Auvik

Auvik Networks system security

NIS and CIS 3.0 compliance for the United Kingdom



Whitepaper

Contents

Introduction 03

Auvik Networks and NIS/CAF Compliance 04

What is Auvik? 04

What is NIS? 04

What is CAF? 04

1. Data in transit protection 05

2. Asset protection and resilience 05

2.1 Physical location and legal jurisdiction 05

2.2 Data center security 06

2.3 Data at rest protection 06

2.4 Data sanitization 07

2.5 Equipment disposal 07

2.6 Physical resilience and availability 07

3. Separation between users 08

4. Governance framework 08

5. Operational security 08

5.1 Configuration and change management 08

5.2 Vulnerability management 09

5.3 Protective monitoring 09

5.4 Incident management 10

6. Personnel security 11

7. Secure development 11

8. Supply chain security 12

9. Secure user management 12

9.1 Authentication of users to management interfaces and support channels 12

9.2 Seperation and access control within management interfaces 13

10. Identity and authentication 13

11. External interface protection 14

12. Secure service administration 14

13. Audit information for users 15

14. Secure use of the service 15

Introduction

Moving your services from on-premises to the cloud presents its own set of security challenges. As part of your transition, Auvik's network monitoring and management system can be considered a useful and safe evaluation tool for the overall health and security of your network.

Why? Because network visibility is key to awareness, and awareness is key to control.

As you gain more insight into your network, you're also more likely to have better control over the granular details of it. You'll be able to make better decisions because you'll have better access and information. When it comes to improving network health, proactive monitoring and delicate control are essential aspects of traffic management and data protection.

Simply put: you can't address what you can't see. If you're not aware of what's happening from moment to moment across the network you're responsible for, you're only ever going to be reactive in your work, fixing things after they break, instead of taking preventative care to minimize the chances of emergencies. Not only that, but when emergencies do occur (and they will!), a lack of visibility can cause increased downtime and a negative end user experience, since troubleshooting will take you much longer.

Network visibility is a big step forward from firefighting issues after they happen, to staying ahead of all potential problems.



Auvik Networks and NIS/CAF Compliance

It's critically important that the systems you use to evaluate your security and compliance, like Auvik, are also up to the task. To help network professionals, the UK National Cyber Security Centre (NCSC) has created a guidance document for the safe configuration, implementation, and upkeep of cloud services (NIS Cyber Assessment 3.0). In response, our security staff have created this white paper to detail how Auvik meets all 14 points listed in the NCSC Cloud Security Principles.

At Auvik, we believe in transparency as part of our security commitment to customers. Should you have any questions about any of our security features, feel free to contact our team anytime at security@auvik.com.

What is Auvik?

Auvik is a cloud-based network monitoring and management system that provides unprecedented insight into networks and automates complex and time-consuming tasks. Auvik keeps network maps and documentation up to date in real-time, captures and manages device configurations, monitors network performance, alerts you to potential network issues, and more. Data security was built into Auvik from the beginning. We've followed industry best practices, ensuring Auvik is as safe and secure as possible.

What is NIS?

Enacted in 2018, The Directive on Security of Network and Information Systems, or NIS, is European-Union wide legislation on cybersecurity. This requires all member states to develop and implement their own preparedness strategies to boost the overall level of cybersecurity within the EU. The NIS is continually evolving, with a second iteration currently under review.

What is CAF?

The CAF (Cyber Action Framework) is the UK government's implementation of NIS. Through the UK National Cyber Security Centre, the CAF collection is a set of 14 principles meant to help assess cybersecurity and cyber resilience for critical services. The 14 principles are written in terms of outcomes, i.e. specification of what needs to be achieved rather than a checklist of what needs to be done. The CAF is currently in its third version, released in late 2019.

1. Data in transit protection

CAF recommendation:
You should be confident that data in transit is protected between your end user device(s) and the service, that data in transit is protected internally within the service, and that data in transit is protected between the service and other services.

All data transferred between end-users and Auvik use TLSv1.2 and greater for all connections, including API endpoints. All production services are hosted within Amazon Web Services (AWS), and reside on virtual private cloud (VPC) instances with multiple firewall connections between each endpoint. Internally, Auvik uses a multi-tiered architecture to avoid a "flat" network. Internal communications between components is done over private subnets.

2. Asset protection and resilience

2.1 Physical location and legal jurisdiction

CAF recommendation:
You should understand in which countries your data will be stored, processed and managed. You should also consider how this affects your compliance with relevant legislation, e.g. Data Protection Act (DPA), and whether the legal jurisdiction(s) within which the service provider operates are acceptable to you.

Auvik offers customers the ability to select which AWS data center location they would like to host their service to meet performance and data residency needs. You can find a list of the regions where Auvik is available in our knowledge base.

Per our Terms of Service (ToS): "Auvik will not change the location of Your Selected Data Centre except (1) where You have requested the change, or (2) where a change is prompted by business continuity, disaster recovery or other similar concern."

Data that's sent to a region is stored, processed, and backed up in that location. We don't sell, share, or otherwise move data sent to our SaaS application from the target region. Account and billing information is stored in other systems, with appropriate data protection agreements in place with those providers.

Auvik operations are based in Canada, and the Terms of Service shall be construed in accordance with and governed by the laws of the Province of Ontario and the laws of Canada.

2.2 Data center security

CAF recommendation:
You should be confident that the physical security measures employed by the provider are sufficient for your intended use of the service.

All physical security for the Data Centers is the responsibility of AWS, as we don't store customer data outside these environments.

Details on AWS physical security can be found in their compliance documentation.

2.3 Data at rest protection

CAF recommendation:
CAF recommendation: You should have sufficient confidence that storage media containing your data are protected from unauthorized access.

All data is encrypted at rest using AES-256-bit encryption. In addition, we use our own AES-based encryption on per-tenant data, adding another layer of encryption. Data is decrypted and made available to the system only as needed for delivering product features.

We follow industry best practices in every aspect of secure data collection and storage. Auvik servers use an industry standard four-tier architecture, with security protocols at every layer. Even if someone gained unauthorized access to our system, the risk of them being able to compromise all four layers to see or make use of customer data is extremely low.

AES-256

The Advanced Encryption Standard or AES is a symmetric block cipher used by the US government to protect classified information. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. AES-256 encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 256-bits.

Source: TechTarget

2.4 Data sanitization

CAF recommendation:
You should be confident that your data is erased when resources are moved or re-provisioned, when they leave the service, or when you request it to be erased. Storage media which has held your data is sanitized or securely destroyed at the end of its life.

AWS handles all the data destruction and sanitization for services we use.

Details can be found in their device management documentation.

2.5 Equipment disposal

CAF recommendation:
You should be confident that all equipment potentially containing your data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled), and any components containing sensitive data are sanitized, removed or destroyed as appropriate. Additionally, accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.

AWS handles all equipment disposal for services we use.

Details can be found in their device management documentation.

2.6 Physical resilience and availability

CAF recommendation:
You should be confident that the availability commitments of the service, including their ability to recover from outages, meets your business needs.

Details around Auvik's network infrastructure and resilience techniques can be requested from Product Management or Engineering. Feel free to contact us directly at any time.

3. Separation between users

CAF recommendation:
You should understand the types of users you share the service or platform with, have confidence that the service provides sufficient separation of your data and service from other users of the service, and that management of your service is kept separate from other users.

AWS utilizes hypervisors to separate users of their services. Auvik uses AWS as our public cloud provider, and we entrust them to ensure other clients on the same physical hardware do not attack our services. Auvik performs annual penetration testing for our services by a trusted 3rd party who is certified by **GIAC, ISC(2)** and **Offensive Security.** In addition, Auvik uses secure software practices, such as peer code reviews, as part of our development process.

4. Governance framework

CAF recommendation:
You should have confidence that the service has a governance framework and processes which are appropriate for your intended use.

Auvik is **SOC2 Type 1** certified, and is currently working towards **SOC2 Type 2** certification. Auvik's governance structure also includes dedicated security, privacy, risk, and compliance teams. Internally, Auvik uses the **CIS Controls** framework to shape our security programs.

5. Operational security

5.1 Configuration and change management

CAF recommendation:
You should have confidence that the status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime. As well, changes to the service should be assessed for potential security impact, then managed and tracked through to completion.

Auvik uses CRB (change review board) discussions on a bi-weekly basis to review all changes going into a release, ensuring all quality controls have been met, including security concerns. In addition, all infrastructure changes are done using **infrastructure-as-code tools** like Terraform and Kubernetes, making sure we have a documented handle on all infrastructure during its lifecycle.

5.2 Vulnerability management

CAF recommendation:
You should have confidence that potential new threats, vulnerabilities or exploits are assessed, and corrective action is taken, and that relevant sources of information relating to the threat are monitored by the service provider. The severity of threats and vulnerabilities is considered within the context of the service, and this information is used to prioritize the implementation of mitigations. As well, using a suitable change management process, known vulnerabilities are tracked until mitigations have been deployed, and you know service provider timescales for implementing mitigations and are happy with them.

Auvik makes use of Tenable.io for vulnerability management within the organization, and the infrastructure components we use for production systems are also scanned for vulnerabilities with scanners provided by AWS. Auvik releases changes on a bi-weekly schedule and configures our services to use auto-update mechanisms to ensure we are appropriately patched.

We also monitor various news and industry publications for security concerns and review our own controls to see if we require changes, and make adjustments as appropriate. Our own monitoring tools make use of threat intelligence feeds to help keep us up to date on potential IOCs (indicators of compromise) within our environments.

Our Service Level Agreements for internal remediation of security findings are as follows:

- **Critical:** top priority until resolved
- **High:** 5-10 business days
- **Medium:** 30-90 business days
- **Low:** 90+ business days

Risk ratings are based on their CVSS 3.1 scores, after being adjusted for our own environment.

5.3 Protective Monitoring

CAF recommendation:
You should have confidence that incident management processes are in place for the service and are actively deployed in response to security incidents. Also, that pre-defined processes are in place for responding to common types of incident and attack. A defined process and contact route should exist for the reporting of security incidents by consumers and external entities, and that security incidents of relevance to you will be reported in acceptable timescales and formats.

The Auvik software itself generates an audit log for clients that they can monitor and use as necessary. Internally, Auvik makes use of a centralized log management system for audit logging and security events (IDS, configuration changes, health indicators, endpoint security, etc.), to monitor for potential malicious actions targeting our endpoints and infrastructure. This system also includes subscriptions to threat intelligence reports, which can help highlight new threats as they are made public.

5.4 Incident management

CAF recommendation:
You should have confidence that the service generates adequate audit events to support effective identification of suspicious activity, and these events are analyzed to identify potential compromises or inappropriate use of your service. The service provider should take prompt and appropriate action to address incidents.

Auvik makes use of an internal incident management process based on the SANS Incident Response Process. The process can be initiated by an Auvik customer, internal employee, or the public. If a security incident is identified, we follow this high-level process:

- The security or privacy incident is identified and communicated to the Security Incident Response Team (SIRT).
- We assess the incident to determine its severity, priority, scope, and impact.
- We make recommendations for containing, eradicating, or recovering from the incident, then execute on the recommendations.
- Where applicable, we scan the environment(s) to make sure we've completely mitigated the incident.
- We communicate with internal resource teams, stakeholders, and Auvik customers based on the findings of triage and analysis.
- We gather feedback and look at lessons learned to evolve our incident response. process and procedures. Where applicable, we identify and log the incident's root cause.

Customers can reach out to their Success Manager (or success@auvik.com), Auvik Support (support@auvik.com), or Auvik Security (security@auvik.com) to report an incident.

Auvik evaluates security events as they come in, and each are triaged and determined if further investigation is required. In case of an incident, Auvik will inform affected customers within 48 hours of confirmation of the incident. Subsequent updates will be provided as the investigation proceeds, with a root cause analysis provided upon completion of the investigation to those parties who request it.

6. Personnel security

CAF recommendation:
You should be confident that the level of security screening conducted on service provider staff with access to your information, or with ability to affect your service, is appropriate, and that the minimum number of people necessary have access to your information or could affect your service.

All Auvik employees are required to undergo a criminal background check prior to being hired. In addition, Auvik uses a role-based approach to access sensitive data, namely only those employees with a specific need for access to customer data have it.

All access to sensitive data is done with named accounts, using two-factor authentication, and is fully logged and audited. Quarterly reviews of access are also performed.

New employees are also required to take security training, and throughout the year we perform audits to make sure training is completed. We have regular refresher training for all staff once per quarter to ensure security is top of mind for everyone at Auvik.

7. Secure development

CAF recommendation:
You should be confident that new and evolving threats are reviewed, and the service improved in line with them. That development is carried out in line with industry best practice regarding secure design, coding, testing and deployment. As well, configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.

Auvik development practices include security reviews as part of our standard process, including:

- Threat modeling for new, sensitive features using STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege)
- Peer code reviews
- Separate stage and test environments that are physically different from each other and the production environment, with all environments handled using an infrastructure-as-code approach
- Annual penetration testing performed by an independent 3rd party

8. Supply chain security

CAF recommendation:
You understand and accept:

- How your information is shared with, or accessible to, third party suppliers and their supply chains
- How the service provider's procurement processes places security requirements on third party suppliers.
- How the service provider manages security risks from third party suppliers.
- How the service provider manages the conformance of their suppliers with security requirements.
- How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.

Auvik does not, and will not, share data with outside parties. **Data ownership remains with the customer.** For our own vendors, we have a screening process that includes:

- Review of any available **SOC2** and/or **ISO27001:2013** reports
- Required completion of the VSA questionnaire if the above reports are not available

As our production environments are physically hosted in AWS facilities, we don't have any hardware review for their equipment. But we regularly evaluate software components in production environments to ensure we're not using outdated libraries or container images for our Kubernetes clusters.

9. Secure user management

9.1 Authentication of users to management interfaces and support channels

CAF recommendation:
You are aware of all the mechanisms by which the service provider would accept management or support requests from you, and that only authorized users from your organization can use those mechanisms to affect your use of the service.

Auvik has a dedicated support team who can be accessed by phone, email, web, or online chat. We require a phone call to handle sensitive matters, such as MFA token resets, and even then it must be a named account with knowledge of the account. As well, our customers are assigned a dedicated success manager to assist when and as needed.

9.2 Separation and access control within management interfaces

CAF recommendation:
You should be confident that other users cannot access, modify or affect your service, that you can manage the risks of privileged access using a system such as “principle of least privilege”, and you can understand how management interfaces are protected.

Auvik uses a role-based security model by restricting access to the production environment to on-call engineers and support staff. Each customer can determine if they want to allow our support staff to access their data, and can disable this access if needed. In all cases, access is logged and individual named accounts are used. Within the application itself, Auvik offers a strong role-based access system as well, allowing our customers to control access and functionality to whatever control scheme fits them best.

All account access from Auvik staff is protected using two-factor authentication in addition to strong passwords, and management interfaces are restricted further using named VPN accounts, which are only provided to on-call engineering staff, further limiting access to customer information.

Auvik also uses a least-privileges model for data access.

10. Identity and authentication

CAF recommendation:
You should have confidence that identity and authentication controls ensure users are authorized to access specific interfaces.

Auvik supports MFA (multi-factor authentication) and SSO (single-sign-on) using **SAML (security assertion markup language) federation,** in addition to username and password solutions. Internally, Auvik makes use of SSO, MFA, VPNs, and named accounts for all access, in addition to the role based access described in section nine. Auvik has strong password requirements (minimum of 10-character passwords, preferably longer passphrases), as well as mandatory 2FA on all accounts. We use a SSO system for the majority of our accounts, and have policies and procedures in place for job changes, as well as employee onboarding and offboarding.

11. External interface protection

CAF recommendation:
You should understand what physical and logical interfaces your information is available from, and how access is controlled. As well, you should be confident that the service identifies and authenticates users to an appropriate level over those interfaces.

Auvik is a cloud-based application, with all communication using **TLSv1.2 encryption.** The infrastructure for Auvik is set up so that no individual server is directly accessible by the end-user, and everything is layered with AWS load balancers and security groups (firewalls).

The Auvik collector itself only makes outbound connections to the Auvik servers at AWS and does not need to be put in a DMZ or other areas of lesser security. We encourage it to be kept behind a firewall at a customer's site.

Access is done using the web interface with named accounts, which require 2FA. We use a least-privileges and role-based access control model for our production environment.

12. Secure service administration

CAF recommendation:
You should understand which service administration model is used by the service provider, and be content with any risks the model in use brings to your data or use of the service.

Auvik uses a VPN and a **bastion-host**-based administration model. Only authorized users can access the necessary controls to administer the infrastructure for the Auvik application itself.

13. Audit information for users

CAF recommendation:
You should be aware of the audit information that will be provided, how and when it's made available, and the retention period associated with it. Additionally, you should be confident that the audit information will meet your needs for investigating misuse or incidents.

Auvik's software provides audit information for user actions within the product itself, including account changes, logins, configuration changes, etc. This audit data is retained and available to Auvik users for at least 12 months.

Auvik also maintains its own logs for auditing purposes, which are held for up to 18 months for security-related logs, or 14-90 days for other production-related logs (load balancer logs, application logs, etc.).

Upon termination of contracted services with Auvik, data is fully purged and deleted from all backups within 90 days.

Additional details around data retention for network data can be found in our knowledge base.

14. Secure use of the service

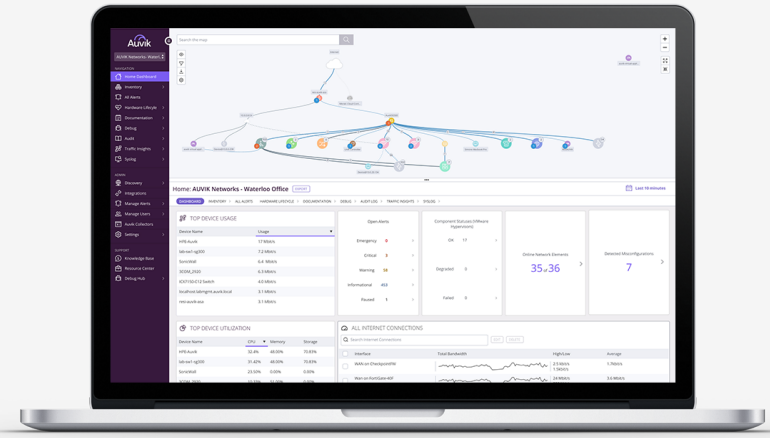
CAF recommendation:
You should understand any service configuration options available, and the security implications of the choices you make. As well, you should be aware of the security requirements of your uses of the service, and be able to educate your staff using the service in how to do so safely and securely.

Auvik provides deployment guides for our collector, as well as a training program for users of the Auvik platform. We pride ourselves in our simplicity of design and flexibility for the configuration of our system to meet the needs of our customers.

From using a trusted cloud service provider to enforcing 2FA on all accounts, Auvik aims to provide a solid user experience while maintaining security for our customers.

More questions?

Have a question about Auvik or our system security that's not answered here? Give us a call or send an email. We're happy to talk to you.



1-866-59-AUVIK (28845) | North America

+44 (0)203 884 1655 | UK & Europe

+61 2 9159 8088 | Australia & New Zealand

security@auvik.com

About Auvik

Auvik is a cloud-based IT management platform that helps IT departments proactively manage their networks, endpoints and SaaS applications. The key is absolute simplicity: seamless deployment, an intuitive interface, and effortless automation. The result is less friction for IT departments, so that everyone can work however and wherever they want.

© Copyright 2013-2024 Auvik Networks Inc. All rights reserved. Auvik, the logo, and other identifiers of Auvik goods or services are trademarks of Auvik Networks Inc and may not be used without express written permission. All other trademarks, service marks, trade dress, and logos are the property of their respective owners. Reference to them does not imply sponsorship, affiliation, or endorsement.