



# Security, Identity, and Compliance for Healthcare Workloads

Infrastructure, services and partners to  
elevate the security of NHS workloads in  
the cloud.



## AWS in healthcare

The Amazon Web Services (AWS) healthcare mission is to enable access and delivery of person-centred care in order to improve outcomes and lower costs by accelerating the digitisation and utilisation of healthcare data. Our aim is to help the National Health Service (NHS) and its partners develop cloud strategies to achieve more with less, modernise technology, and digitally transform back office and clinical services.

## What does cybersecurity mean for the NHS?

In an increasingly digitised healthcare landscape, ensuring the security and confidentiality of patient, workforce and estates data is of paramount importance. In this digital age, where cyber threats loom large, the NHS is embracing AWS and its associated partners enabling to bolster its cybersecurity infrastructure, safeguard patient data, and uphold its commitment to providing secure and reliable healthcare services to millions of individuals across the UK.

By leveraging AWS's secure cloud computing environment, the NHS can enjoy scalable and robust data storage and processing capabilities without compromising data privacy. AWS provides data encryption, access controls, and compliance with stringent industry regulations, providing the NHS with the necessary tools to achieve and maintain robust cybersecurity standards.



## Benefits of AWS Cloud security services

### Scale securely with superior visibility and control

With AWS, you control where your data is stored, who can access it, and what resources your organisation is consuming at any given moment. Fine-grain identity and access controls combined with continuous monitoring for near real-time security information ensures that the right resources have the right access at all times, wherever your information is stored.

### Automate and reduce risk with deeply integrated services

Automating security tasks on AWS enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work critical to your business. Select from a wide variety of deeply integrated solutions that can be combined to automate tasks in novel ways, making it easier for your security team.

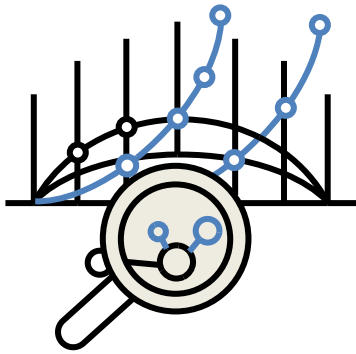
### Inherit the most comprehensive security and compliance controls

To aid your compliance efforts, AWS regularly achieves third-party validation for UK government and NHS compliance requirements to help you meet security and compliance standards for UK healthcare, government, and beyond.



## Strategic security

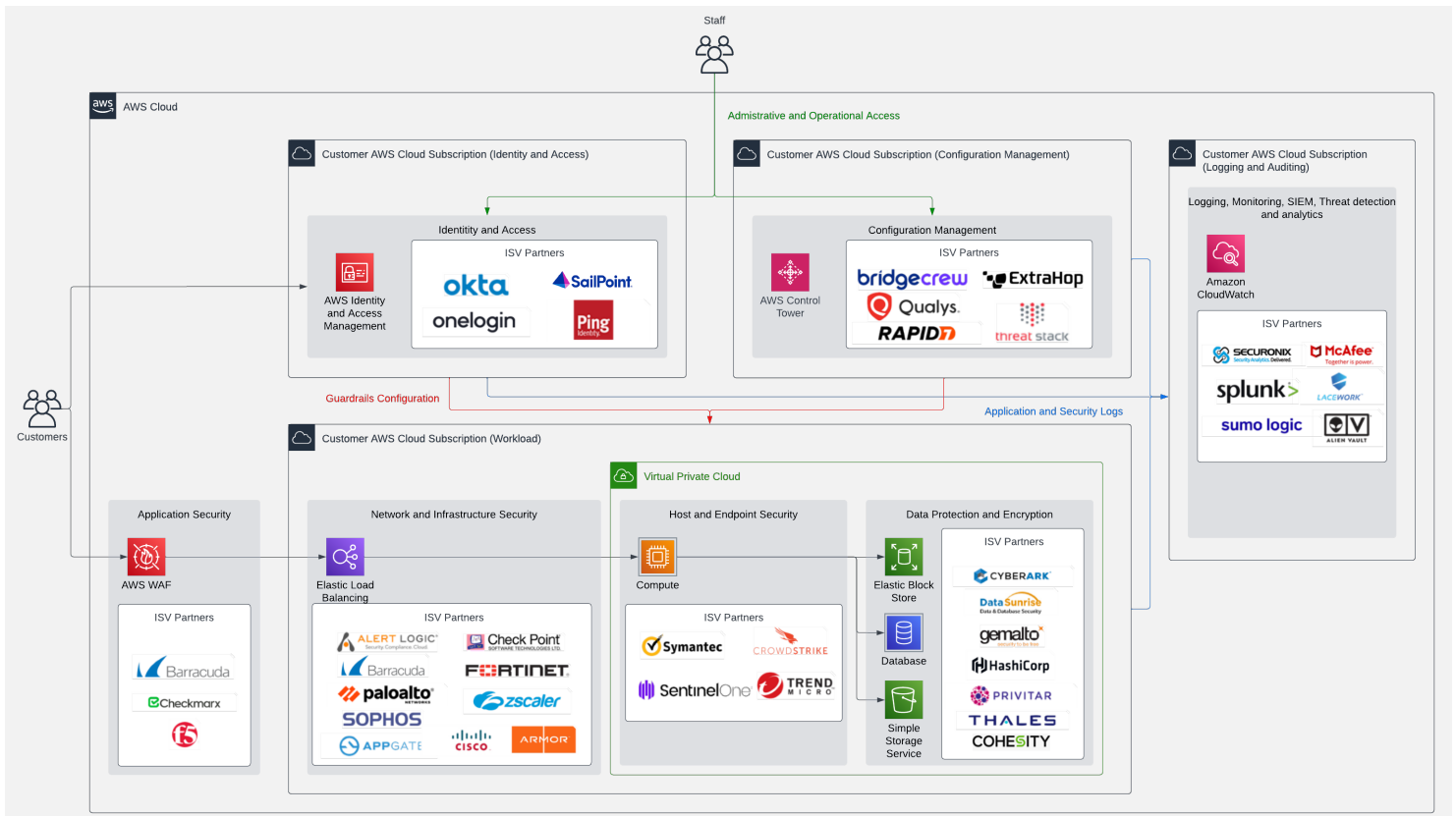
AWS supports NHS organisations to build secure, high-performing, resilient, and efficient infrastructure for your applications. Our world-class security experts, responsible for managing our own infrastructure, also build and maintain a broad selection of security services for our customers. Our services and solutions are designed to help you simplify security compliance, and deliver the following benefits to help you implement an optimal security posture:



- Prevent:** Define user permissions and identities, infrastructure protection and data protection measures for seamless AWS adoption strategy.
- Detect:** Gain visibility into your organisation's security posture with logging and monitoring services. Ingest this information into a scalable platform for event management, testing, and auditing.
- Respond:** Automate incident response and recovery to help shift the primary focus of security teams from response to analysing root cause.
- Remediate:** Leverage event driven automation to quickly remediate and secure your AWS environment in near real-time.

## AWS and partner solutions to safeguard your NHS workloads

Supplement the current benefits of AWS Cloud security services by integrating security technology and consulting services from familiar solution providers you already know and trust. AWS have carefully selected providers with deep expertise and proven success securing every stage of cloud adoption, from initial migration through ongoing day to day management.



APN Partners offer hundreds of industry-leading security solutions that help customers improve their security and compliance posture. The scalability, visibility, and affordability our partners inherit with the AWS Cloud enables them to create world-class offerings for customers which can be easily deployed and consumed.



## AWS security bundle for NHS organisations

We have developed a no-cost security bundle for NHS organisations, designed to provide a comprehensive set of curated activities in a short-time scale with limited trust resources to improve your security posture. These activities do not require any commercial agreements to be in place and provide NHS organisations with advanced knowledge and understanding abouts how to define, plan and deliver the right cloud-driven security outcome with no upfront commitment.

### Step 1

**Understand the challenge:** Meet with AWS account team to explore the business drivers behind the security challenges; understand categories of security concerns and historic events; discuss the current barriers to adoption of security best practice adoption

### Step 2

**Dive deep with an AWS-led discovery workshop:** Undertake a detailed workshop with the AWS account team and solution architects to dive deep on the security challenges being faced; identify KPIs and understand areas of potential AWS support.

### Step 3

**Learn and be curious about AWS security and services:** Build knowledge and capability. Topics include AWS Well Architected Framework, the shared responsibility model, high availability, disaster recovery, and continuous improvement. Learn via hands-on AWS instructor-led immersion days and on-demand workshops.

### Step 4

**Demonstrate the value with a PoC:** Work with AWS solution architects to build a proof of concept (PoC) and quick starts, supported by AWS prescriptive guidance and AWS Promotional Credit.

### Step 5

**Go build:** Explore implementation options through customer capability, customer enablement, AWS or partners.

No cost AWS offering

AWS Customer Incentives

AWS Proserve or Partner



## NHS AWS Partner offerings for NHS customers

One significant advantage that AWS Partners bring to the table is the availability of no-cost offerings to customers. These no-cost offerings enable businesses to explore and adopt their solutions on AWS Cloud services more effectively without incurring any upfront expenses. Through these initiatives, AWS Partners offer a range of valuable resources, such as workshops, training sessions, and PoC support to assist customers in understanding how AWS can address their unique requirements.

Partner	Offering
Checkpoint	Checkpoint is a leading global provider of cybersecurity solutions and is committed to safeguarding NHS technology environments against evolving threats. Based on their research, Misconfigurations are a major public cloud security threat, according to 59 percent of cloud users. Checkpoint's dedicated team is excited to offer you an exclusive opportunity for a complimentary consultation and a comprehensive digital security assessment. Experts will take you on a journey through the assessment results, ensuring a clear understanding of any potential security risks lurking within your NHS technology and digital estate. Trust Checkpoint to stand by your side, providing professional guidance and unwavering support as we work together to fortify and safeguard your valuable digital assets.
CrowdStrike	As a cloud-native industry leader, CrowdStrike was the first cybersecurity organisation to build their cybersecurity services on AWS as a seamless software as a service (SaaS) offering. Our deep integration with AWS extends across 15+ critical services, including AWS Control Tower, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Security Lake, and AWS Verified Access. This unique collaboration empowers NHS organizations to consolidate their defences onto a single platform, enhancing security and providing unmatched visibility. Underpinned by Falcon Agent, a lightweight agent that deploys without the need for system restarts or consuming excessive resources. Unlike other solutions, the Falcon agent is a one-time deployment, simplifying the NHS's security infrastructure requirements. NHS organisations can leverage CrowdStrike's modular solutions approach when securing their ecosystems, all while eradicating the necessity for multiple fragmented solutions that adversaries exploit. Leveraging CrowdStrike, NHS organisations not only achieve comprehensive protection but also eliminate the resource headaches associated with managing multiple consoles and agents. They make sure that NHS organizations can seamlessly align with the AWS Shared Responsibility Model, safeguarding every asset in the AWS environment and fortifying new workload migrations as they happen.
Okta	Okta offers free trials on both the workforce and customer identity cloud platforms. NHS organisations can use Okta tenants for Staff and Patients. For workforce users, Okta's Workforce Identity Cloud acts as the identity platform to consolidate disparate IT infrastructures and domains with Okta Universal Directory, enabling one source of truth for user data that can then interact with ESR, finance and IT systems. With adaptive multi factor authentication (MFA), Okta helps NHS organisations to meet cyber assurance requirements. For patients, Okta's Customer Identity Cloud acts as the digital front door to your patient services. Giving the organisation a secure single view of the patient, allowing you to build a compliant personalised user experience that includes contextually aware step-up authentication. This significantly enhances the digital journey for the end user and can increase engagement by up to 30 percent. NHS organisations can realise the flexibility and extensibility offered by Okta for Identity and Access Management (IAM).

Partner	Offering
Splunk	Splunk and Cysiam join forces to offer a free risk assessment to support NHS trusts in addressing organisational risks. The risk assessment service will empower NHS Trusts to evaluate their existing security measures, identify potential weaknesses, and proactively address any vulnerabilities that could compromise patient data, critical systems, and the overall integrity of healthcare services. By leveraging cutting-edge technologies and industry-leading cybersecurity methodologies, this joint initiative aims to equip NHS Trusts with the knowledge and insights needed to strengthen their security posture and protect the valuable assets they safeguard.
TrendMicro	Trend Micro offers NHS Customers a 30-day free trial and of Cloudfone Conformity and cybersecurity assessment sweep services. The integration into your AWS workloads is a 2-3 minute activity and assisted by experts. The outcome is that NHS Organisations gain visibility over the Shared Responsibility Model with concise compliance reports for AWS resources. The tool provides total security for cloud builders and DevOps pipelines, supporting various critical use cases like cost optimization and performance efficiency within AWS. The application also detects dangerous configurations and produces a Heatmap of its findings with guided steps and fix them using CLI, GUI, or Cloud Formation scripts. Full API integration is available, and additional solutions can be explored through Trend Micro's partnership with AWS.





## AWS Security Consulting Partners

Our AWS Consulting Partners provide expert guidance to AWS customers on how to leverage security tools and embed best practices into every layer of their AWS Cloud environments and integrations.

Consulting Partner	Overview
CloudScaler	CloudScaler have experience implementing enterprise-grade compliance and security best practices within AWS in both the private and public sector – implementing controls and guardrails that protect you at all times.
CirrusHQ	As AWS experts, CirrusHQ are always up-to-date on the latest trends and have access to all the latest digital resources to create effective solutions. You can rely on them for adequate guidance and assistance when managing data and infrastructure in the cloud ensuring your business does not lose any critical information.
IBM	IBM is a global technology company that provides a wide range of cybersecurity solutions. Their offerings include threat intelligence, data security, identity and access management, and incident response services. IBM's comprehensive approach helps organizations defend against cyber threats, detect and respond to attacks, and maintain a robust security posture in today's digital landscape.
TCS	Tata Consultancy Services (TCS) is a leading IT services company that offers cybersecurity solutions to businesses worldwide. TCS provides services such as threat detection, incident response, and risk assessment, helping organizations protect their digital assets and data from cyber threats while ensuring regulatory compliance and maintaining business continuity.



## AWS Security Technology Solutions Partners

### Network and Infrastructure Security

Network inspection designed to detect and protect your workloads from malicious or unauthorised traffic.

Solution partner	Solution overview
AlertLogic	Alert Logic is a cybersecurity company offering cloud-based security solutions, including threat detection, incident response, and compliance services. They help businesses protect their digital assets from cyber threats, ensuring a secure and resilient cloud environment
AppGate	AppGate is a cybersecurity company specializing in providing secure access solutions. Their Zero Trust Network Access (ZTNA) platform allows businesses to establish secure connections to their applications and resources. By applying a Zero Trust approach, Appgate ensures robust security and access control, mitigating potential cyber threats effectively.
Barracuda	Barracuda Networks is a cybersecurity and data protection company. They provide a comprehensive suite of solutions, including firewalls, email security, cloud security, backup, and data protection services. Barracuda's offerings help businesses safeguard their networks, applications, and data from cyber threats while ensuring data availability and resilience.
Checkpoint	Checkpoint is a leading cybersecurity company providing comprehensive solutions to safeguard businesses from cyber threats. Their offerings include advanced threat prevention, network security, cloud security, and mobile security solutions. Checkpoint's innovative technologies protect organizations worldwide from evolving cyber risks and attacks.
Cisco	Cisco offers a comprehensive portfolio of cybersecurity solutions to protect businesses against advanced threats. Their offerings include firewalls, endpoint security, email security, and cloud security services. Cisco's integrated approach helps organizations strengthen their security posture and defend against cyber attacks across networks, devices, and the cloud.
Fortinet	Fortinet is a prominent cybersecurity company that delivers a wide range of network security solutions. They offer products and services such as firewalls, secure access, cloud security, and threat intelligence to protect businesses against cyber threats and ensure secure network environments.
Palo Alto Networks	Palo Alto Networks is a leading cybersecurity company providing a range of solutions, including next-generation firewalls, cloud security, and endpoint protection. Their platform focuses on preventing cyber threats, detecting and responding to attacks in real-time, and ensuring secure access to applications and data.
Sophos	Sophos is a prominent cybersecurity company delivering comprehensive solutions for businesses and individuals. They offer a wide range of products, including endpoint protection, firewall, encryption, and email security. With a focus on simplicity and effectiveness, Sophos helps organizations stay protected from evolving cyber threats.
Zscaler	Zscaler is a leading cloud security company providing secure access to applications and services. Their cloud-based platform delivers advanced security, web filtering, threat protection, and data loss prevention across various devices and locations, enabling businesses to securely connect to the internet and cloud services without compromising on performance or security.



## Host and endpoint security

Agents that detect and protect against malware and other threats found on your operating system or host. Includes Anti-Virus (AV), Endpoint Detection and Reponses (EDR), Endpoint Protection Platform (EPP), File Integrity Monitoring (FIM), and Host Intrusion Detection System (HIDS).

Solution partner	Solution overview
CrowdStrike	CrowdStrike is a cybersecurity company specializing in endpoint protection and threat intelligence. Their cloud-based platform delivers advanced threat detection and response capabilities to proactively defend against cyber attacks. By leveraging artificial intelligence and machine learning, CrowdStrike helps businesses stay secure and resilient in the face of evolving threats.
SentinelOne	SentinelOne is an advanced cybersecurity company that offers autonomous endpoint protection. Their platform employs artificial intelligence and machine learning to detect and respond to sophisticated cyber threats in real-time. SentinelOne provides businesses with comprehensive security solutions to safeguard endpoints and data from evolving cyber attacks.
Symantec	Symantec, now a part of Broadcom Inc., is a global cybersecurity company. They offered a wide range of products and services, including endpoint protection, encryption, email security, and web security. Symantec aimed to protect businesses and consumers from cyber threats and safeguard critical data and applications.
TrendMicro	Trend Micro is a leading cybersecurity company providing cloud and network security solutions. They offer a range of products, including endpoint protection, email security, and threat intelligence. Trend Micro's comprehensive approach helps organizations defend against cyber threats and protect their digital assets in dynamic and diverse IT environments.

## Identity and access control

Help define and manage user identity, access policies and entitlements. Helps enforce business governance including, user authentication, authorisation, and single sign on.

Solution partner	Solution overview
Okta	Okta is a leading identity management company offering secure and seamless access to more than 7000 applications and services. Okta supports workforce and customer identity (service users) journeys. Their platform provides lifecycle management for onboarding and off-boarding clinical staff, consolidation of identities during mergers and acquisitions, Single Sign-On (SSO), Multi-Factor Authentication (MFA), Governance and Privileged User Management solutions, empowering businesses to enhance security and user experience while efficiently managing user identities and access rights.
Onelogin	OneLogin is a cloud-based identity and access management (IAM) company. Their platform enables organizations to secure access to applications and data through Single Sign-On (SSO), Multi-Factor Authentication (MFA), and user provisioning. OneLogin streamlines access control while enhancing security and user experience in the modern workplace.
Ping Security	Ping Identity is an identity security company providing solutions for secure access to applications and APIs. Their platform offers Single Sign-On (SSO), Multi-Factor Authentication (MFA), and identity governance, helping organizations ensure the right users have access to the right resources while maintaining robust security and compliance measures.

## Logging, monitoring, threat detection, and analytics

Centralised logging, reporting, and analysis of logs to provide visibility and security insights.

Solution partner	Solution overview
Alien Vault	AlienVault, now part of AT&T Cybersecurity, was a leading provider of unified security management and threat intelligence solutions. Their platform integrated security essentials like SIEM, asset discovery, and threat detection, enabling businesses to detect and respond to cyber threats effectively while simplifying security operations.
Lacework	Lacework is a cloud security company offering automated threat detection and compliance solutions. Their platform utilizes machine learning to analyze cloud environments, detecting and remediating security risks and ensuring compliance. Lacework helps businesses secure their cloud workloads and applications, providing real-time visibility and protection against cyber threats.
McAfee	McAfee, now part of Intel Security Group, is a global cybersecurity company providing a wide range of solutions, including antivirus software, endpoint protection, and cloud security. With a focus on threat detection and prevention, McAfee helps businesses and consumers stay secure in today's digital landscape.
Securonix	Securonix is a cybersecurity company specializing in next-gen security analytics and user behavior analytics (UBA). Their platform leverages AI and machine learning to detect and respond to insider threats and cyberattacks in real-time, providing businesses with comprehensive security monitoring and advanced threat detection capabilities.
Splunk	Splunk is a leading data analytics and cybersecurity company. Their platform enables businesses to collect, analyze, and visualize data from various sources, facilitating better insights and decision-making. Splunk's solutions play a crucial role in monitoring, detecting, and responding to cyber threats, enhancing organizations' overall security posture.
SumoLogic	Sumo Logic is a cloud-based data analytics and log management company. Their platform enables businesses to collect, analyze, and derive insights from vast amounts of machine data, helping organizations improve operational and security intelligence. Sumo Logic's solutions empower businesses to make data-driven decisions and efficiently manage their IT environments.

## Identity and Access Control

Help define and manage user identity, access policies and entitlements. Helps enforce business governance including, user authentication, authorisation, and single sign on.

Solution partner	Solution overview
Okta	Okta is a leading identity management company offering secure and seamless access to various applications and services. Their platform provides Single Sign-On (SSO), Multi-Factor Authentication (MFA), and lifecycle management solutions, empowering businesses to enhance security and user experience while efficiently managing user identities and access privileges.
OneLogin	OneLogin is a cloud-based identity and access management (IAM) company. Their platform enables organizations to secure access to applications and data through Single Sign-On (SSO), Multi-Factor Authentication (MFA), and user provisioning. OneLogin streamlines access control while enhancing security and user experience in the modern workplace.
Ping Security	Ping Identity is an identity security company providing solutions for secure access to applications and APIs. Their platform offers Single Sign-On (SSO), Multi-Factor Authentication (MFA), and identity governance, helping organizations ensure the right users have access to the right resources while maintaining robust security and compliance measures.

## Vulnerability and Configuration Analysis

Help inspect your application deployments for security risks and vulnerabilities, while providing priorities and advice to assist with remediation.

Solution partner	Solution overview
BridgeCrew	Their platform provided continuous cloud security and compliance automation, helping organizations identify and remediate cloud misconfigurations and vulnerabilities. It enabled seamless integration of security into the DevOps workflow, ensuring secure cloud deployments.
ExtraHop	ExtraHop is a leading cybersecurity company offering network detection and response solutions. Their platform uses real-time analytics and machine learning to detect and respond to security threats, providing organizations with comprehensive visibility into their networks, applications, and devices, ensuring a proactive defense against cyber attacks.
Qualys	Qualys is a cloud-based cybersecurity and compliance company. Their platform provides vulnerability management, continuous monitoring, and web application security solutions. Qualys helps businesses assess and mitigate security risks in their IT environments, ensuring robust security and regulatory compliance while streamlining security operations.
Rapid7	Rapid7 is a cybersecurity company that offers solutions for vulnerability management, incident detection and response, and application security. Their platform helps businesses proactively identify and address security risks, detect and respond to threats efficiently, and secure their applications to maintain a resilient and secure IT environment.
Threatstack	Threat Stack is a cybersecurity company specializing in cloud security and compliance solutions. Their platform provides real-time threat detection, risk assessment, and security monitoring for cloud environments, enabling businesses to identify and respond to security threats proactively, maintain compliance, and secure their cloud workloads and applications.

## Data Protection and Encryption

Helps protect data via encryption, user behavior analysis, and identification of content.

Solution partner	Solution overview
Cohesity	Cohesity is a data management company providing comprehensive solutions for data backup, recovery, and storage. Their platform consolidates secondary data silos, simplifying data management and enabling businesses to efficiently protect, store, and analyze their data across various cloud and on-premises environments. Cohesity aims to streamline data operations and derive valuable insights from data.
Cyberark	CyberArk is a cybersecurity company specializing in privileged access management (PAM) solutions. Their platform secures and monitors privileged accounts and credentials, preventing unauthorized access and protecting critical assets from cyber threats. CyberArk's solutions help businesses maintain strict security controls over privileged access and mitigate the risk of insider threats and external attacks.
DataSunrise	DataSunrise is a cybersecurity company specializing in database security and compliance solutions. Their platform offers real-time data protection, auditing, and monitoring for databases, helping businesses safeguard sensitive information from unauthorized access and ensuring regulatory compliance.
Gemalto	Gemalto, now part of Thales Group, is a digital security company. They offered solutions for secure access, encryption, identity management, and data protection. Gemalto's technologies helped businesses and governments secure their digital identities, transactions, and sensitive information, ensuring confidentiality and trust in the digital world.
Hashicorp	HashiCorp is known for its suite of DevOps tools, but it also provides data security solutions. HashiCorp Vault is a popular product that offers secure storage, encryption, and access control for sensitive data, including passwords, API keys, and certificates. It helps organizations protect their critical data and manage access securely.
Privitar	Privitar is a data privacy company offering solutions for data protection and compliance. Their platform enables businesses to anonymize and de-identify sensitive data while maintaining its utility for analysis and insights. Privitar ensures data privacy and minimizes the risk of data breaches, enabling organizations to unlock the full potential of their data responsibly.
Thales	Thales provide solutions for secure communication, identity management, cybersecurity, and data protection, serving governments, enterprises, and critical infrastructure industries. Thales focuses on building trust and safeguarding the digital transformation of organizations worldwide.

## Get started

To get started contact your [AWS account team](#) to learn more on how we can:

- Support you on your cloud journey
- Understand your technical landscape
- Build your Cloud Business Case
- Identify the best procurement route for your Trust
- Identify quick wins and initial migration opportunities

## AWS resources

- [Guidance for NHS Trusts Adopting AWS Cloud Services](#)
- [AWS Security](#)
- [AWS for Health](#)
- [AWS Partner Network](#)

## Get in touch

Email: [aws-uk-healthcare@amazon.com](mailto:aws-uk-healthcare@amazon.com)