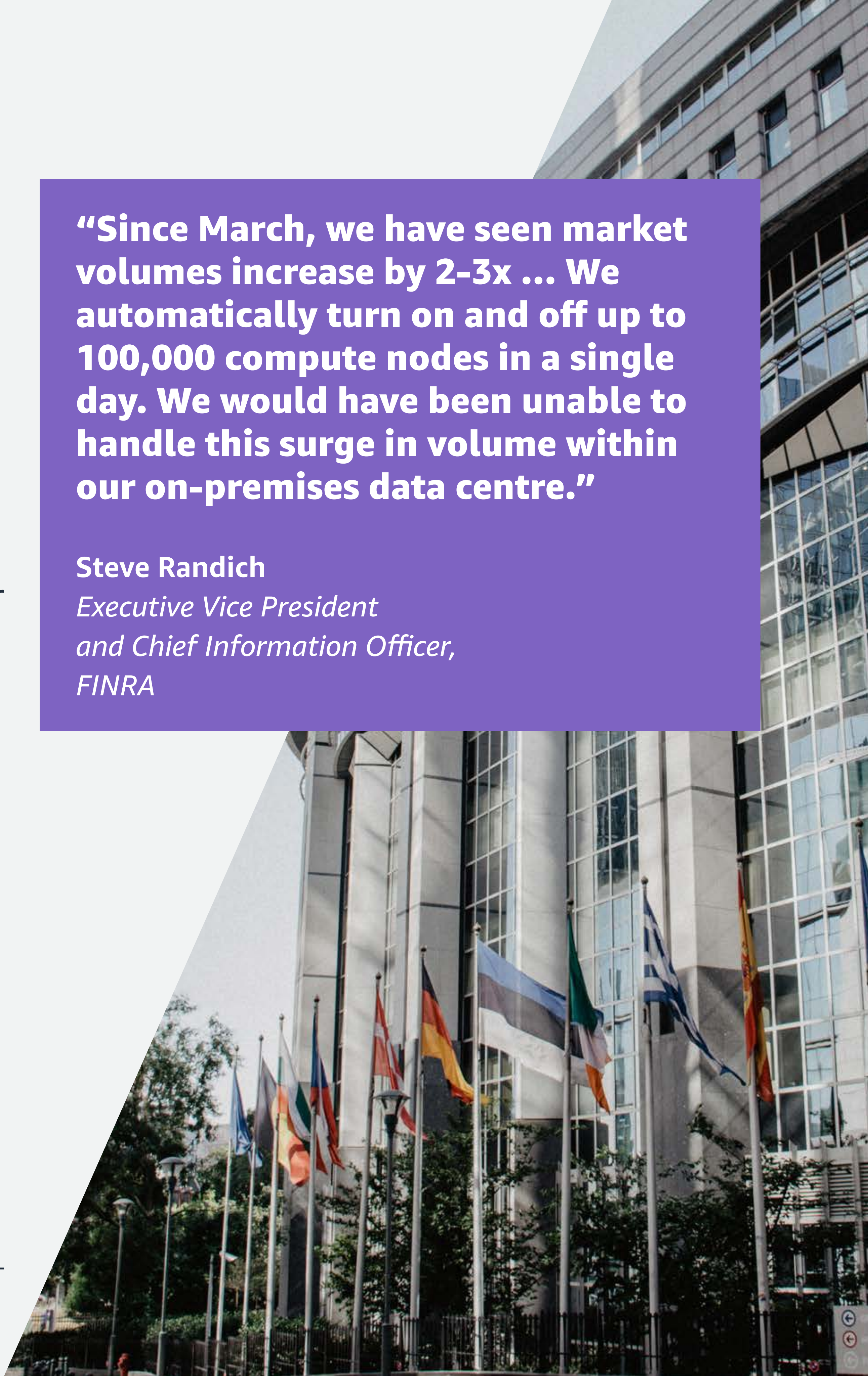
The AWS Cloud allows you to scale and innovate while maintaining a secure environment. Cloud security is a Shared Responsibility between AWS and the customer; AWS has the responsibility for “security of the cloud” and the customer is responsible for “security in the cloud.” AWS provides a wide range of services, capabilities, and features that can help customers implement their security responsibilities.

As a customer, you benefit from data centres, a global private and encrypted network, and hardened cloud services designed to meet the requirements of the world’s most security-sensitive organisations. Our infrastructure is custom-built for the cloud and monitored 24/7/365 to help protect the confidentiality, integrity, and availability of your data. It is designed to provide an extremely scalable, highly reliable platform you can use to deploy applications and data quickly and securely.

This means you get a resilient, highly secure and scalable infrastructure without the capital outlay and operational overhead of a traditional data centre. Solutions such as AWS Auto Scaling monitor your applications and automatically adjust capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it’s easy to set up application scaling for multiple resources across multiple services in minutes.

You can achieve security in the cloud with greater scalability and speed than your on-premise data centres, without the upfront expenses and with much lower operational costs than managing your own infrastructure. In the cloud, there are no physical servers or storage devices to manage – software-based security tools monitor and protect the flow of information into and of out of your cloud resources. Protecting yourself from ransomware, for example, is a heavy burden on premises. In the cloud you can protect yourself more efficiently and automatically using strong access management boundaries and automatic data back up features, which can minimize the impact and speed up recover times dramatically.

> **“Since March, we have seen market volumes increase by 2-3x … We automatically turn on and off up to 100,000 compute nodes in a single day. We would have been unable to handle this surge in volume within our on-premises data centre.”**
>
> **Steve Randich**
> *Executive Vice President*
> *and Chief Information Officer,*
> *FINRA*

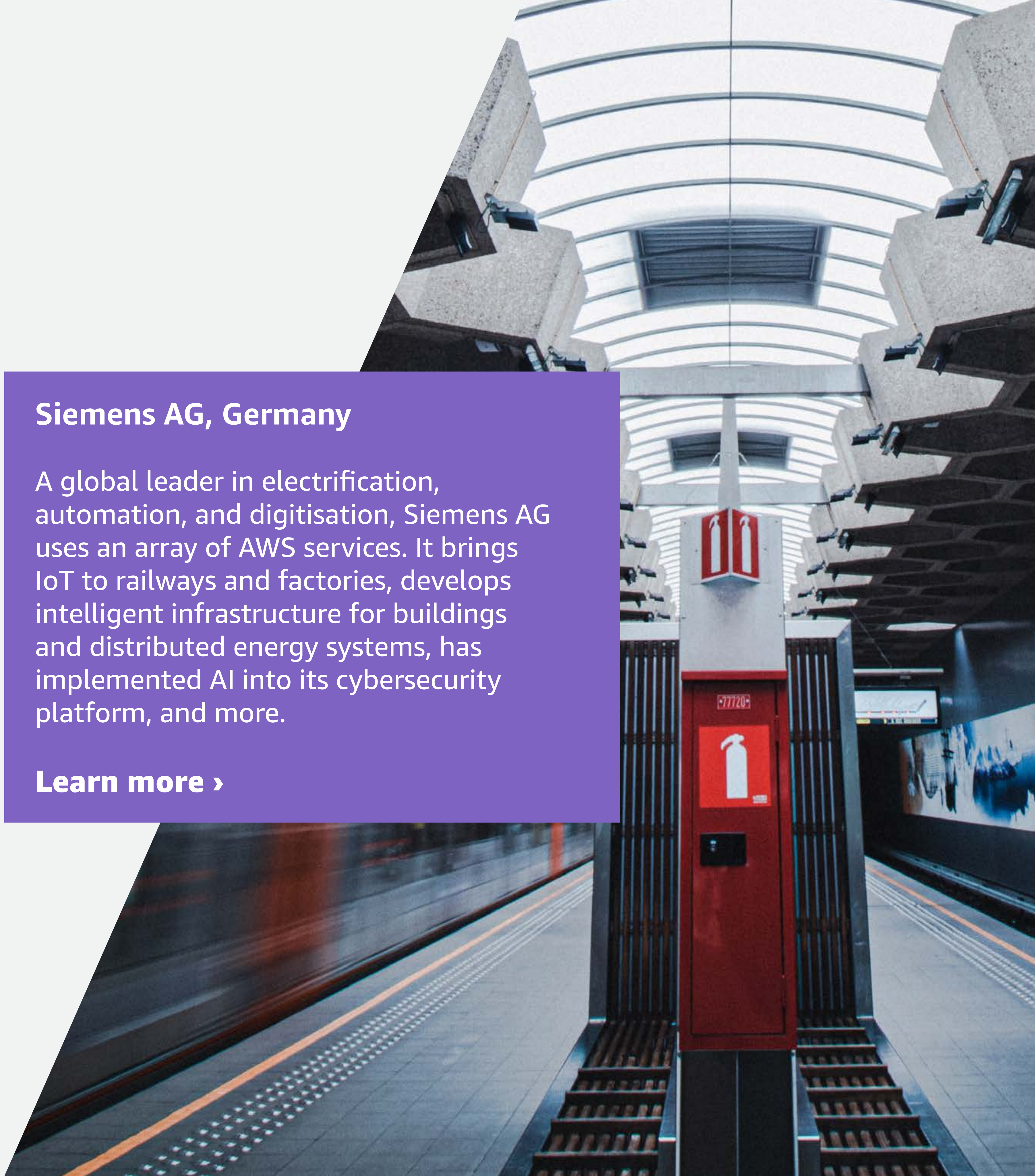


AWS enables and invests in the EU data economy

Sharing data is key in the new economy. The challenge is how to leverage the data distributed by a variety of owners. By using the cloud, you can securely share datasets without the need to copy, without heavy integration projects, and without increasing IT security exposure.

> **“We’re here to help our European customers and partners accelerate cloud-driven innovation in Europe – to compete at home and globally.”**
> **– Max Peterson,** *Vice President of International Public Sector, AWS*

The use of cloud computing services, big data and Artificial Intelligence (AI) will be instrumental to growing the EU data economy. As you plan to navigate this transformation and the new regulations, we’re here to help you – our European customers and partners – accelerate cloud-driven innovation, enabling you to compete both at home and globally. Organisations trust AWS to help them address their digital transformation challenges, and they choose our services and solutions because of our extensive functionality, our large and growing community of customers and partners, and our world-renowned operational and security expertise. They understand that all of this helps them innovate faster, especially in new areas such as Machine Learning (ML) and AI, the Internet of Things (IoT), and Serverless Computing.



Siemens AG, Germany

A global leader in electrification, automation, and digitisation, Siemens AG uses an array of AWS services. It brings IoT to railways and factories, develops intelligent infrastructure for buildings and distributed energy systems, has implemented AI into its cybersecurity platform, and more.

Learn more ›

We respect your data sovereignty

Security is our top priority.

Using AWS, you gain the control and confidence you need to run your business using the most flexible and secure cloud computing environment available today. As noted, you benefit from data centres, a global private and encrypted network, and hardened cloud services architected to protect your data and workloads. You can improve your ability to meet core security and compliance requirements, such as data residency, protection, and confidentiality, with our comprehensive services and features.

Confidential computing

In the past year, there has been an increasing interest in the phrase *confidential computing* in the industry and in our customer conversations. We've observed that this phrase is being applied to various technologies that solve very different problems, leading to confusion about what it actually means. With the mission of innovating on behalf of our customers, we want to offer you our perspective on confidential computing.

At AWS, we define confidential computing as the use of specialised hardware and associated firmware to protect customer code and data during processing from outside access.

You can learn more about this by reading our latest blog post on the subject: [Confidential computing: an AWS perspective]().

Portability

We support numerous industry initiatives – including the data driven economy envisioned by GAIA-X – that define standards for the next generation of Data-Economy-Platforms, such as data lakes or industrial data spaces. GAIA-X is an initiative that aims to bring together representatives from business, science, and politics to help define these standards for the next generation of data infrastructure. This includes an open, transparent, and secure digital environment where data and services can be made available, collated, and shared with trust.

We also support EU data protection standards for cloud infrastructure services such as the Cloud Infrastructure Services Providers in Europe (CISPE) Code of Conduct and the Switching Cloud Providers and Porting Data (SWIPO) Code of Conduct. With AWS Cloud, portability is made easier and less expensive than traditional IT. We're able to achieve this thanks to a large set of technical choices that includes the use of open-source technology, tools, and mechanisms, such as import and export services for very large datasets.

SNCF Réseau, France

SNCF Réseau manages rail infrastructure across France. It used AWS to accelerate the implementation of its Smart Data strategy, quickly analysing data relevant to the maintenance of SNCF rails using smart sensors in near real time.

Learn more ›

Our commitments to you

Our privacy safeguards and security controls lead the industry. They can help you achieve and even exceed privacy and compliance requirements globally. You can implement these privacy protections based on your specific industry requirements, and use our services, tooling, and resources to help protect your data in alignment with the requirements of regulators and auditors. Maintaining this level of customer trust depends on us making ongoing commitments to you. These commitments include...

Data Control

With AWS, you control your data by using services and tools that allow you to determine where that data is, how it is secured, and who has access to it. Services such as AWS Identity and Access Management (IAM), AWS Organizations, and AWS Control Tower allow you to securely manage access to services and resources. AWS CloudTrail, AWS Config, and Amazon Macie enable governance, compliance, detection, and auditing, while AWS CloudHSM and AWS Key Management Service (KMS) allow you to securely generate and manage encryption keys, with deep integration and automatic encryption available for all AWS storage and database services. You can be confident that no AWS operator has access to master keys in KMS, whether they are imported (i.e. you bring your own key) or generated by KMS – learn more about demystifying KMS key operations here.

Flemish Government, Belgium

The IT Shared Service Centre of the Flemish Government chose AWS because it supports its needs for data security and access control. The service centre uses the Amazon CloudFront Edge Location in Brusssels to improve citizens' experience when interacting with its digital offerings.

Learn more ›

Data Privacy

Your organisation has strict and demanding requirements for the privacy safeguards you use to protect data. Implementing controls to match these allows us to innovate continuously on your behalf. Privacy controls that you can implement include advanced access control, encryption, and logging. These provide consistent and scalable processes to manage privacy, including how data is collected, used, accessed, stored, and deleted.

We only process customer data – which includes any personal data you upload to your AWS account – under your documented instructions and do not access or use your content for any purpose without your agreement. We have a wide variety of best practice documents, training, and guidance, provided by our own experts, that can help you protect your data, such as the Security Pillar of the AWS Well-Architected Framework.

AWS has achieved internationally-recognised certifications and accreditations that demonstrate compliance with rigorous international standards and our ongoing commitment to earning your trust. These include ISO 27001 and ISO 27017 for cloud security, ISO 27701 for privacy information management, and ISO 27018 for cloud privacy. We will not access or use your content for any purpose without your explicit agreement and we never use it for marketing or advertising purposes.

Read more in the Data Privacy FAQ ›

Secureappbox, Sweden

SecureAppbox helps organisations manage sensitive data and comply with the GDPR. In 2015, it helped The Swedish Association of Local Authorities and Regions, SKL (Sveriges Kommuner och Landsting) build a secure national platform to rehome 60,000 child refugees who entered Sweden without parents.

Learn more ›

What's GAIA-X?

GAIA-X is a data economy-driven initiative that aims to bring together representatives from business, science, and politics to help define standards for the next generation of data infrastructure. This includes an open, transparent, and secure digital ecosystem, where data and services can be made available, collated, and shared in an environment of trust. AWS has participated in multiple GAIA-X technical working groups and supported the initiative from its beginning.

Learn more about GAIA-X ›

Learn more about GDPR

The EU's General Data Protection Regulation (GDPR) protects EU individuals' fundamental right to privacy and the protection of personal data. It includes robust requirements that raise and harmonise standards for data protection, security, and compliance. Our customers can use all our services to process personal data (as defined in the GDPR) that is uploaded to the AWS services under their AWS accounts or generated within the AWS account (customer data) in compliance with the GDPR. We offer services and resources to help you comply with GDPR requirements that may apply to your activities, and we have over 500 features and services focused specifically on security and compliance with new features launching regularly.

Visit the GDPR Centre ›

Data Sovereignty

You can choose to store and process your customer data in any one or more of our European Regions. Today, these include France, Germany, Ireland, Italy, Sweden, and beginning in 2022, Spain. You can also use AWS services with the confidence that customer data stays in the AWS Region you select. A small number of these services involve the transfer of data to help, for example, develop and improve those services. You can opt-out of this transfer, unless the transfer is an essential part of the service (e.g. it's a content delivery service). Our systems prohibit – and are designed to prevent – remote access by AWS personnel to customer data for any purpose, including service maintenance, unless that access is either requested by you or if it is required to prevent fraud and abuse, or to comply with law. We are committed to important EU privacy, portability, and digital sovereignty programmes – including Cloud Infrastructure Services Providers in Europe (CISPE) Code of Conduct, the European Commission Standard Contractual Clauses (SCC), the SWIPO Code of Conduct, and GAIA-X.

We are transparent about our commitments to protect your data

AWS contracts are jargon-free and include commitments to protect your data that go beyond those available from other cloud providers. These strengthened commitments build on our long track record of challenging law enforcement requests. If we do receive a law enforcement request for customer data from any government body, we commit to challenging those that are overbroad, or where we have any appropriate grounds to do so, including where the request conflicts with EU law. We also provide a bi-annual Information Request Report listing the types and number of information requests we receive from law enforcement.

Customers who are subject to GDPR automatically benefit from our GDPR Data Processing Addendum, including Standard Contractual Clauses. We offer an on-line summary of Privacy Features of AWS Services to help you to determine whether the maintenance and provision of our services to you may involve customer data being transferred outside of the AWS Region you chose to store that data.

These resources can help you comply and demonstrate compliance with regulations, including GDPR. They can also help you complete your data transfer assessments in accordance with the European Data Protection Board Recommendations on measures that supplement transfer tools.
You can also choose AWS services that only store and process customer data in the EU.

Veolia, France

Veolia Water Technologies reduces operating costs by 90 percent and accesses new opportunities for innovation using AWS. Our services and solutions have enabled it to set up virtual data centres and operate its systems without any constraints, while fully protecting their sensitive data.

Learn more ›

Security

Security is our top priority. At AWS, cloud security is a shared responsibility between us and you. But you can improve your ability to meet core security, confidentiality, and compliance requirements easily with our comprehensive services, whether that's through Amazon GuardDuty or our AWS Nitro System – the underlying platform for our EC2 instances. In addition, services such as AWS CloudHSM and AWS Key Management Service, allow you to securely generate and manage encryption keys, and AWS Config and AWS CloudTrail deliver monitoring and logging capabilities for compliance and audits.

AWS complies with internationally recognised standards such as Cloud Computing Compliance Controls Catalog (C5, Germany) and Esquema Nacional de Seguridad (ENS, Spain). We have also achieved certifications including PCI-DSS, Hébergement de Données de Santé (HDS, France), and TISAX (EU Automotive). The TISAX standard provides the European automotive industry a consistent, standardised approach to information security systems and our certification enabled our Industrial Cloud work with Volkswagen, which you can read about in the next section.

All our certifications help satisfy compliance requirements for regulatory agencies across the EU. Financial services providers, healthcare providers, and government agencies are among the customers who trust us with their most sensitive information.

Unlock the potential of open data in the cloud

Open data on AWS lets you spend more time on data analysis, rather than data acquisition. When data is shared on AWS, whether privately or publicly, you can analyse it and build services on top of it using a broad range of compute and data analytics products, including Amazon EC2, Amazon Athena, AWS Lambda, and Amazon EMR. Our Registry of Open Data makes it easy to find datasets made publicly available through AWS services.

Open data also enables initiatives for a better world now and for future generations. The Amazon Sustainability Data Initiative (ASDI), for example, seeks to accelerate sustainability research and innovation by minimising the cost and time required to acquire and analyse large sustainability datasets. ASDI supports innovators and researchers with the data, the tools, and the technical expertise to move sustainability to the next level.

European Space Agency
Sentinel-2 is an ongoing collection of satellite imagery of all land on Earth built by the European Space Agency. Through AWS public datasets, Sentinel-2's complete datasets are regularly archived and made freely available to users (both registered and non-registered).

Learn more ›

Joint-solutions that drive digital transformation

United by a passion for delivering constant innovation and customer obsession, AWS and Intel have collaborated to deliver a steady beat of infrastructure and service offerings tailored for mission critical applications such as massively scalable data analytics, high performance computing, artificial intelligence, and the Internet of Things. As business and engineering partners for over 15 years, Intel and AWS share similar core beliefs around the importance of data privacy. Intel believes that responsible access and use of data is crucial in order to enrich trust in technology. Robust privacy protection is a key component of consumer awareness and trust.

Intel has also committed to developing technologies that improve cloud security and has been collaborating with AWS around this for years. An example of Intel technology dedicated to improving security measures is Intel's® Advanced Encryption Standard New Instructions (Intel® AES-NI). AES-NI greatly improves the performance of algorithms implementing the Advanced Encryption Standard (AES) standard to provide faster data protection and greater security. These significant performance improvements make it practical to utilize state-of-the-art encryption in realms that would have previously had too much impact on performance. All current generation of Amazon Elastic Computer Cloud (EC2) instances support this processor feature. In addition, the new M6i EC2 instances, which are powered by 3rd generation Intel® Xeon® Scalable processors, include support for always-on memory encryption using Intel Total Memory Encryption (TME).

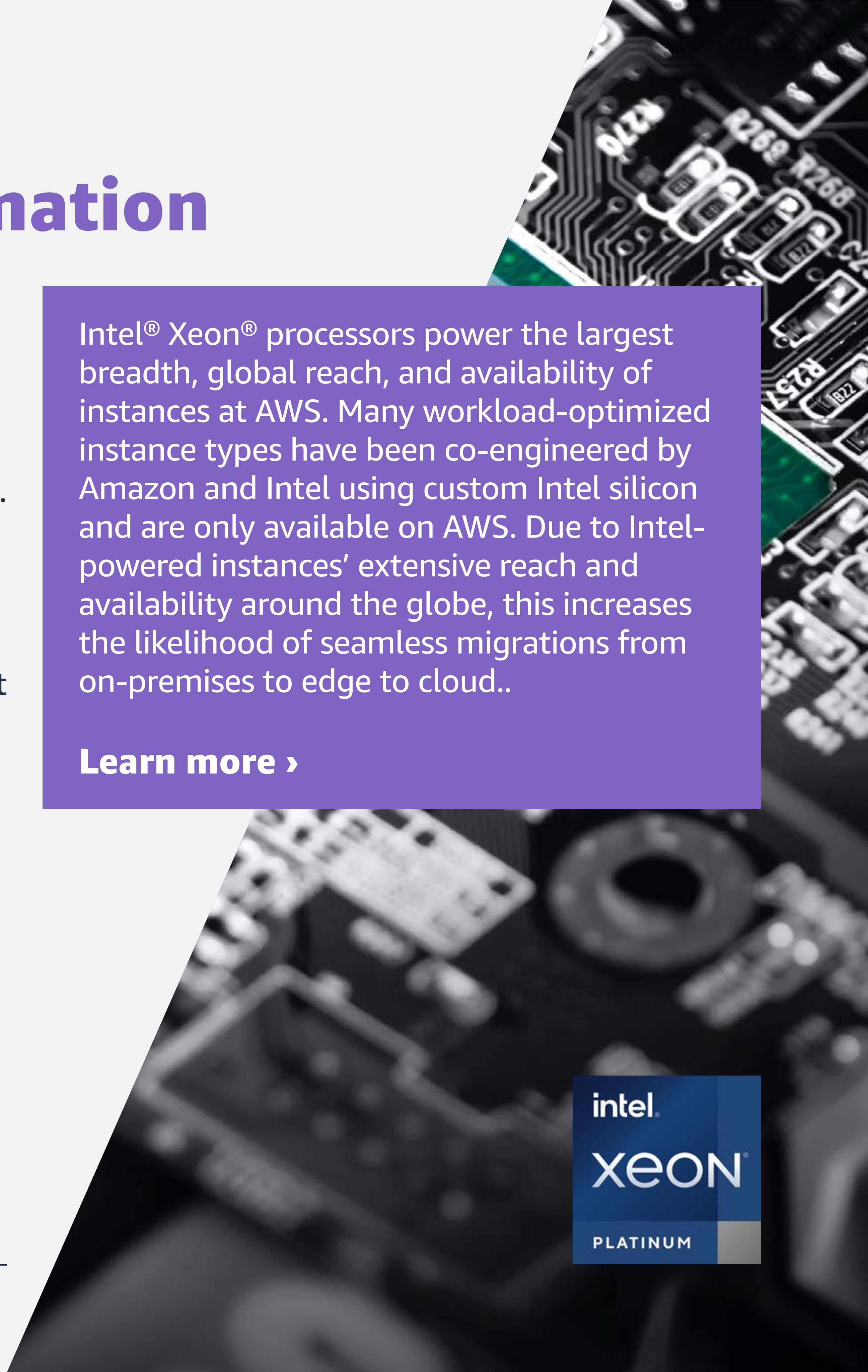
AWS offers a multitude of Amazon EC2 instance types featuring Intel® Xeon® Scalable processors – allowing customers to scale their instance choice to match the compute, memory, storage and latency demands of their workloads.

Explore our world ›

See our global infrastructure ›

Intel® Xeon® processors power the largest breadth, global reach, and availability of instances at AWS. Many workload-optimized instance types have been co-engineered by Amazon and Intel using custom Intel silicon and are only available on AWS. Due to Intel-powered instances' extensive reach and availability around the globe, this increases the likelihood of seamless migrations from on-premises to edge to cloud..

Learn more ›



Start your journey

Our online resources can help you to better understand EU data protection. Why not start by reading our latest blog post on how we help EU customers navigate data protection?

Level up your knowledge on EU data protection

Over at our EU Data Protection site, you can find out more about our commitments to protect customer data in the European Union, as well as additional success stories and resources for you to explore.

Helping you protect your data in a world with constantly changing regulations, technology, and risks takes teamwork. If there's anything you would like to discuss, please get in touch:

Start the conversation