OpenEye®

OPENEYE WEB SERVICES

PLATFORM SECURITY OVERVIEW

LIBERTY LAKE, WA • (509) 232-5261 • OPENEYE.NET

CONTENTS

INTRODUCTION

Security is a top priority for companies doing business in the cloud. As the number of cloud connected devices continues to grow, so does the risk of data breaches and the potential for unwanted access to vital information. In order to mitigate these risks, organizations need a video surveillance platform that leverages the latest in network security, proactively protecting against people or programs that might cause harm. OpenEye Web Services (OWS) is a secure and powerful web-enabled platform that reduces maintenance costs and streamlines the management of video surveillance systems.

Customers using OpenEye Web Services can store account credentials and access information on cloud servers without fear of exposing their security system to potential threats. OpenEye's service ensures the security and integrity of your data by implementing technologies that are designed to prevent a wide range of hacking and data loss scenarios. The following security overview outlines how OpenEye shields your data from unwanted access by hackers, and how we protect it from physical threats such as natural disasters, hardware failure, and on-site tampering.

DATA & NETWORK SECURITY

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication requires more than one independent form of credential to verify the user's identity. OpenEye Web Services (OWS) uses multi-factor authentication to ensure that unauthorized parties are unable to gain access to user accounts.

Once enabled, account access is subject to a user successfully entering a time restricted and unique authorization code delivered to their mobile device via SMS. This ensures that an account cannot be accessed even if the user's login credentials are compromised. Similarly, if the system administrator wishes to change their password, they must first enter the randomized code delivered via SMS. This prevents a third party from locking a user out of their account by changing passwords.

TRANSPORT LAYER SECURITY

The Transport Layer Security (TLS) protocol ensures privacy between communicating applications and their users on the Internet. TLS is one of the most common security protocols used by sites dealing with transactions involving sensitive data.

All data transferred between the recorder, OpenEye Web Services, and the remote client is encrypted using the TLS protocol. Since eavesdroppers don't know the server's private key, it is infeasible for them to hijack the connection. Upon successfully establishing a TLS connection, authentication, control information and video data transferred between the client and server is encrypted. Third parties cannot tamper with or read this data.

NO INBOUND PORTS OPEN ON NETWORK FIREWALL WITH OTC

Proper user authentication and a successful TLS handshake will establish what is known as an Outbound Trusted Connection (OTC). With an OTC, a recorder will only communicate with and respond to verified clients. This OTC methodology also enables WAN client connections without permanently opening an inbound port on the network's firewall. The result is tighter network security and does not require specialized IT configuration at individual sites.

Recorders using traditional connection methods listen to and can potentially respond to any incoming network traffic. Apex recorders only respond to requests from OWS servers upon successfully creating an outbound TLS connection once established by an authorized user.

CROSS-SITE REQUEST FORGERY PROTECTION

A Cross-Site Request Forgery attack forces users to execute an unwanted action on a site they're currently authenticated with. This is typically accomplished by tricking the user into clicking a decoy link or logging in to a fake version of a legitimate website. To prevent this, OpenEye has implemented CSRF protection techniques similar to those implemented by banks, stock traders, and other websites that require a high degree of online security.

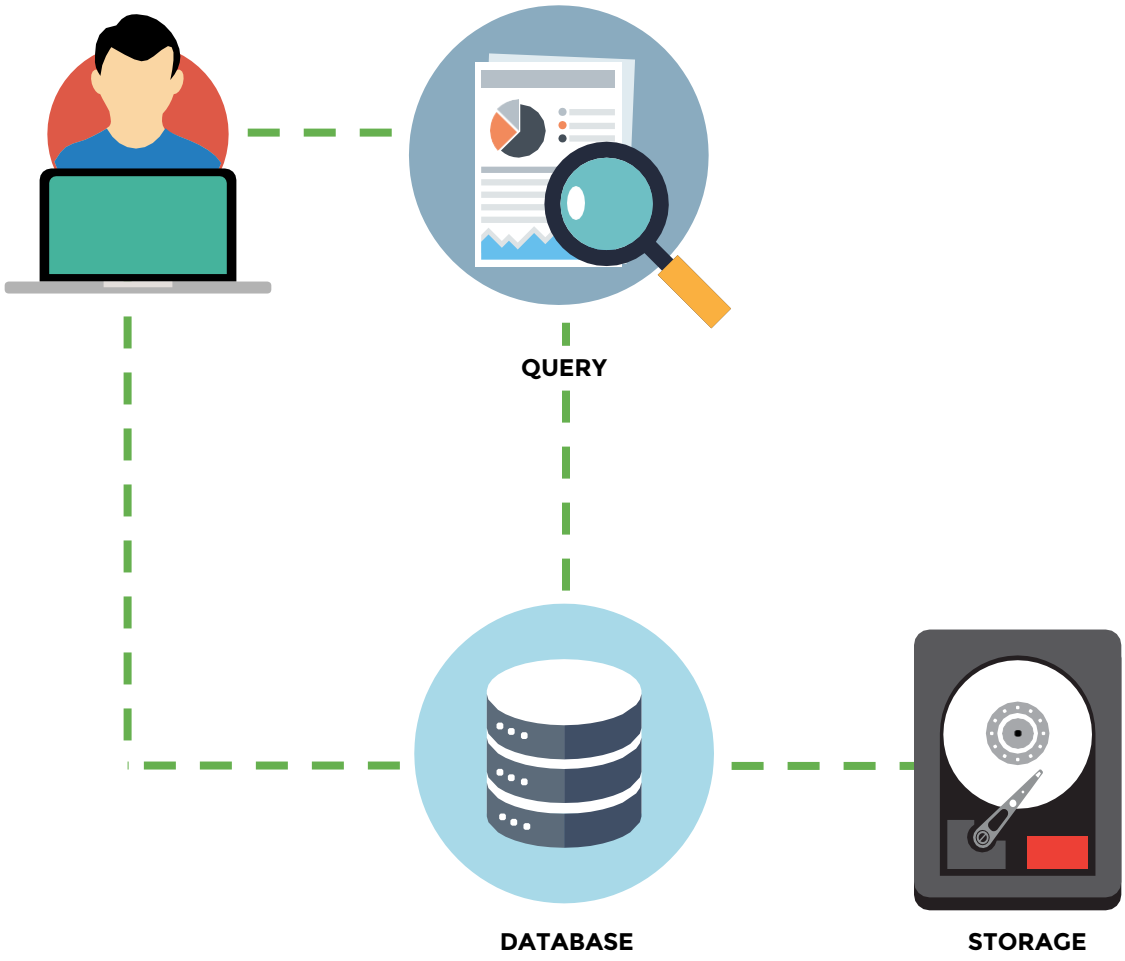
PROTECTED LOGIN CREDENTIALS

Processes compliant with the National Institute of Standards and Technology (NIST) protect users' passwords from hacking attempts. These processes encrypt stored passwords, making them practically unusable, even in the event of a server breach. The NIST reviews these processes on a semiannual basis to look at conformance and assess new methodologies.

LOGICALLY SEPARATED DATA

Customer data is logically compartmentalized through a tenant isolation layer. This acts as a virtual storage location to keep customer data contained and ensures that even a direct attempt to access another customer's data by manipulating a query will fail.

User data is separated into its own virtual container independent of queries and is protected when it's active or inactive. Using this framework, users can't affect the integrity of other users' data, even if they attempt to gain access to their container through a fraudulent data query. All credentials, connection information, and video clips are stored in virtual containers, and thus protected.

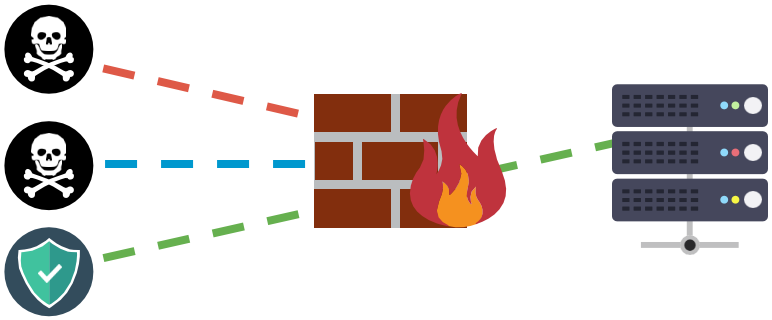


DATA INTEGRITY

One of the benefits of OpenEye's cloud managed video model is that customer video stays on the local recorder, within your protected network, and is only transmitted over the WAN when you choose for it to. The cloud is used to store user groups, permissions, exported video clips, image thumbnails from alerts or reports, and health monitoring data. It is extremely important this cloud data be redundant and available at all times to users who wish to access it. OWS multiple mechanisms to ensure the high availability and redundancy of cloud data.

FIREWALLS

Customer data in the OWS cloud is stored on a private network that is not directly accessible from the Internet. This network is secured by firewalls that only allow access to and from the designated application servers. In the unlikely event of a breach in the private network, firewalls filter all incoming and outgoing traffic, allowing only approved users and devices to access OWS cloud servers.



ENCRYPTION

Cloud data stored on OWS cloud servers is automatically encrypted using AES-256, the same encryption used in banking, health care, and government. OWS cloud user data is encrypted using a data encryption key, which is then itself encrypted and stored on a separate server for added protection. Video clips saved to OWS are encrypted the same way. This ensures that backup cloud data cannot be accessed by an unauthorized party.

DATA REDUNDANCY

ROLLING BACKUPS

To protect users from loss of their cloud data (user groups, exported clips, alert and report data), all OWS cloud server locations store 60 days of rolling backups. This ensures cloud user data will not be lost even in the event an entire cloud data server or data center is rendered inoperable.

OFFLINE STORAGE

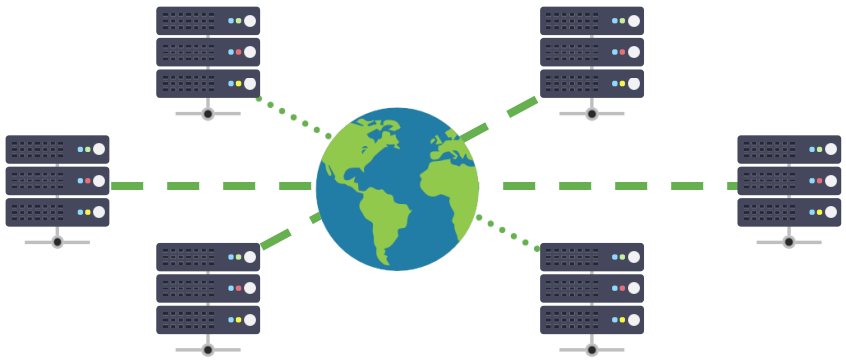
As a final layer of data protection, thirty days of backup cloud data are stored 'offline', isolated from public networks, to prevent unwanted access and tampering.

OWS PROXY SERVER SUPPORT

OpenEye Web Services supports the use of network proxy services to securely aggregate HTTP communication in corporate environments. OWS requires an HTTP 1.1 compliant proxy and can accommodate null or basic authentication. Relayed connections will route all video traffic through the proxy host, while a peer-to-peer negotiated connection will deliver video directly from the recorder to the client, while control messages will remain routed through the proxy.

HIGH AVAILABILITY

The data centers housing OWS cloud user data operate on the principle of high availability. This approach focuses on eliminating single points of failure, delivering reliable crossover points, and detecting failures as they occur. Using high availability engineering, servers can add redundancy, so that one component failure won't spread to the rest of the system. This approach to system engineering leads to less downtime.



REDUNDANT SERVERS

OWS cloud user data is securely stored on multiple servers within each data center in order to add redundancy and minimize downtime. This prevents users from losing or being unable to access data in the event of an unforeseen failure.

COLLOCATION

OWS cloud user data is securely stored in multiple data centers across diverse geographic regions. Data replicates throughout these centers, mitigating the risk posed by catastrophic hardware failure, sabotage, or natural disasters. If any single data center is compromised, an automated process seamlessly redirects traffic from the affected location to unaffected data centers. Redundant data centers are designed to handle all redirected traffic, meaning the failure of any one data center won't affect the quality of a user's service.

STORAGE DEVICE DECOMMISSIONING

As OWS cloud data center servers are upgraded and decommissioned, storage devices from systems are degaussed and physically destroyed using processes recommended by the Department of Defense and National Institute of Standards and Technology. This ensures that unauthorized third parties are unable to recover data from decommissioned servers.

PHYSICAL SECURITY

INFRASTRUCTURE

Ensuring the physical safety of servers is as critical as electronically protecting the data housed on them. User data is stored in state-of–the-art data centers designed to withstand physical and geological threats.

UPS SYSTEMS

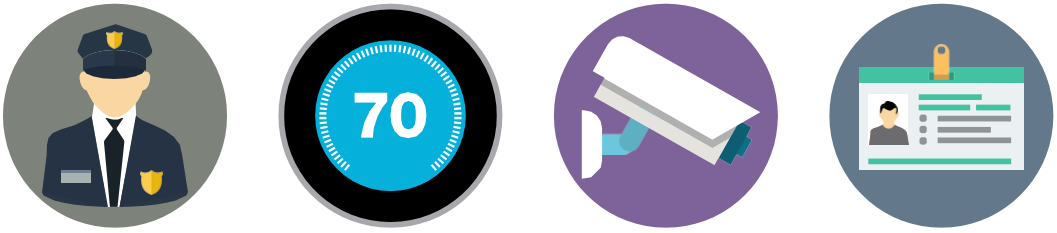
OWS data centers feature fully redundant power systems that deliver uninterrupted 24/7 operation. In the event of electrical grid failure, UPS systems and generators ensure power continues to flow to servers as well as to the entire facility.

FIRE SUPPRESSION

OWS data centers are equipped with automated fire detection and suppression systems. Gaseous sprinkler systems suppress fire without damaging critical equipment.

CLIMATE CONTROL

Data centers with large numbers of servers require an extensive climate control system to keep machines working at peak efficiency. Thermostats monitor conditions to maintain a constant level of temperature and humidity ideal for server operation.



24/7 GUARD

Data centers housing OWS user data are monitored 24/7 by trained security staff. All personnel are screened upon leaving areas containing user data.

ACCESS CONTROL

Restricted access to data centers is strictly enforced through multi pass two-factor authentication requiring staff to authenticate a minimum of 2 times before accessing data center floors. An authorized staff member provides continuous escort to any visitor or contractor on site.

SURVEILLANCE

State-of-the-art electronic video surveillance systems and intrusion detection systems are in place for round the clock monitoring of data center locations.

BACKGROUND CHECKS

Personnel with direct access to data center servers housing OWS data receive a thorough background check. All administrative actions carried out by OpenEye employees are tracked and audited to ensure that no unauthorized changes are made to your service.

OPERATING SYSTEM SECURITY

OS UPDATES

OpenEye offers remotely deployable operating system updates to all platforms in the product lineup. Professional vulnerability scans are performed on each incremental software release, and reports are available for review upon request.

Windows

OpenEye provides a hosted WSUS [Windows Server Update Service] for all Windows 10 IoT products. Microsoft critical security updates are delivered by the internal update system of the OS once they are tested and approved by the OpenEye quality assurance team.

The update service is enabled by default out of the box, with an opt-out icon on the Windows desktop for organizations managing software updates internally.

Linux

OpenEye delivers key updates to the Linux OS via a two phased approach. Linux Kernel modules and userspace components [such as Java and libc] are updated on a regular basis via system image ISO for new products leaving the factory. Critical patches to address zero-day and high severity CVE vulnerabilities are also released on an immediate basis once the component vendor releases an update and OpenEye quality assurance teams perform validation.

CONCLUSION

OpenEye Web Services simplifies the management of your video solution, delivering value beyond physical security, while simultaneously reducing the burden on IT. Using state-of-the-art facilities and industry-leading technology, OpenEye Web Services shields user data from unwanted access and protects it against physical threats.

- The OWS infrastructure places a heavy emphasis on multi-factor authentication, numerous forms of user authentication, protected credentials, and permission controls.
- The OWS infrastructure reduces the burden on IT by eliminating the need to forward and permanently open inbound ports on the network firewall.
- OpenEye secures user data through firewalls, encrypted backups, and redundant storage across multiple locations.
- Access to servers containing user data is tightly controlled and carefully managed.
- Access control, CCTV systems, and security guards monitor servers 24/7, enforcing user credentials and access rights.

At OpenEye we take the security and integrity of your data seriously. Rest assured, as your online security needs evolve so will the OWS platform.

To learn more about the OpenEye Web Services platform and how you can benefit, visit www.openeye.net or contact OpenEye at (888) 542-1103.

OpenEye®

The information in this publication is believed to be accurate in all respects. However, OpenEye cannot assume responsibility for any consequences resulting from the use thereof.

The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes.

OpenEye

(509) 232-5261

Liberty Lake, WA • USA
www.openeye.net

33478AH