videri

videri.com

SECURITY OVERVIEW

THE VIDERI PLATFORM

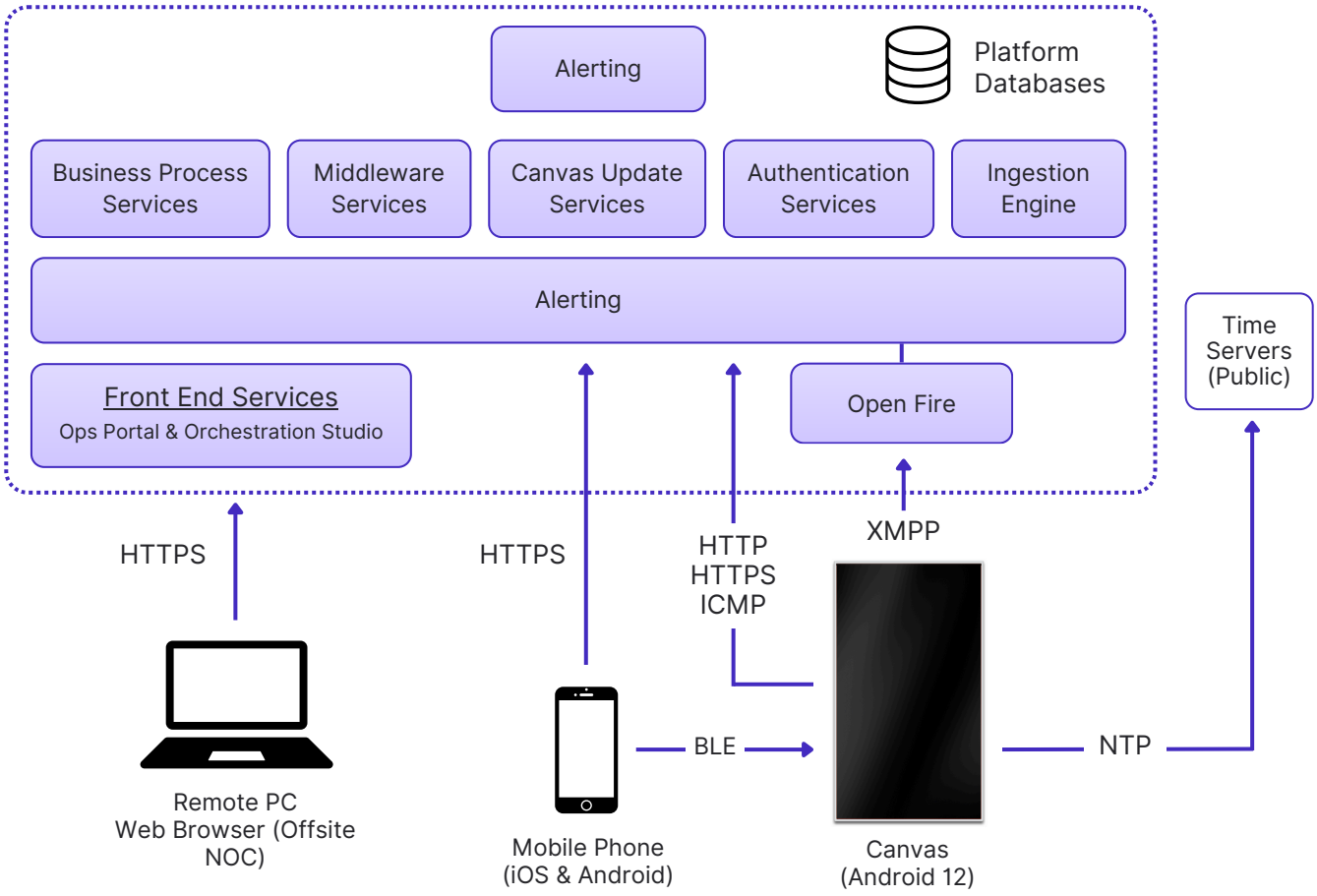
APRIL 2024

Security Overview

Our top priority is to provide you with a robust and secure platform. We maintain high security processes across all aspects of our platform.

Videri performs annual security audits and penetration testing with a 3rd party firm. Results are not shared outside the company. Immediate action is taken to resolve any threats rated medium or above at the code, architecture or operational level.

Videri Cloud Services (AWS)



The Videri Platform uses the AWS Cloud and leverages their security policies and practices. https://aws.amazon.com/security/

Network Connectivity Requirements

For connectivity to the cloud-based network the Canvas and Videri SparkBridge, SparkBridge+ and SparkBridge+ Sealed - use the following ports and protocols:

Protocol	Ports	Port Direction	DINS
HTTP	TCP 80	Outbound	ANY - our Canvases and SparkBridge* may contact public websites as part of normal signage operations. Depends on content. HTTP is used only in the case that a 3rd party CMS / website uses HTTP and it is scheduled to the canvas.
HTTPs	TCP 443	Outbound	ANY - our Canvases and SparkBridge may contact public websites as part of normal signage operations. Depends on content. All Videri hosted content uses HTTPS.
XMPP	TCP 5222 and 5223	Outbound	msg.videri.com
NTP	UDP 123	Outbound	The following NTP pools will be contacted. Note that each pool contains 1000s of individual servers with specific IPs. Generally, it is required to whitelist the NTP protocol rather than individual IPs. • time.nist.gov • 0.android.pool.ntp.org • 1.android.pool.ntp.org • 2.android.pool.ntp.org • 3.android.pool.ntp.org • 0.us.pool.ntp.org • 1.us.pool.ntp.org • 2.us.pool.ntp.org • 3.us.pool.ntp.org
ICMP		Outbound	msg.videri.com

*SparkBridge henceforth refers to all 3 models, SparkBridge, SparkBridge+ and SparkBridge+ Sealed.

Canvas Security

- There are no externally accessible hardware ports on Canvases.
- Canvases have no open network ports in “listen” mode and will not accept any incoming connections.
- Android debugging commands have been proactively disabled.
- All cloud-based communications are encrypted using standards based on open-source encryption technologies.
- Direct commands from the Videri Mobile application over Bluetooth is the only available method of communication with the Canvas. Bluetooth communication is encrypted with a key stored in the Canvas’s secure storage area and user authorization to connect is handled by the Videri cloud.
- All software installed on the Canvas must be signed and can only be installed with access to the secure Videri cloud portal. The chain of trust for system software starts with unique keys burned into the CPU, preventing third party software from being accepted by the OS.
- If you choose this option in your settings (not a default), all content on the Canvas is signed with an MD5 hash and you can compare prior to playback to ensure no Canvas content has been modified.
- Videri conducts regular audits of code patches available by Google to ensure that the latest security updates are incorporated into the operating system and distributed to Canvases.

SparkBridge, SparkBridge+ & SparkBridge+ Sealed

- Android debugging commands have been proactively disabled.
- All cloud-based communications are encrypted using standards based on open-source encryption technologies.
- Direct commands from the Videri Mobile application over Bluetooth is the only available method of communication with the SparkBridge*. Bluetooth communication is encrypted with a key stored in the SparkBridge’s secure storage area and user authorization to connect is handled by the Videri cloud.
- All software installed on the SparkBridge must be signed and can only be installed with access to the secure Videri cloud portal. The chain of trust for system software starts with unique keys burned into the CPU, preventing third party software from being accepted by the OS.
- All content on the SparkBridge is signed with an MD5 hash and compare prior to playback to ensure no content has been replaced.
- Videri conducts regular audits of code patches available by Google to ensure that the latest security updates are incorporated into the operating system and distributed to SparkBridge devices.

Backend Security

- Videri’s platform uses the OAuth 2.0 open standard for authorization. Every Videri service and endpoint is treated as a third party by the Authorization Server. Every protected resource requires a valid access token provided by our identity management solution. Therefore, if one service is compromised, the remaining services are not immediately threatened.
- Videri uses standards based on open source and third-party identity management solutions to ensure compliance with the strictest security standards of our partners and customers.
- Access to servers is managed by AWS key management tools. All access is through the use of public-key cryptography and requires a 1024-bit SSH-2 RSA key pair to login.
- Videri also uses AWS Identity and Access Management (IAM) user management tools to finely manage access rights, and in particular, key revocation for operations personnel.

Operational Security

All access to the cloud product is logged regardless of access level, this includes Videri employees as well as customer access:

- For customers not using SAML federated sign-on, Videri's own identity management solution enforces strong password, password rotation.

Videri Privacy Policy

Videri cares about your privacy. This privacy policy applies to all of our products, services and websites offered by Videri Inc., or its partners, subsidiaries or affiliated companies. We refer to all of these as Videri's "Services".

Videri Follows Privacy Policies Required by Law

Videri follows the legal advice provided in several countries, including, but not limited to, the California Online Privacy Protection Act (CalOPPA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the EU's General Data Protection Regulation (GDPR) act, and Australia's Privacy Act of 1988. We strive to keep up to date and to ensure our customers are covered by the latest privacy regulations.

When we ask for information, we keep track of where the information is collected. If you provide us information, we will apply the policy according to your country's privacy laws. When in doubt, we will follow commonly accepted standards such as the GDPR.

Videri Follows Privacy Policies Required by Third Party Services

In the case where Videri uses third party services such as Google Analytics or Facebook Appstore, we will publish the privacy policy in accordance with those agreements.

How does Videri use your information?

- Create and administer your account
- Asses the needs of your business to determine suitable solutions
- Send you product updates, marketing communication (with permission) and service information
- Respond to customer inquiries and support requests
- Analyze data, including through automated systems and machine learning to improve our services and/or your experience

[For more information contact us at info@videri.com.](mailto:info@videri.com)