



Avid® | Edit On Demand

Security Guide

2024

Legal Notices

Product specifications are subject to change without notice and do not represent a commitment on the part of Avid Technology, Inc. This product is subject to the terms and conditions of a software license agreement provided with the software. The product may only be used in accordance with the license agreement. Product specifications are subject to change without notice.

This guide is protected by copyright. This guide is for your personal use and may not be reproduced or distributed, in whole or in part, without permission of Avid. Reasonable care has been taken in preparing this guide; however, it may contain omissions, technical inaccuracies, or typographical errors. Avid Technology, Inc. disclaims liability for all losses incurred through the use of this document.

© 2024 Avid Technology, Inc. All rights reserved.

Microsoft, Windows, Active Directory, and Azure are registered trademarks of Microsoft Corporation.

Mac and macOS are registered trademarks of Apple, Inc.

CrowdStrike is a trademark of CrowdStrike, Inc., or its affiliates or licensors.

FileCatalyst is a registered trademark of FileCatalyst by HelpSystems.

Teradici is an HP company. HP, HP Anyware, Teradici, PCoIP, and PCoIP Ultra are trademarks of HP, Inc., and are registered in the United States and/or other countries.

Nessus is a registered trademark of Tenable, Inc.

Snyk is copyrighted by Snyk, Inc.

Attn. Government User(s). Restricted Rights Legend

U.S. GOVERNMENT RESTRICTED RIGHTS. This Software and its documentation are “commercial computer software” or “commercial computer software documentation.” In the event that such Software or documentation is acquired by or on behalf of a unit or agency of the U.S. Government, all rights with respect to this Software and documentation are subject to the terms of the License Agreement, pursuant to FAR §12.212(a) and/or DFARS §227.7202-1(a), as applicable.

Trademarks

Avid, the Avid Logo, Avid Everywhere, Avid DNXHD, Avid DNXHR, Avid NEXIS, Avid NEXIS | Cloudspaces, AirSpeed, Eleven, EUCON, Interplay, iNEWS, ISIS, Mbox, MediaCentral, Media Composer, NewsCutter, Pro Tools, ProSet and RealSet, Maestro, PlayMaker, Sibelius, Symphony, and all related product names and logos, are registered or unregistered trademarks of Avid Technology, Inc. in the United States and/or other countries. The Interplay name is used with the permission of the Interplay Entertainment Corp. which bears no responsibility for Avid products. All other trademarks are the property of their respective owners. For a full list of Avid trademarks, see: <http://www.avid.com/legal/trademarks-and-other-notices>

Avid | Edit On Demand Security Guide 2024 • Revised Monday, April 29, 2024 • This document is distributed by Avid in online (electronic) form only, and is not available for purchase in printed form.

Contents

Using This Guide	5
Revision History	5
Who Should Use This Guide	5
Symbols and Conventions	5
If You Need Help	5
Online Documentation	6
Avid Training Services	6
Introduction	7
System Diagram	7
Cloud Resources Overview	7
Avid Infrastructure and Provisioning Backend	7
Customer Systems and Solutions	7
Avid-Provided Third Party Software	8
Network	8
VNET	8
Traffic and Ports	8
Encryption and Data Protection	11
Data at Rest Protection	11
Data in Transit Protection	11
Endpoint Protection	11
Identity and Access Management	11
Access Channels	11
Role-based Cloud Access	12
Maintenance Access	12
Authentication	12
User Management	12
User Account Creation	12
Password Guidelines	12
Monitoring, Logging, and Auditing	13

Monitoring	13
Logging and Alerts	13
Audit Trail	14
Vulnerability Assessments	14
System Scans	14
Code Scans	14
Vulnerability Remediation	14
Operating Systems	14
Avid Products and Components	14
Third Party Software	15
Penetration Testing	15
Exceptions	15

Using This Guide

Avid® | Edit On Demand is a service that provides a cloud-based editing environment with Media Composer® workstation instances (Edit Seats) backed by Avid NEXIS® | Cloud Storage. This guide describes security information and considerations for Avid | Edit On Demand.

Revision History

Date Revised	Version	Title
March/April, 2024	N/A	Avid Edit On Demand Security Guide
August, 2023	N/A	Avid Edit On Demand Security Guide
April 21, 2022	2022.4.1	Avid Edit On Demand Security Overview
August 26, 2021	2021.8.0	Avid Edit On Demand Security Overview

Who Should Use This Guide

This guide is for system and network administrators and Avid | Edit On Demand administrators responsible for the security for Avid | Edit On Demand and its users.

Symbols and Conventions

Avid documentation uses the following symbols and conventions:

Symbol or Convention	Meaning or Action
	NOTE; provides important related information, reminders, recommendations, and strong suggestions.
	TIP; provides a helpful hint that can aid you in getting the most from your system.
<i>Italic font</i>	Italic font; emphasizes words.
<Italic font>	Angle brackets and italic font; indicates variables.
(pipe character)	Pipe character; in some Avid product names, such as Avid NEXIS® Cloud Storage. In this document, product names include the pipe character when they are in headings or upon their first use in text.

If You Need Help

If you have trouble with your Avid product:

1. Retry the action, carefully following the instructions given for that task. It is especially important to check each step of your workflow.
2. Check the latest information that might have become available after the documentation was published.

Always check online for the most up-to-date release notes or ReadMe as Avid updates the online version whenever new information becomes available.

To view the online versions, visit the online Avid Knowledge Base at www.avid.com/KB. Use the left sidebar to refine your search by product and document type.

3. Check the documentation that came with your Avid product for maintenance or other issues.
4. Visit the online Avid Knowledge Base at www.avid.com. Online services are available 24 hours per day, 7 days per week. Search this Knowledge Base to find answers, to view error messages, to access troubleshooting tips, to download upgrades, and to read or join online message-board discussions. Use the left sidebar to refine your search.

Online Documentation

You can access the [Avid Edit On Demand documentation](#) on the online Avid Knowledge Base.

Avid online documentation contains all the product documentation in PDF format. You can access PDF documentation on the online [Avid Knowledge Base](#). Be sure to refine the search with your specific product and release number or year.

Avid Training Services

Avid makes lifelong learning, career advancement, and personal development easy and convenient. Avid understands that the knowledge you need to differentiate yourself always changes, and Avid continually updates course content and offers new training delivery methods that accommodate your pressured and competitive work environment.

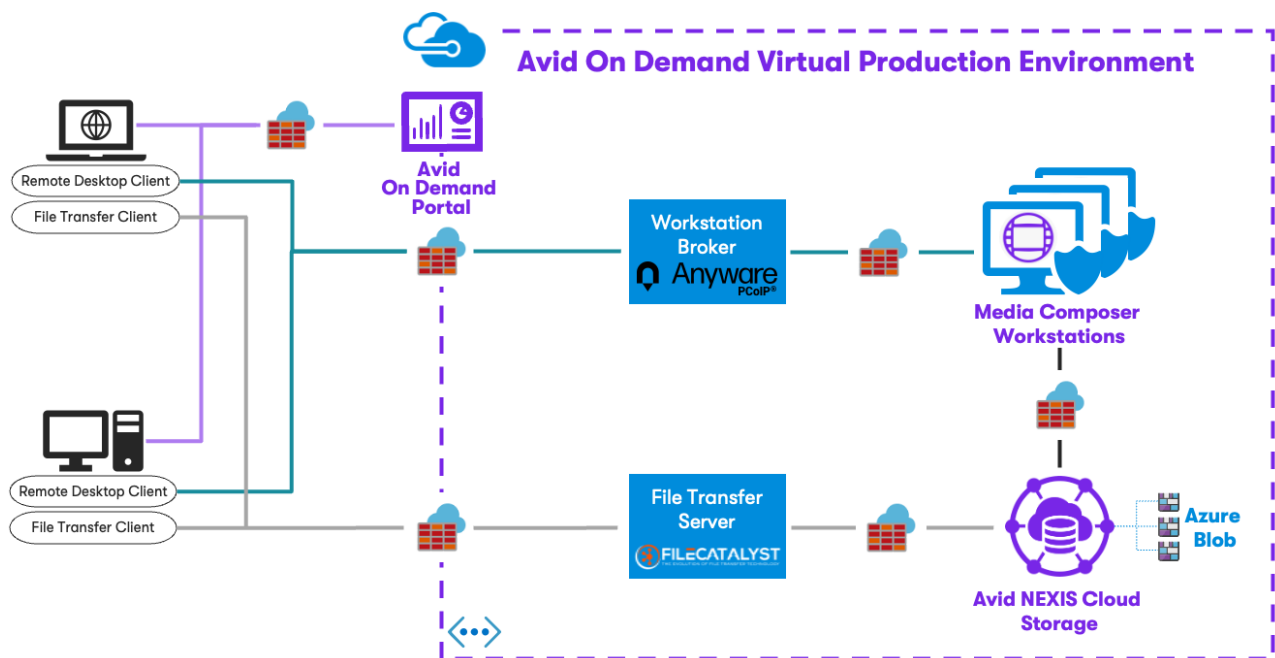
For information on courses/schedules, training centers, certifications, courseware, and books, visit [Avid Learn and Support](#) and follow the **Learn from Avid** links, or call Avid Sales at 800-949-AVID (800-949-2843).

Introduction

This document describes security-related aspects of the Avid | Edit On Demand® (EOD) solution offered in the cloud. It covers areas that are of interest when running Avid products and solutions in cloud environments. Cloud Providers and environments currently include Microsoft® Azure®.

System Diagram

In addition to Avid products and solutions, customers may want to run additional third party software in the designated environment. Avid supports this idea and helps with provisioning the third party software applications. However, Avid does not actively conduct security-related scans or risk mitigations for software that is not part of the respective Avid EOD solution purchased by customers.



Cloud Resources Overview

Systems and solutions provisioned by Avid reside in a dedicated resource group in Avid’s subscription of the Cloud Provider’s environment. When looking at security, two sides require consideration:

1. The infrastructure and provisioning backend.
2. The systems or solutions that customers purchased for their operations.

Avid Infrastructure and Provisioning Backend

After a customer submits an order for an Avid On Demand service, the provisioning backend deploys and configures all components requested by the customer. Provisioning uses Avid code running on dedicated machines in Avid’s Cloud subscription.

Customer Systems and Solutions

Each EOD subscription (customer system and deployment) resides in a dedicated, isolated environment. All resources that the provisioning backend creates are in a resource group dedicated to that system.

An EOD resource group contains a variety of resources, such as:

- Virtual network
- Managed storage
- Virtual machines with resources for Active Directory® (AD), Avid NEXIS®, and Media Composer®
- Virtual machines with resources for access and transfer (third party software)

Avid-Provided Third Party Software

- HP Anyware® PCoIP® (formerly Teradici PCoIP) remote desktop software

For remote editing sessions, Avid's EOD solution uses the HP Anyware software. The client side is either a thin or zero client with the PCoIP software on it, or an application installed on Windows® or Mac® machines. After initiating a connection to the site, the system first authenticates the user. Upon successful authentication, the user connects to a Media Composer workstation (an EOD Edit Seat). The PCoIP protocol uses dedicated ports and encrypts all desktop streaming.

- FileCatalyst® file transfer solution

EOD uses FileCatalyst for file transfers. Up/downloads are point-to-point connections between a client app or, in this case, the FileCatalyst Transfer Agent installed on the user's workstation and the FileCatalyst server in the backend of the system. A Web app initiates the connection. Users then must log in (via HTTPS) and authenticate against the Active Directory in the system's resource group. For the up/downloads, the system uses dedicated transfer ports, and encrypts all traffic between the client and server.

Network

Avid's EOD solution implements network security through VNETs, traffic control, and ports.

VNET

There is a virtual network (VNET) in place for communication between the various virtual machines (VMs) of a system. The VNET of an EOD subscription's resource group is isolated from all other resource groups, including those of other subscriptions purchased by the same customer.

The VNET in EOD uses one subnet. Within that subnet, Avid assigns multiple firewall rules to the network interfaces of the VMs in that resource group. A group of firewall rules contains all the security rules managing traffic into and out of the components in that subnet.

For every group of firewall rules, all inbound and outbound network traffic is blocked, with exceptions only for required traffic between components. Firewall rules are stateful, which means that return traffic for allowed outbound traffic is allowed automatically. All VMs have a private IP address that allows for communication within the subnet. A VM only receives a public IP address when it must be accessed explicitly from outside; for example, the HP Anyware server and the FileCatalyst server.



In Avid's EOD solutions, the HP Anyware PCoIP protocol helps implement access to Media Composer workstations (the Edit Seats). After authentication (by the designated server), the user session gets routed to the specific Media Composer VM. This is why Media Composer VMs do not need a public IP address, as all connections take place within the EOD subnet.

Traffic and Ports

Most of the external network traffic results from up/downloading of data to and from Cloud storage (managed by Avid NEXIS). In addition, the remote connections to the dedicated Media Composer machines also contribute to the traffic. All other network traffic is internal to the VNET and is isolated from the outside.

Table: Inbound Open Ports lists of Avid EOD Solution – Firewall rules / one subnet

<u>Inbound</u> Open Ports				
Destination	Protocol	Ports	Source	Description
AD Server	TCP	5986	Avid Backend IPs	Management ¹
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
HP Anyware PCoIP Connection Manager	TCP	443	Any	PCoIP Connection Request
HP Anyware PCoIP Security Gateway	TCP	4172	Any	PCoIP Control Information
	UDP	4172	Any	PCoIP User Data
	TCP	22	Avid Backend IPs	Management ¹
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
FileCatalyst (Transfer Station)	TCP	443, 900	Any	Communication (SSL)
	TCP	8000 - 8999	Any	File Transfer / Transport
	UDP	8000 - 8999	Any	File Transfer / Transport
	TCP	22	Avid Backend IPs	Management ¹
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
Avid NEXIS	TCP	22	Avid Backend IPs	Management ¹
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
Media Composer	TCP	5986	Avid Backend IPs	Management ¹
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure

¹ WinRM and SSH port rules are set up to “Deny.” Those are allowed only for management tasks conducted by the backend at the point in time it is needed; i.e., user creation and assignment.

Table: Outbound Open Ports lists of Avid EOD Solution – Firewall rules / one subnet

<u>Outbound</u> Open Ports				
Source	Protocol	Ports	Destination	Description
AD Server	TCP	443	Dynamic Storage <Region>	Cloud Provider Diagnostics
	TCP	443	Internet	Windows Updates
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
HP Anyware PCoIP Connection Manager	TCP	80, 123, 443	Internet	NTP, SaaS, and Linux updates
	TCP	60443	PCoIP Agent	PCoIP Agent Protocol
	TCP	443	Dynamic Storage <Region>	Cloud Provider Diagnostics
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
HP Anyware PCoIP Security Gateway	TCP	4172	PCoIP Agent	PCoIP Control Information
	UDP	64172 - 64176	PCoIP Agent	PCoIP Ultra Collaboration Session Data
	UDP	4172	PCoIP Agent	PCoIP User Data
	TCP	443	Dynamic Storage <Region>	Cloud Provider Diagnostics
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
File Catalyst (Transfer Solution)	TCP	443	Dynamic Storage <Region>	Cloud Provider Diagnostics
	TCP	443	Internet	Linux Updates
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
Avid NEXIS	TCP	443	Dynamic Storage <Region>	Cloud Storage
	TCP	3443	Avid Backend	Licensing
	TCP	443	Dynamic Storage <Region>	Cloud Provider Diagnostics
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure
Media Composer	TCP	443	Proxy Service IPS	Media Composer Licensing
	TCP	443	HP Anyware Server IPs	HP Anyware PCoIP Licensing
	TCP	*	Internet	Internet Access
	TCP	443	Dynamic Storage <Region>	Cloud Provider Diagnostics
	Any	*	Cloud Provider Management IPs	Cloud Provider Infrastructure

Encryption and Data Protection

Data at Rest Protection

Avid Cloud Solutions, like Edit On Demand, do not directly use any databases. Third party Software as a Service (SaaS) products (for example, HP Anyware Cloud Access Manager, accessed only through its API) may use databases in their implementations.

For user and video content, Edit On Demand utilizes the powerful Avid NEXIS storage solution. In cloud environments, Avid bases Avid NEXIS storage space on high performance cloud storage. EOD also makes use of data encryption at rest, as provided by the Cloud Provider.

Data in Transit Protection

For data transfer to and from the Edit On Demand environment, Avid uses third party software. All relevant software components involved encrypt data in transit. On a regular basis, Avid verifies that these components follow best practices; for example, encryption algorithm and key size.

Endpoint Protection

CrowdStrike™ protects all servers and hosts of any EOD resource groups that are part of an Avid subscription (except Avid NEXIS; refer to ["Exceptions" on page 15](#)). The hosts in various customer cloud subscription deployments report to Avid's CrowdStrike infrastructure, which allows central management and updating, as well as instant messaging of and notifications to Avid's Operations Teams in case of malware findings.



Avid installs CrowdStrike as an endpoint detection and response solution for your EOD cloud subscription deployment. While Avid does not support any specific solution for you to use on prem or in any cloud, you can find general guidelines and information related to CrowdStrike Falcon in the [Avid Endpoint Security Guidelines](#) document.

Identity and Access Management

Access Channels

Users access the Virtual Desktop Infrastructure (VDI) either through a zero client or through the HP Anyware PCoIP software client. Authentication of users utilizes credentials stored in Active Directory in the subscription's resource group.

For file transfers, users log in through a Web UI. All users have access to storage with privileges granted by their administrator (the `wsadmin` user). Once logged in, the system directs users to the storage (Avid NEXIS Workspaces and folders) to which they have access.



For such administrative tasks, EOD deploys a special user account (`wsadmin`) the customer can use to grant storage access permissions.

Customers do not have direct access to the cloud infrastructure or its resources. Neither do they have access to the Avid deployment systems nor to the backend servers (e.g., Active Directory, Avid NEXIS VM, and others) deployed for their subscription. In addition to the access channels mentioned above, a designated customer administrator can manage all aspects of the purchased environment. The customer administrator logs in using MyAvid credentials which then allows administration of the EOD subscription, such as add seats, add/delete users, download usage data, etc.



MyAvid users, and their credentials, are separate from Avid Edit On Demand subscription users.

Role-based Cloud Access

Accessing Avid's cloud subscription is governed by the Avid Cloud Solutions group's Change Control Process. Only a small number of users are assigned specific roles to access the environment. Furthermore, the Change Control Process requires a ticket to be opened. Only after approval of the ticket, by a second engineer in charge, is the user allowed to access the environment. The Avid Cloud Systems Engineer must configure access rules to allow him/her to connect to cloud resources. Upon completion of the task, those access rules revert and the approver must verify this reversion.

Maintenance Access

Only Avid personnel perform maintenance or other administrative tasks on customers' EOD deployments. For such access, the same rules apply as those outlined in the preceding section.

Additionally, Avid personnel use a dedicated machine or jump station, created only when needed, to access the backend as there is no direct internet access. Avid's company-wide access control policies govern access to such administrative machines. Only a limited user base can access jump stations. Avid records these sessions for auditing purposes. Avid stores and manages recordings within Avid's infrastructure for a retention period of 180 days. The Avid PTG Group handles storage and management of these recordings.

Authentication

Users who want to connect to the EOD environment authenticate by username and password. The Active Directory (AD) dedicated to the environment's resource group verifies the user information and controls access. The following section describes user management details.

User Management

User Account Creation

A customer's subscription administrator, or the designated MyAvid user, creates new EOD users of the subscription through the Avid On Demand portal. The Windows Active Directory (AD) dedicated to each subscription centrally stores all users for that subscription.

User creation triggers automated processes that do the following:

- Generates a random, temporary password for a new user.
- Adds the user to the subscription's dedicated AD Lightweight Directory Access Protocol (LDAP, a protocol for interacting with directory servers).
- Adds the user to the subscription's Avid NEXIS | Cloud Storage as a remote/LDAP user.
- Assigns workstations to the user in the HP Anyware broker.
- Returns a user's random password to the Avid On Demand portal.

Users must change temporary passwords upon first login via PCoIP. The system prompts the user to change the random password to a new, private password.

The Avid EOD Solution enforces a password rotation policy.

If a user's private password is lost, the subscription administrator can reset it to a new random temporary password (through the Avid On Demand portal).

The subscription administrator also can delete user accounts as needed.

Password Guidelines

The following guidelines apply to user passwords for Avid Edit On Demand:

- Maximum password age: 42 days
- Minimum password age: 1 day
- Minimum password length: 7 characters
- Enforce password history: 24



This means the last 24 passwords cannot be used when changing a password.

- Password must meet complexity rules

Complexity rules:

- Uses characters from three (3) of the following four (4) categories:
 - English uppercase characters, A through Z
 - English lowercase characters, a through z
 - Digits 0 through 9
 - Non-alphabetic characters; for example: #, \$, %, !
- Does not contain the user's account name or parts of the user's full name that exceeds two (2) consecutive characters



Have users change their password whenever asked to do so and follow these guidelines to avoid errors.

Monitoring, Logging, and Auditing

Monitoring

Avid monitors its cloud backend service components and services 24x7. Failures or other events trigger alerts to Avid's Cloud Operations team to react immediately. For subscriptions and systems, Avid collects health and performance data and stores it in a central repository. The retention period for such data is 60 days. The system sends alerts for certain events to a broader group of Avid engineers. This group has additional Avid product knowledge and can triage the issues for immediate resolution or for a scheduled maintenance window.

Logging and Alerts

The system activates cloud-based logging for backend services as well as for customer subscriptions. Certain events generate alerts that route to the Avid operations team and/or Cloud Solutions engineers, depending on their responsibility.

Activity Logs

In the Cloud infrastructure, there is a [platform log](#) that provides insight into subscription-level events. This activity log includes information on when a resource changes, or a virtual machine starts, and other items. Avid personnel can view the activity log in the Cloud Provider's portal or retrieve entries with the help of an API.

Firewall Flow Logs

In EOD deployments, Avid activates firewall Flow Logs in Azure. Flow Logs are a feature that allows Avid to log information about IP traffic flowing through a firewall. Flow data is sent to storage accounts where it can be accessed and exported to a visualization tool, to Security Information and Event Management (SIEM), or to an Intrusion Detection System (IDS). Customers do not have direct access to this information.

Audit Trail

Avid has implemented logging of usage data for Editing sessions and File transfers in EOD subscriptions. Avid stores such information in a database in the backend and retains it for a period of one year. Customers can access data through the Avid On Demand Portal and can download a report in CSV format for further processing.

Detailed technical session logs of the various components (Avid NEXIS and third party software like HP Anyware and FileCatalyst) are captured, but only available to Avid personnel. In case of a breach, customers should contact Avid Customer Support, and ask for support and investigation into the issue. Avid does not allow customers to access the backend.

Vulnerability Assessments

For releases to Cloud Subscriptions, Avid implemented a process that requires a security checklist sign-off from all stakeholders for the respective release. This process makes sure that, from design to implementation and deployment to the cloud, all parties confirm that their deliverable complies with best practices. In addition, Avid scans source code using source code analysis tools, and also regularly scans test deployments for vulnerabilities.

System Scans

Prior to releasing a solution to Production and making it available for customers, Avid conducts vulnerability scanning of test deployments using the Nessus® scanning tool. Avid uses the results from the scans to harden the environment.

Code Scans

As outlined earlier, the source code of Avid standard products gets checked during product development and during the product's lifecycle. To make sure Avid does not introduce additional risks to the deployment code, we conduct additional recurring code scans with Snyk®. This solution helps discover and fix vulnerabilities in the code introduced by other components. Avid assesses any findings directly so that releases do not add additional risks to the solution.

Vulnerability Remediation

A variety of software components are employed in Avid's Cloud Solutions:

- Virtual machines with their operating systems
- Avid software products
- Third party software

Operating Systems

For each release (and at least once a quarter), Avid checks and updates the corresponding OS builds as needed. Long-running deployments implement a patching schedule that covers installation of critical and high-risk security patches. Zero-day vulnerabilities are taken care of immediately, and patching is done as soon as a patch becomes available.

Avid Products and Components

All Avid products and components have their own release cycles. Security review is part of each product release. In case of critical issues of any component that is employed in the Avid EOD Solution, Avid updates the relevant piece of software once a fix becomes available.

Third Party Software

Several third party software products contribute to Avid's Edit On Demand. While Avid is not responsible for the security of third party software, Avid observes any security-related updates and makes sure to incorporate them into our releases. Business critical fixes roll out to customers as soon as they become available.

Penetration Testing

Avid conducts penetration testing on an on-demand basis. We intend to increase the frequency of penetration testing to cover every major release.

Avid does not share penetration test results with customers, but we support customers who want to do their own tests on an Avid Cloud deployment. While such tests should be done in close cooperation with Avid's Cloud Solutions Engineering, the level of engagement needs to be fixed upfront. If the involved effort for preparing the environment for penetration testing exceeds two (2) hours, Avid might involve the Professional Services team (which will be a paid engagement).

Exceptions

For product compatibility reasons, the Avid NEXIS product is excluded from endpoint protection with CrowdStrike. As part of the product lifecycle, Avid Engineering validates releases accordingly. Avid's goal is to use endpoint protection on Avid NEXIS in the future. Note that for other products in your EOD solution, Avid does use CrowdStrike for endpoint detection and response.

Avid limits direct access to Avid's Cloud subscription, infrastructure, and its resources to Avid employees, and permits only a small group of engineers to connect and act on those resources. If customers need maintenance, investigation of issues, and/or other cloud environment-related work, they should reach out to Avid Customer Support and ask for help.

Logs of any kind within the Avid EOD subscription are accessible to Avid personnel only. In case of a breach or if logging details are needed, customers should contact Avid Customer Support and ask for support and investigation of the issue.

Avid does not share testing results, neither from vulnerability assessments nor from penetration testing. In case of any kind of security assessment customers may want to conduct, they should contact Avid Customer Support. Requests will be routed by this group within Avid to the appropriate team.