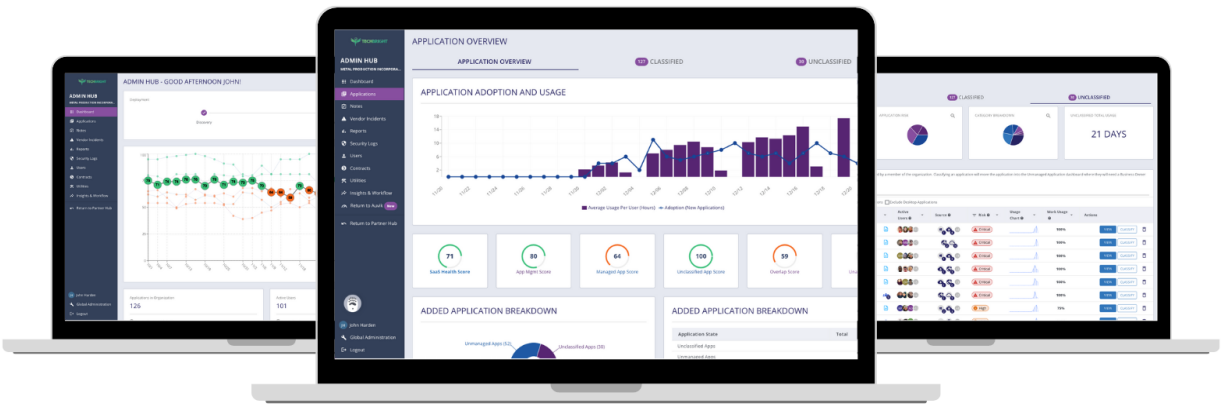
Auvik Networks
System Security
SaaS Management

CONTENTS



YOU CAN'T TAKE CHANCES WITH YOUR IT ENVIRONMENTS.

Security is a big part of your business today. Are the infrastructure and data you manage safe? You carry a lot of responsibility as an IT administrator or managed service provider.
We know that.

It's why we built our SaaS management system from the ground up with safeguards in mind. Our goal is always to make your life easier. Less stressful. More effective.

This white paper will give you an overview of how Auvik collects and transfers data and the security protocols we follow to keep the environments you manage, safe.

Read on to learn more.

WHAT IS AUVIK SAAS MANAGEMENT?

Auvik SaaS Management is a cloud-based system that provides unprecedented insight into SaaS, desktop, and business applications. Auvik SaaS Management is a software offering of the Auvik company.

Auvik SaaS Management was built to secure organizations by giving them insight into all the software they use and unveiling risky behaviors inside ecosystems that IT administrators are unaware of. The technology uses proprietary technology to achieve this goal, and those are outlined below.

WHAT ARE THE COLLECTORS AND WHAT DO THEY DO?

The Auvik SaaS Management technology uses three proprietary types of collectors in its systems. These three collectors are used to establish the software inventory and security information about the inventory.

The Auvik SaaS Management **endpoint collector** is a Windows and macOS collector installed on each managed workstation in the environment. All configuration and data collected by the Auvik SaaS Management software on the workstation is encrypted on the disk. Data transmitted from the endpoint collector to the cloud is encrypted with SSL/TLSv1.2. The endpoint collector has four primary functions:

- **Authenticate to SaaS management web service:** the endpoint collector is responsible for authorization & authentication to the secure cloud-based environment.

- **Identify the active user:** the endpoint collector uses information on the systems to determine the logged-in user, such as the user principal name, desktop name, mac addresses, and registry keys.
- **Identify the active window:** the endpoint collector determines which window is active on the workstation to determine which application should be counted for usage.
- **Communicate with the browser collector:** a native messenger[1], encrypted in transit is opened between the endpoint collector and the local browser collector to exchange authentication and configure the browser collector's configuration.

The Auvik SaaS Management **browser collector** is a browser extension that is installed on each of the individual browsers on the workstation. When the endpoint collector is initially installed, these browsers are installed via group policy / MDM. The browser collector is hosted in the application store for the respective browser. The browser collector has three primary functions:

- **Identify the active web application:** the browser collector captures the base name of the web application in use to determine the application to track usage against.
- **Identify behaviors justifying classification:** the browser collector captures the events of web form logins, downloads, and usage time on web activity. The collector uses this information to determine when an application needs to be classified.

The Auvik SaaS Management **cloud collector** is an API integration into the Microsoft 365 / Azure AD environment. The cloud collector has two primary functions:

- **Identify user information:** the cloud collector will pull in information on the users in the system, such as first name, last name, and email addresses, to match with the other collector's data.
- **Identify single sign-on events:** the cloud collector will pull in single-sign-on events to help identify whether applications being accessed are secured with their provider or are used leveraging web form logins.

The collector supports multiple installation methods, as detailed in the Auvik SaaS Management Knowledge Base.

[1]Native messaging is a Web-to-App communication mechanism supported in all modern browsers (Firefox, Chrome, Edge) to exchange UTF8-encoded JSON messages between a browser extension and a native host application.

WHAT INFORMATION DOES AUVIK SAAS MANAGEMENT COLLECT AND HOW IS IT HANDLED?

1) Auvik SaaS Management collects the authentication credentials for cloud collectors:
Auvik SaaS Management needs this information to configure the cloud collectors. This information is stored securely with AES-256-GCM[2] encryption. They're decrypted and made available to the system only as needed for delivering product features.

2) Auvik SaaS Management collects web-login events in the browser collector:
Auvik SaaS Management collects usernames from web forms. The collector uses this information to determine how a user is accessing web applications. The collector does not ever capture passwords. The collector does not collect sensitive query parameters for login events and strips the URL down to the base web domain and directory structure. These events are securely sent to the SaaS management data aggregator using data encryption and SSL/TLSv1.2.

3) Auvik SaaS Management collects file transfer events in the browser collector:
Auvik SaaS Management uses this information to help IT administrators better understand the usage of web applications. The browser collector only collects metadata related to the event and never has access to the file contents. These events are securely sent to the SaaS management data aggregator using data encryption and SSL/TLSv1.2.

[2] Data encrypted under AES-256-GCM is protected now and in the future. Cryptographers consider this algorithm to be quantum resistant. Theoretical future, large-scale quantum computing attacks on ciphertexts created under 256-bit AES-GCM keys reduce the effective security of the key to 128 bits. But, this security level is sufficient to make brute force attacks on ciphertexts infeasible.

4) Auvik SaaS Management monitors activity on the workstation with the endpoint collector:

Auvik SaaS Management monitors keyboard & mouse activity to determine if the user is active. These keyboard & mouse events are only analyzed to identify an idle state of the device and the mouse & keyboard dataset is never sent to the cloud environment. The endpoint collector captures the start and stop events of application activity and stores these events. The endpoint aggregates usage of endpoint applications installed on the device then securely transfers this data to the Auvik SaaS Management data aggregator using data encryption and SSL/TLSv1.2.

Auvik SaaS Management does not collect any of the following:

- Third-Party Web Login Passwords
- Page Contents
- Full Page URLs
- Keystroked characters
- File Contents
- Sensitive User Information
- Web Portal Authentication Passwords
- Mouse Location Data

HOW DOES AUVIK SAAS MANAGEMENT USE COLLECTED INFORMATION?

Auvik SaaS Management uses the information gathered by the collector to deliver product features. For example, the usernames collected by the browser collector are analyzed across an entire work environment to check for shared and generic logins. Auvik SaaS Management analyzes, distills, and visually renders SaaS information, then shows it to your approved users through a secure login from a web browser.

HOW IS SAAS INFORMATION KEPT SAFE ON AUVIK SERVERS?

Auvik SaaS Management stores data in a cloud-hosted, multi-account environment like many SaaS offerings. We follow industry best practices in secure data collection and storage.

Auvik SaaS Management encrypts all data at rest. Our encrypted database instances use the industry standard AES-256 encryption algorithm to encrypt your data on the servers.

Auvik SaaS Management encrypts all data in transit. All traffic between the collectors is securely sent to the SaaS management data aggregator using data encryption and SSL/TLS.

At Auvik, we make it impossible for non-approved employees to access customer information. Systems holding customer data are not exposed publicly and can only be accessed by authorized personnel through a controlled access mechanism. Authorized personnel credentials are regularly rotated based on industry best practices. You may opt out the functionality allowing employees to access your customer information through the web portal.

HOW IS USER ACCESS TO AUVIK SAAS MANAGEMENT CONTROLLED?

An Auvik SaaS Management account allows for multiple users. Each user has their own login credentials. The account administrator(s) can specify whether users should have full access to view and change things in the software or read-only access. Users with permission to define

other users' roles can further specify which environments each user has access to.

Role-based access controls

Auvik SaaS Management offers granular role-based access controls. Each user is designated a specific role on each client account. As a starting point, Auvik SaaS Management offers several preset roles. You can tailor each of these presets and add custom roles you build yourself.

Auvik Application Programming Interface (API) access

Auvik SaaS Management exposes a set of APIs for customers and third-party integrators to tap into. Data accessed through the API is requested through an x-api-key (API Key) and Authorization (API Secret) header which can be generated in the Auvik SaaS Management UI and is scoped to the set of client access the user has access to.

ACCESSING AUVIK SAAS MANAGEMENT

Single sign-on

Auvik SaaS Management provides single sign-on capabilities through two industry standards: SAML 2.0, and OAuth 2.0. SAML integration with an identity provider like Microsoft's Azure Active Directory enables you to manage authentication from a central location and to use more advanced policies through your identity provider. You can choose who has to use SAML authentication. If SAML authentication isn't enforced, users can enable single sign-on with the OAuth protocol through Google's G Suite or Microsoft's Azure Active Directory. This can be set up after receiving their initial invitation to Auvik or later through their user profile.

Two-factor authentication

For additional security, Auvik SaaS Management requires two-factor authentication for all users that don't use single sign-on. Auvik SaaS Management's two-factor authentication uses the time-based one-time password (TOTP) algorithm. TOTP ensures compatibility with mobile apps like Microsoft Authenticator, Authy, and Google Authenticator

WHERE IS DATA STORED?

Auvik SaaS Management is hosted on Amazon Web Services (AWS) in two geographies: United States & Europe. Your data will be stored in the best region for your location.

HOW IS THE DATA CENTER SECURED?

Physical security

Auvik SaaS Management is hosted on Amazon Web Services (AWS). Amazon's physical and operational security processes are documented in Amazon Web Services: Overview of Security Processes, which outlines AWS data center controls such as:

- Physical and environmental security
- Fire detection and suppression
- Power
- Climate and temperature
- Storage device decommissioning
    - AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.
- Amazon's fault-tolerant infrastructure design
    - Core applications are deployed in an N+1 configuration so that in the event of a data center failure, there's sufficient capacity for traffic to be load-balanced to the remaining sites.
- Certification
    - AWS holds numerous security certifications, which can be reviewed at https://aws.amazon.com/compliance/.

ADDITIONAL SECURITY MEASURES

Security monitoring
Auvik SaaS Management monitors its production environment through various means, including log aggregation and monitoring, intrusion detection, and periodic audits of the platform to ensure a strong security posture and a proactive approach to potential threats.

Application security
Auvik SaaS Management software is developed and tested following the principles set out in the Open Web Application Security Project (OWASP) Top Ten framework to help ensure no vulnerabilities are deployed into production.

Endpoint protection
Auvik deploys anti-virus software on all employee laptops and desktops and manages the software centrally to ensure all signatures are up to date. Auvik also performs daily vulnerability scanning and patching from a centralized management platform within our IT organization. With centralized reporting, we can make sure security incidents are properly quarantined and escalated for further action where needed.

Vendors and subprocessors
Auvik reviews relevant vendors and subprocessors to ensure they provide an appropriate level of security.

Security awareness
Auvik has a security awareness program to ensure all employees understand the importance of security and how it intertwines with their workday. New employees are required to take security training, and throughout the year, we perform audits to make sure training is completed. We also have regular refresher training for all staff annually to ensure security is top of mind for everyone at Auvik. Auvik uses several intelligence sources to keep up to speed on the latest security threats. This information is shared regularly with staff to ensure everyone is aware of threats and knows what to do if they encounter them.

WHAT IS AUVIK SAAS MANAGEMENT'S DATA RETENTION POLICY?

If you ever decide to cancel your Auvik subscription—which you may do at any time—the SaaS application data in your account is completely recoverable within 30 days of cancellation. After 30 days, customer information is periodically deleted for housekeeping purposes. Auvik usually keeps some anonymized metadata[3] from your account to analyze and optimize our system performance. If you prefer that data from your account not be included in our aggregated metadata set, let our support team know when you make your cancellation request. In that case, we'll manually delete all information about your account from our system. The deletion will be permanent, and the information will not be restorable.

[3] Metadata are records derived from or generated by SaaS collectors & data aggregators. They include items such as application information, community notes, and types of activity usage in applications.

MORE QUESTIONS?

Have a question about Auvik SaaS Management 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 SaaS-based technology provider. Offering solutions ranging from network management software to SaaS management solutions. Auvik keeps IT organizations around the world running optimally. By automating and simplifying IT management, Auvik helps rocket an IT team's efficiency and capacity while protecting the business from risks.