HPE POINTNEXT

AWS security program for cloud adoption

Securely adopting AWS at scale

Elements of the security practice

- **Logging and monitoring:** Visibility into issues as they arise
- **Encryption and key management:** Appropriate protection for your sensitive data
- **Access management:** Defined and established role-based access controls
- **Nearly continuous compliance:** Organizational visibility into compliance controls

"Engaging Natixis' security, legal, and compliance personnel, Cloud Technology Partners, a Hewlett Packard Enterprise company, ensured that access to the AWS production environment was adequately protected, appropriate data governance mechanisms were in place, and full traceability of activities was available to fulfill regulatory requirements."

– George Marootian, EVP, Head of Technology, Natixis.

Talk to an AWS security expert today

Learn more at
hpe.com/services/cloud

Make the right purchase decision. Click here to chat with our presales specialists.

Share now

Get updates

Hewlett Packard Enterprise

AWS security practice

Our AWS security practice is developed by a group of architects, engineers, developers, and technology enthusiasts dedicated to defining, automating, and helping ensure secure environments on Amazon Web Services (AWS).

Following AWS, cloud security alliance (CSA), NIST, and other industry best practices, the security practice enables our clients to safely and confidently operate in compliant environments.

Gaining the benefits of cloud in a safe and secure manner requires successfully navigating a highly complex technical and regulatory environment. The security practice addresses the following challenges:

- **Infrastructure security and network protection**—Implement secure network components on AWS, including perimeter protection, VPC/subnet segmentation, and IDS/IPS capabilities
- **Data security**—Manage access and protection of sensitive data in the cloud
- **Identity and access management**—Establish appropriate mechanisms for user access to cloud environments based on the principle of the least privilege
- **Logging, monitoring, and audit trail**—Monitor the aspects of secure cloud operations and enable forensic capabilities
- **Governance, risk, and compliance**—Meet regulatory, audit, and legal requirements while retaining agility; enable nearly continuous governance and management practices
- **Industry standards**—Leverage AWS, cloud security alliance (CSA), ISO 270xx, and NIST guidelines to accelerate your cloud adoption journey

AWS security practice

We work with the world's leading enterprises and financial institutions to solve their unique security, governance, and regulatory concerns when moving to the cloud. The security practice is a key component during the phases of the cloud adoption program providing a clear, safe, and secure path to end-to-end cloud adoption.

Figure 1. Enterprise cloud prescriptive approach

Client success story

Cloud adoption
How Natixis is pioneering cloud in the financial services industry—Natixis turned to HPE and AWS to securely support their future IT and business operational needs.

Read the case study

a00059831ENW, November 2018