



Answer to common security questions

1. Do you have any compliance certifications?

AWS Cloud is used. <https://aws.amazon.com/compliance/>

2. Do you conduct penetration tests of your service regularly?

Yes, we conduct internal penetration tests either every 3 months or after every major release.

3. Do you conduct audits regularly?

Yes, internal, every 3 month's or major release.

4. Are policies and procedures established for labeling, handling, and securing customer data?

Yes, AWS data is anonymized. AWS IAM Policy in place to prevent data access.

5. Do you have the capabilities to enforce customer data retention policies?

Yes, customer data is purged with Customer or Camera deletion. The integrator has control over deletion.

6. Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Yes, AWS VPC is used to separate environments. No on-premise staging environment is used.

7. Do you have controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-tenant environment?

Yes, AWS data is anonymized. AWS IAM Policy in place to prevent data access.

8. Do you have a Data Loss Prevention (DLP) or extrusion prevention solution for all systems that interface with your cloud service offering?

Yes, no 3rd party access to AWS cloud infrastructure. AWS GuardDuty is used.

9. Will customers' data be moved from one physical location to another?

No, all data is always stored on AWS servers.

10. Do your information security and privacy policies align with particular industry standards?

Yes, AWS SecurtyHub is used. <https://aws.amazon.com/compliance/>

11. Do you utilize 3rd party providers for your service?

Yes, AWS cloud

12. Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?

Yes, the AWS IAM policy is used.

13. Do you maintain documentation for the granting and approval of access to data?

Yes, AWS CloudTrail and SecurityHub.

14. Is timely deprovisioning, revocation or modification of user access to the organization's systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or third parties?

Yes.

15. Do you encrypt customer data at rest (on disk/storage) within your environment? What Encryption strength?

Yes, AWS encryption at rest at applicable services used. For footage, AWS S3 server-side encryption AE-256 is used.

16. Do you encrypt data during transport? If so, what encryption strength?

Yes, In the case of 3dEYE PUSH technology a secure SSL tunnel is created between camera and cloud. AES-256 is used.

17. Do you conduct network, OS, and/or application vulnerability scans at some regular interval?

Yes, the latest AWS AMI based on AWS ECS ASG, Fargate and AWS Serverless architecture is used.

18. Do you have the capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?

Yes, On critical vulnerability AWS will recall AMI. AWS ECS and AWS serverless infrastructure will re-deploy.

19. Do you have anti-malware programs installed on all systems which support your cloud service offerings?

Yes, AWS WAF, AWS GuardDuty, the latest AWS AMI, ECS, and AWS serverless architecture are used.

20. Is the customer informed of an incident in the event of unauthorized release of confidential or sensitive data?

Yes.

21. Do you have a security information and event management (SIEM) system?

Yes, AWS SecurityHub, AWS Guard Duty, AWS CloudTrail.

22. Does your logging and monitoring framework allow isolation of an incident to specific customers?

Yes, AWS data is anonymized and not available. Customers can review Application logs in the Admin panel related to the specific customer.

23. Are controls in place to prevent unauthorized access to application, program or object source code, and assure it is restricted to authorized personnel only?

Yes, AWS IAM policy is used, AWS GuardDuty, AWS CloudTrail.

24. Do you have outsourced providers that manage your service?

No

25. Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?

Yes. Separate, personalized Private Cloud installation can be used to ensure logical segmentation.

26. Do you have policies and procedures in place describing what controls you have in place to protect customers' intellectual property?

Not applicable. We don't store, process, or access Customers' intellectual property.

27. Do you allow customers to specify which of your geographic locations their data is allowed to traverse into/out of?

Yes, the Public cloud is available in the US and Europe AWS region. Personalized Private Cloud installation can be located in any AWS region and zones including GovCloud.

28. Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?

Yes.

29. Do you enforce and attest to customer data separation when producing data in response to legal subpoenas?

Yes,

30. Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific customer without freezing other customer data?

Yes, the Customer can save video footage clips in Library for evidence. Such footage won't be deleted unless the Camera or Customer is deleted.

31. Do you utilize or access customer data and/or metadata? If so, how?

Yes, In case the customer creates an Alert schedule, AI Video analytics will access customer footage to produce relevant events.

32. Do you collect or create metadata about customer data through the use of inspection technologies (search engines, etc.)?

No

33. Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?

Yes, AWS SAML, OAuth2 is available for integrations.

34. Do you provide customers with strong (multifactor) authentication options (digital certs, tokens, biometric, etc..) for user access?

Yes, MFA is available for end-users.

35. Do you enforce strong (multifactor) authentication options (digital certs, tokens, biometric, etc..) for your administrators to manage the solution?

Yes, AWS IAM policies and MFA is used

36. Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build-in security for your Systems/Software Development Lifecycle (SDLC)?

Yes

37. Are passwords stored in an encrypted format? Provide encryption algorithm used?

Yes, AWS SSM and SecretsManager are used. AES 256 or AWS service relevant cipher.

38. Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?

Yes.

39. Does the solution provide for built-in userID/Password management?

Yes, "AWS IAM and SecretManager are used. MFA is Mandatory. The minimum password length is 8 characters

Require at least one number

Require at least one non-alphanumeric character (! @ # \$ % ^ & * () _ + - = [] { } | ')

Allow users to change their own password

Remember the last 3 password(s) and prevent reuse

40. Do you have a risk assessment program that has been approved by management, communicated, and assigned ownership?

Yes.

3dEYE has integrated a risk and compliance program throughout the organization. This program aims to manage risk in all service design and deployment phases and continually improve and reassess the organization's risk-related activities.

41. Do you have a security program with established information security policies that have been approved by management, communicated, and assigned ownership?

Yes

42. Has the 3dEYE program and policies been reviewed within the last year?

Yes

43. Do you have a third-party management program that has been approved by management, communicated, and assigned ownership?

3dEYE leverages AWS Security and Compliance tools <https://aws.amazon.com/products/security>

44. Do you execute background checks on employees?

Yes

45. What is the frequency of the background checks performed on the employees?

Annual or change related to employee status.

46. Do you have a change control or change management program and policy that has been approved by management, communicated, and assigned ownership?

Yes

47. Is there an antivirus/malware policy and program that has been approved by management, communicated, and assigned ownership?

3dEYE leverages AWS Detection, AWS Network, AWS application protection tools, GitHub security and vulnerability tools, and Microsoft security tools.

AWS Services, such as GuardDuty, provide us with continuous monitoring for malicious activity and unauthorized behavior.

48. Are system backups of Data performed? How often?

3dEYE leverages AWS snapshot and backups <https://aws.amazon.com/backup/>

Services are redundant. AWS Serverless architecture is used. Backups and snapshots storage duration and recurrency are service dependent. For instances is usually daily recurrence snapshots.

49. Is there any firewall / ACLs at the edge?

3dEYE leverages AWS Detection, AWS Network tools

<https://aws.amazon.com/products/security/?nc=sn&loc=2>

50. Are vulnerability assessments, scans and/or penetration tests performed on internal or external networks? How often? Is documentation available?

Yes, we conduct internal penetration tests either every 3 months or after every major release.

3dEYE performs load tests and code inspection on every new version build.

3dEYE follows AWS Well Architected framework and respective AWS tools.

<https://aws.amazon.com/architecture/well-architected>

51. Are vulnerability tests (internal/external) performed on all applications at least annually?

Yes, we conduct internal penetration tests either every 3 months or after every major release.

3dEYE performs load tests and code inspection on every new version build.

End-user UI (web/mobile) is checked against the common vectors of attacks

52. Is there a formal Software Development Life Cycle (SDLC) process that includes security and privacy by design?

Yes.

3dEYE exercises mandatory policy to move to new framework versions.

The latest updated libraries during the build process are used.

Best practices during the development process are followed.

Standard libraries and approaches to encryption, authentication and authorization are used.

3dEYE performs load tests and code inspections on every new version build.

End-user UI (web/mobile) is checked against the common vectors of attacks. Extraneous content on the client is blocked using CSP headers.

53. Are encryption tools managed and maintained?

3dEYE utilizes AWS Encryption. Every AWS Service where data lands provide Encryption at rest and in transit.

54. Do you have an Incident Management program?

AWS Incident Management services are used.

<https://aws.amazon.com/products/security/?nc=sn&loc=2>

55. Is there a documented policy for business continuity and disaster recovery that has been approved by management, communicated, and an owner to maintain and review the policy?

Yes

AWS D/CP is leveraged: <https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

56. How often are BC/DR tests performed?

Annually or after major infrastructural changes.

AWS Config is used continuously to monitor and record AWS resource changes.

AWS CloudFormation is used to automate tests.

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

57. Is a Business Impact Analysis conducted at least annually?

Yes

58. Is there an internal audit, risk management, or compliance department with responsibility for identifying and tracking the resolution of outstanding regulatory issues?

Yes

59. Are there regular privacy risk assessments conducted?

Yes, annually or during new region acquisition and expansion.

60. Is there a formal process for reporting and responding to privacy complaints or privacy incidents?

Yes

61. Is there a documented response program to address privacy incidents, unauthorized disclosure, unauthorized access, or breach?

Yes, 3dEYE leverages AWS Automated Incident Response and Forensics Framework, AWS Incident Response.

62. Is there a documented privacy program with administrative, technical, and physical safeguards for the protection of Systems and Data?

3dEYE leverages respective guidelines and policies.

AWS Security and Compliance tools <https://aws.amazon.com/products/security>

AWS FTR program

AWS Well Architected Framework and toolset <https://aws.amazon.com/architecture/well-architected/>