The Engine Shed Station Approach Bristol BS1 6QH

YELLOWDOG

YellowDog Rendering Security Overview

October 2018

YellowDog's Security is constantly being updated and expanded. Information contained herein may therefore be subject to change.

For further details, customised requests, or detailed enquiries, please contact the YellowDog team on woof@yellowdog.co

Contents

Introduction

When designing the YellowDog service, security was the primary design consideration.

- YellowDog customer distributed components are digitally signed using a Microsoft Authenticode code signing certificate e.g. YellowDog agent, plug-ins, and YellowDog Sync.
- Communication is encrypted, primarily using HTTPS, whenever it is transferred between computers or servers, examples include:
    - YellowDog Sync and Platform
    - Platform and the YellowDog Agent (running on render nodes)
    - Customer uploads and downloads between the customer web portal and client computers
    - Customer and web portal.
- All render nodes authenticate with the YellowDog Platform to ensure that they are authentic authorised nodes
- All YellowDog software write logs both to YellowDog servers and 3rd party secured infrastructure to ensure full audit trail even if YellowDog logging were unavailable or compromised
- Credit card payments are handled by Stripe with no card details residing on or passing through YellowDog servers
- YellowDog works with multiple cloud datacentre providers allowing nodes to run in multiple datacentres should there be issues with one or more providers
- Denial of service measures are built in to all our datacentre locations with all platform infrastructure being available through a second secure internal network should public interfaces be attacked. Traffic is automatically managed to protect against denial of service attacks. A denial of service attack could potentially affect public interfaces e.g. web portal, but render jobs continue and agents such as plugins and YellowDog Sync are able to continue operating though our global infrastructure which links datacentres without the need to go over Public Internet connections.

Both YellowDog the organisation and our YellowDog rendering service are ISO 27001: 2013 registered and compliant (this is an internationally recognised standard for data security). To ensure continued compliance we have monthly ISO 27001 review meetings and are audited by a third party annually. Rather than running through ISO 27001 (requirements upon which the MPAA certification is based) this document outlines the main areas that have been addressed.

Security Areas

Facility

Datacentres

YellowDog rendering services using its private pack of public cloud render nodes operates exclusively from ISO 27001:2013 certified datacentres. The majority of these datacentres are also SOC 1 type II (SSAE 16 and ISAE 3402) and SOC 2 type II certified.

Office Location UK

The UK office uses key card access to the building upper floor where the YellowDog offices are located. The YellowDog offices are locked and alarmed when no members of staff are present. There is no access to YellowDog offices by members of the public. All meetings with customers at YellowDog offices are conducted in meeting rooms within our office building, these are in a separate location to our offices. Access to our offices is granted only to employees.

CCTV is installed on all corridors and common spaces within the building and operated by the landlord's security personnel.

YellowDog does not have printing facilities and operates an entirely paper-free environment.

YellowDog has its own VLAN within the building that is monitored and maintained by a 3rd Party network security specialist.

All computers physically located onsite have all the usual policies you might expect from compliant organisations such as locked down status, anti-virus/anti-malware software, and hardware encrypted 256 bit AES local disks.

No customer renders take place at our offices, these only occur within secure datacentre environments.

Data transfer and YellowDog Plugin permissions

YellowDog Plugins add additional functionality to 3D modelling software such as the ability to export data and pass it to YellowDog Sync for transfer to YellowDog to start rendering. The Plugins uses the same privileges as the user account that has installed them into 3ds Max, Maya, Cinema 4D or Modo. There is no need to grant special access for the Plugin.

If assets required for the render are needed and are on a shared network resource, then the Plugin and Sync will access those files in the same way that Max or Maya would, compress them into a .zip file on the local workstation before securely sending the .zip to the YellowDog Platform. YellowDog Sync will not access any data on workstations or the network that is not linked to the render job. All data transfer is authenticated and encrypted over HTTPS.

YellowDog Sync automatically and securely downloads the completed renders, one frame at a time, from the YellowDog Platform. All data transfer is authenticated and encrypted over HTTPS for security.

Office Location Lithuania

Part of our development team are based in Kaunas, Lithuania and are in a building with high security standards. The same standards that exist in the UK for locked down PCs and encrypted drives are applied to the YellowDog development team. CCTV is in place within the building.

Culture

A large part of any security plan is ensuring awareness among staff. Our Operations team is based in the UK office; awareness of security procedures has become second nature as a result. We have regular visits by our Head of Operations, Director of Engineering, and CTO to the office in Kaunas for awareness training and to monitor onsite practices. A staff training course in information security has been created and will be run for all new joiners and annually for existing staff.

Staff

Staff Checks

At present, employment and personal references are sought for all new members of staff. We are introducing Disclosure and Barring Service (DBS) checks for all new and existing employees.

Employment and Outsourcing Contracts

YellowDog contracts are very strong with regard to intellectual property protection and security procedures. Consequences of non-compliance by staff, whether permanent employees or contractors are made very clear.

Authentication Security

All system related passwords are secured using a specialist credentials application hosted on our own infrastructure. These passwords are stored in a 256 bit encrypted database. Dual factor authentication is used for access to all 3rd party datacentre infrastructure and activity logged. Linux systems are secured with certificate only authentication. Hosted Windows systems are only accessible via VPN or from our office static Public IP address. Staff can access company email from their computers and mobile devices.

3rd Party Office Systems

YellowDog outsources email and CRM functions to Microsoft and Capsule CRM respectively, both of whom offer industry standard based security including dual factor authentication. Staff do not have access to customer passwords.

Development Procedures

YellowDog uses the Agile Scrum software development methodology, delivering new capability in timeboxed two-week sprints. No changes are planned for development procedures such as code repositories, check in/check out, code reviews and test procedures. All current development and release management tools are based upon industry leading tools such as Jira/Confluence and Jenkins/Team City.

Penetration Testing

Penetration tests are carried out by an independent monthly against both our publicly accessible platform and internal systems. A security review meeting is held monthly and our Operations team is available to work on any newly identified security vulnerabilities 24/7.

Personally identifiable data

YellowDog stores customer data that is potentially personally identifiable in business email, Capsule CRM and the YellowDog Platform (customer registration information). This is normally limited to name, business address, phone number and email address. YellowDog does not share any personally identifiable information with 3rd Parties expect upon explicit agreement with the customer, e.g. an agreement to a joint promotion. Business email is stored online within Microsoft's Office 365 infrastructure in their Dublin Datacentre, emails received within the last 3 months are cached locally to hard disks, but only where the disks are encrypted to the 256-bit AES standard. Emails are also synchronised to mobile devices where the storage is encrypted and a password is required to unlock the device. Anti-virus and anti-malware is installed on PC devices to offer an additional layer of protection. Capsule CRM dual-factor authentication is rolled out to all CRM users within YellowDog. The YellowDog Platform is actively monitored for access attempts and administrative access is secured over SSH from a selected list of our own Public IP addresses and accessed only using certificates.

Customer Intellectual Property

During rendering, scenes are copied to render nodes and deleted upon the completion of the render. Decommissioned bare metal render nodes are securely wiped to ensure that data is not retrievable. For virtual nodes, the storage is reallocated to the SAN or local SSD storage pool as soon as the node is terminated. Storage volumes for virtual nodes are stored as single files, the reference table for which is cleared when the node is terminated. Customer uploaded scenes and render output is stored on YellowDog servers for retrieval purposes by the customer. Long term storage is in encrypted object storage. Should customers want their scenes and render output deleted from YellowDog, this is done by selecting the job within the web portal and choosing "Delete" which removes all copies from YellowDog system.