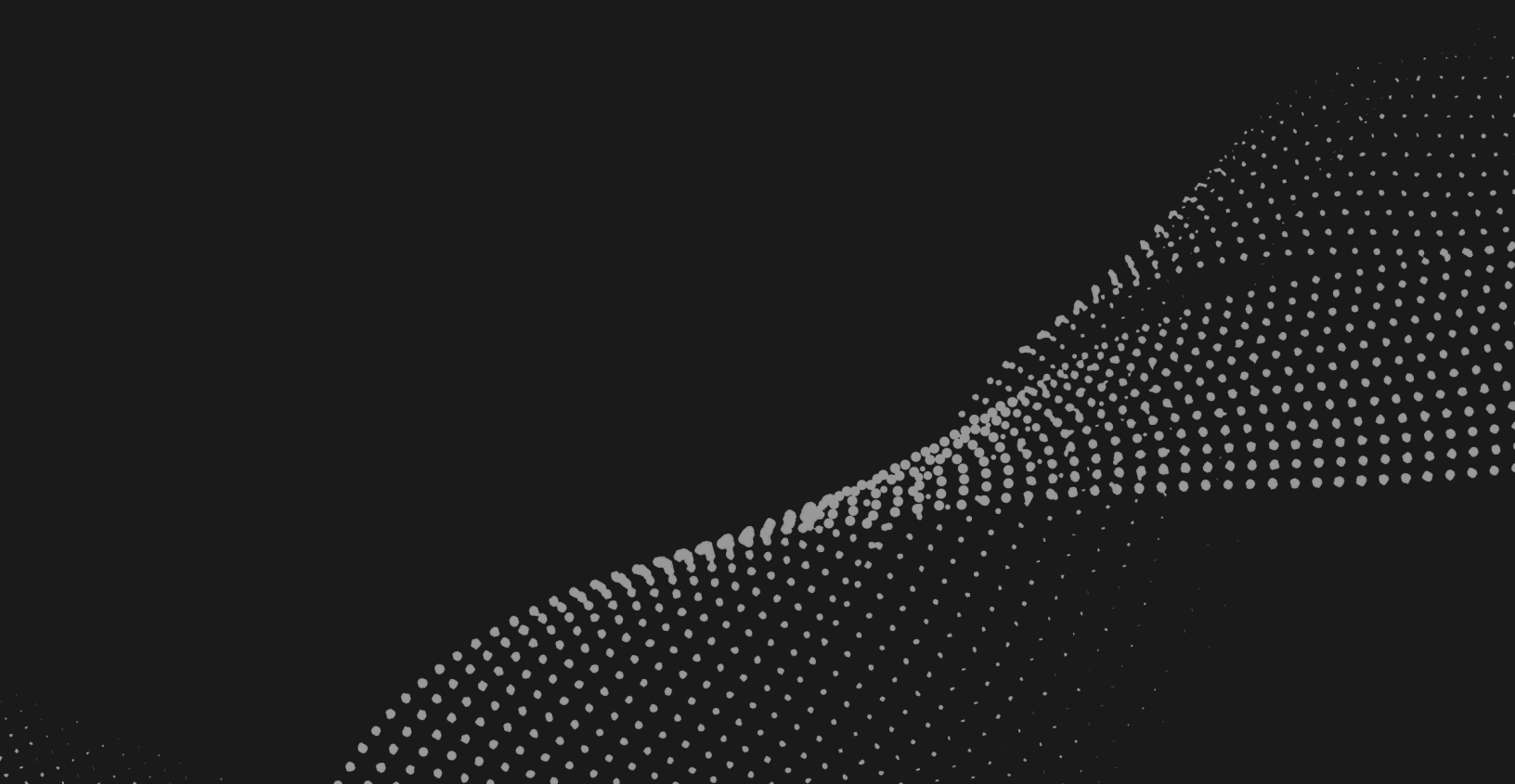


**USERFUL™**

## **Security Guide**



Legal Department,  
Customer Organization

To All Readers

This document provides a comprehensive security overview of the Userful Infinity Platform. Userful deploys a secure local server with a locked-down operating system and no third-party applications. Customers have full control over their security, from role-based access control to locking down all components in an isolated (offline) network, to deploying a private cloud infrastructure.

For information relevant to Decisions control room deployments, see page 6 for technical details and **Appendix A** for an example security vetting questionnaire.

For information relevant to Engage digital signage deployments, see page 11 for technical details and **Appendix B** for an example security vetting questionnaire.

# Index

<b>Platform Security Summary</b>	4
Server Architecture	4
Client Architecture	4
Management	4
Optional - External Data Sources	4
Architecture Overview	5
Userful Data Processing and Privacy	5
Userful's Business Model	5
<b>Useful Decisions and Dedicated Servers</b>	6
Operating System Base & Administration	6
OS Hardening Measures	6
Server Deployment	7
Dual Network Interfaces	7
No Internet access	7
Network Services	8
Network Ports	8
Information Stored on Useful	9
Additional Steps to Secure Useful	9
<b>Useful Engage</b>	10
<b>Useful Manager, Useful Support, and Data Integrity</b>	13
Useful Manager	13
Useful Cloud Servers	13
Useful Servers	14
System Access	14
Data Storage	15
uClient	15
Useful uClient Adapter	16
Useful Zero Clients	16
<b>Network Security</b>	17
<b>Software and Role-Based Access Control (RBAC)</b>	18
Administrator Account	18
Role-Based Access Control	18
<b>Conclusion</b>	19
<b>Appendix A: Example Questionnaire, Decisions Control Room Deployment</b>	20
<b>Appendix B: Example Checklist, Engage Digital Signage Deployment</b>	21

# Platform Security Summary

The Useful Infinity Platform™ consists of elements in three categories. The client usually chooses one element from each category to build their solution.

## Server Architecture

Useful **dedicated** servers are installed within the customer's premises and perform all data acquisition, processing, and transmission within the customer's secured network. Useful servers do not store or reproduce any customer data. Information is transmitted to local displays over an isolated network segment in video format only.

Useful **Cloud** servers are hosted within Useful's secure AWS environment where they distribute content and control signals to uClient devices but do not acquire or re-transmit data.

## Client Architecture

Useful **Zero Clients** are simple purpose-built devices that receive information encoded as images from dedicated servers and perform a simple operation to turn the data into HDMI video-out. They do not contain any local storage or other processing capabilities. They will only function within the same premises as their controlling server.

**uClient** is a secure software application that can be installed on a variety of digital signage platforms within customer premises and can connect to dedicated or cloud servers.

## Management

Useful servers support **fully local management**, where local users can access, manage, and control a Useful server using a web browser from their workstation. Dedicated servers can be deployed in environments with no Internet connection whatsoever and retain full functionality and access control.

Customers have the option of using **Userful Manager** to remotely connect to and manage instances of Useful from a single interface, however, this secure AWS-hosted connectivity service does not store or transmit sensitive customer data, and is not required.

## Optional - External Data Sources

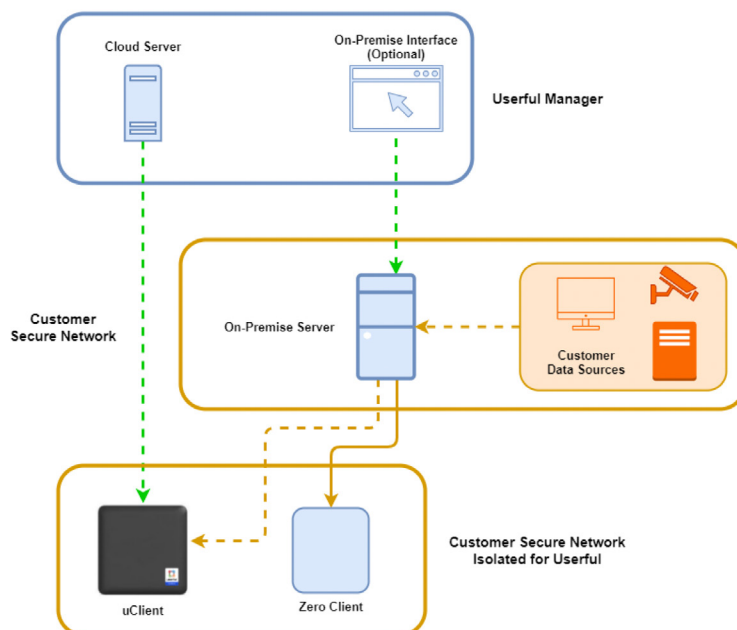
Customers can choose to purchase an optional subscription to the Engage CMS service. This AWS-hosted service provides customization of public data feeds, and optionally the ability to upload private data for distribution.

The Engage service follows all AWS best practices for data security and integrity, including native access controls and SSO authentication.

If the Engage subscription is not purchased, no connectivity or transmission to the service is established.

## Architecture Overview

- Green lines are control signals.
- Orange lines are customer data.
- Broken lines are optional data channels.
- Solid lines are required data channels.



## Userful Data Processing and Privacy

Userful servers access information visually. Information is processed into and out of the server as video data and without context. The exception to this is information acquired by web browser sources, which operate in their own highly secure environment.

In all instances, Userful does not, and can not, scan, duplicate, or record any information that passes through a server, regardless of that server's connectivity to Userful services.

## Userful's Business Model

While Userful counts revenue as a software as a service (SaaS) company, our focus is on providing solutions that predominantly or entirely exist within the customer's physical premises.

As a company, our focus is entirely on providing the tools that empower organizations to manage their visual information as they see fit.



## **DECISIONS**

### **Control Room Solutions** (NOC/SOC)



# **Useful Decisions and Dedicated Servers**

## **Operating System Base & Administration**

Useful is a software appliance based on CentOS Stream, a binary-compatible version of Red Hat Enterprise Linux. The Red Hat base is engineered and tested by highly security-conscious individuals and organizations around the world. However, since all administration of Useful can be done through the browser-based interface, you do not have to be familiar with Linux to run, operate and manage Useful. Administrators who are familiar with Linux can assume additional (root level) control over their Useful system if desired. Patches and feature updates are rolled out every quarter; Updates are optional and accompanied by a changelog. Due to the robust base platform, urgent security-related patches are highly infrequent.

## **OS Hardening Measures**

Useful employs the following measures to secure itself or to limit attack vectors:  
(The work to further harden and secure Useful never stops - new features are added regularly).

- Utilizes security-conscious, well-maintained, and a long-term supported Linux distribution as the base platform (CentOS/RHEL).
- Removed regularly compromised software and ports, thereby restricting possible attack vectors. (e.g., PHP, flash, and samba are examples of services that are not included, Apache and FTP are not enabled by default).
- Useful only uses required ports and services to operate. The base OS image has been locked down so that only necessary software and services are installed.
- Quarterly operating system updates are taken from the upstream (CentOS/RHEL) source.
- Useful systems are locked down to only allow updates from Useful's officially maintained and secured repositories.
- The upstream source reliably applies security fixes that are applied to the Useful system as regular updates. CentOS/RHEL are reliable, secure upstream sources that are routinely trusted by military and other security-conscious organizations around the world for critical IT infrastructure.
- The Useful server runs a local firewall restricting inbound connections to the server by default which has been configured to block all network ports not necessary for regular operation.
- To prevent individuals from compromising the root account, no root password is set. The root account is not directly accessible by remote network SSH or local login. Only the user account created in the setup process will have SUDO privileges.
- The (not required) connection to the Useful Manager server is exclusively over HTTPS.

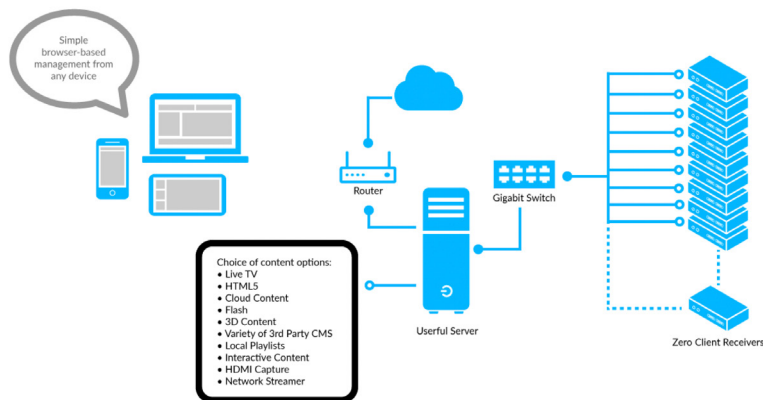
## Server Deployment

Useful servers are deployed all over the world, most of the time using one of the two below network topologies.

### Dual Network Interfaces

Useful ships at least two network interfaces in all servers and recommends using a primary (onboard) interface for network connectivity within your corporate/primary network, and a second interface to connect to an isolated network for only client traffic. This is the most common type of Useful deployment.

**Note:** Zero Clients can function entirely isolated from the Internet, but uClient devices must have internet connectivity to retrieve app and firmware updates.



#### Benefits:

- Isolated LAN provides ideal bandwidth and network isolation for clients
- Isolated LAN is non-routable, providing a secure environment for clients

#### Notes:

- The Useful host's primary interface is exposed to the corporate network on all listening ports
- As part of the client discovery process, the Useful server broadcasts its host information over both primary and secondary interfaces and is open to discover and lock devices on all interfaces

### No Internet access

Installing Useful without an Internet connection dramatically reduces attack vectors, however, it also limits Useful's functionality and access to updates, remote management tools, and support. Should you employ this approach, you will not be able to use Useful Manager, and if you require additional features or patches, you will need to install the newest version of Useful manually.

#### Benefits:

- Most secure possible configuration
- Ideal bandwidth for client traffic

#### Drawbacks:

- Inability to receive system updates, Useful Manager, remote support, and send automated troubleshooting data

# Network Services

## Network Ports

Since Userful relies on the network for communication between the server and clients, certain ports must remain open. Below is a complete list of the ports utilized and an explanation of every port used.

### Remote Management Access

The following sites must be accessible by the Userful server for complete remote management and support from Userful but are not required for daily operations.

Protocol	Port	Destination	Rule	Description
TCP	443	updates.userful.com updates2.userful.com umirror2.com cloud-connect.userful.com	Out	Software Updates Userful Manager Licensing
TCP	443	remote.userful.com	Out	Support VPN
TCP/UDP	3478	turn.userful.com	In/Out	Remote content upload and (optional) webcam

### Local Access Rules

These ports must be accessible from the LAN to allow local browser-based access to Userful

Protocol	Port	Destination	Protocol	Description
TCP	5353	LAN		Peer Discovery
TCP	5701	LAN		Failover
TCP	9000	LAN	HTTP	Userful Control Center
Multicast	54327	224.2.2.3		Failover
UDP	54327	LAN		Failover
TCP	54328	LAN		Failover

### Zero Client Access Rules

**Managing Zero Client Receivers on a separate switch, network, or VLAN is strongly recommended** rather than attempting to firewall zero clients as they require many dynamic ports, some of which can be exploited to attack system services.

Protocol	Port	Destination	Description
UDP	26668	Zero Clients	Zero Client Discovery
TCP	52330	Zero Clients	Zero Client Discovery
UDP	52330 - 52630 incl.	Zero Clients	Zero Client Discovery
TCP/UDP	<b>Various High Numbers</b>	Zero Clients	Zero Client Communication



## uClient Access Rules

The following ports and services must be available between a Useful server and endpoints running uClient, or between uClients in a Cloud deployment, for proper functionality.

Protocol	Port	Destination	Description
UDP	123	uClients	NTP
TCP	8554	uClients	RTSP Streaming
TCP/UDP	14725	uClients	Video Synchronization
TCP	14276	uClients	Video Synchronization
UDP	16668	uClients	uClient Discovery
TCP	16669	uClients	DNS Discovery

## Optional Functionality

These local ports on a server are optional and are disabled by default

Protocol	Port	Destination	Protocol	Description
TCP	21	LAN	FTP	FTP File Transfer
TCP	22	LAN	SSH	Local SSH
TCP	80	LAN	HTTP	Redirects to 9000
TCP/UDP	137-139, 445	LAN	SMB	Windows File sharing
TCP/UDP	631	LAN	HTTP	Printer Configuration

## Information Stored on Useful

Useful is a video wall and display controller and in most cases does not store information shared with it to display content. The following is a list of possible sources of sensitive data that could be stored on Useful:

- Useful Control Center/Linux Desktop usernames and passwords (hashed).
- Files are saved in the Linux Desktop under the above credentials.
- Browser history, cookies, and sessions saved in web browser sessions. (note: Any browser source session can be set to automatically clear at session end which eliminates this).
- Credentials are stored in the Useful Control Center for purposes of accessing assets such as RDP, RTP, RTSP, or VNC servers on the local network.
- Content played via the Signage Player source is stored locally on Useful's hard drive in the /var/source-content/ directory.

## Additional Steps to Secure Useful

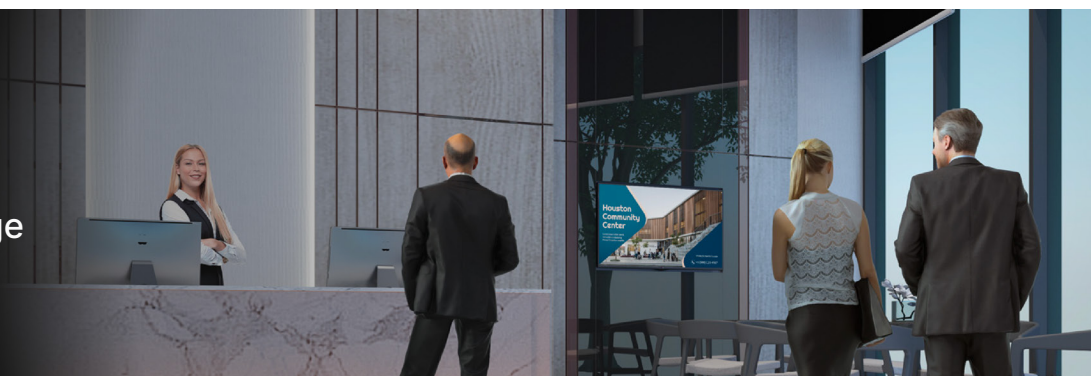
Useful employs the following measures to secure itself or to limit attack vectors:

(The work to further harden and secure Useful never stops - new features are added regularly).

1. Physically secure the computer case using a locking mechanism.
2. Disable booting from other devices in the BIOS and set a BIOS password.
3. Add a UPS to Useful for added redundancy and increased stability in situations with unreliable power.
4. Restrict **SSH access: in /etc/ssh/sshd\_config** set **PasswordAuthentication** to no
5. Disable Remote control settings under Settings in the Useful Control Center to prevent administrators from interacting with or viewing user desktop sessions.



## Engage Corporate Signage

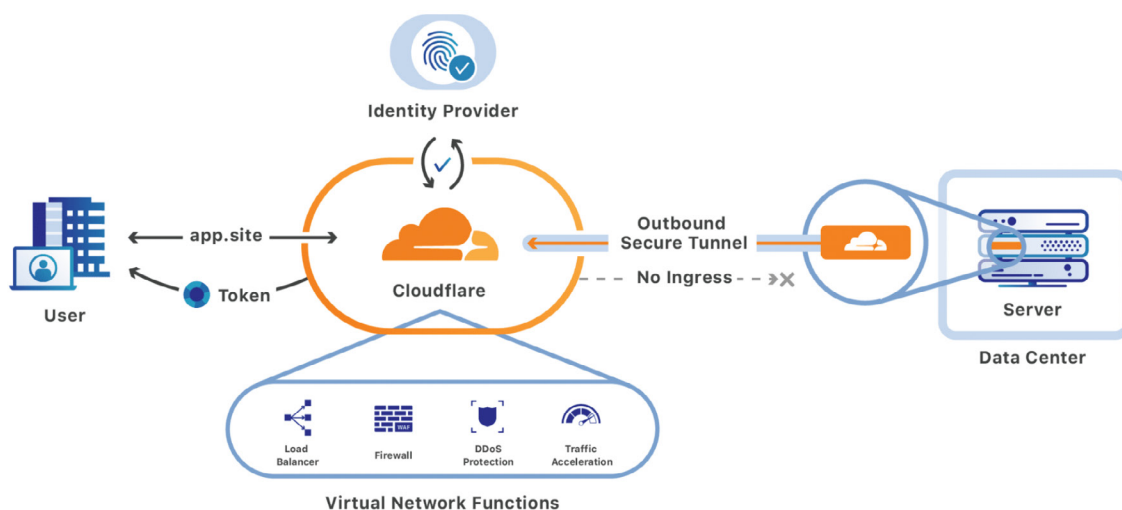


## Userful Engage

Engage Signage is based on a three-tiered structure.

The Engage web application connects directly to Cloudflare as a reverse proxy/threat mitigation and targets Digital Ocean (NYC-1 and NYC-2) as the primary data centers. As a secondary resource, Engage utilizes Amazon Web Services which also contains the same three-tiered structure as Digital Ocean.

The following providers meet the ISO 27001:2013 compliance standard. (ISO/IEC 27001:2013 (formerly ISO/IEC 27001:2005) is the specification for an information security management system (ISMS), a structure of policies and procedures that covers all legal, physical, and technical controls involved in Userful's information risk management processes).



In this diagram, “Data Center” represents “Digital Ocean” as the primary provider of Cloud Services. “Amazon Web Services” is the secondary provider, in which both route through Cloudflare before ending at the Users of Engage Signage.

Engage Signage Web Application > Cloudflare > Digital Ocean  
 Engage Signage Web Application > Cloudflare > AWS (Backup)

## Cloudflare

Cloudflare is a web infrastructure and website security company that provides content delivery networks, DDoS attack mitigation, Internet security, and distributed domain name server services. Cloudflare's services are designed to allow website visitors and hosting providers to Cloudflare users, acting as a reverse proxy for websites.

[Cloudflare ISO Compliance](#)



## Digital Ocean

Digital Ocean is a cloud hosting provider that offers cloud computing services to business entities so that they can scale themselves by deploying DigitalOcean applications that run parallel across multiple cloud servers without compromising on performance.

[Digital Ocean Security Compliance](#) ISO/IEC 27001:2013

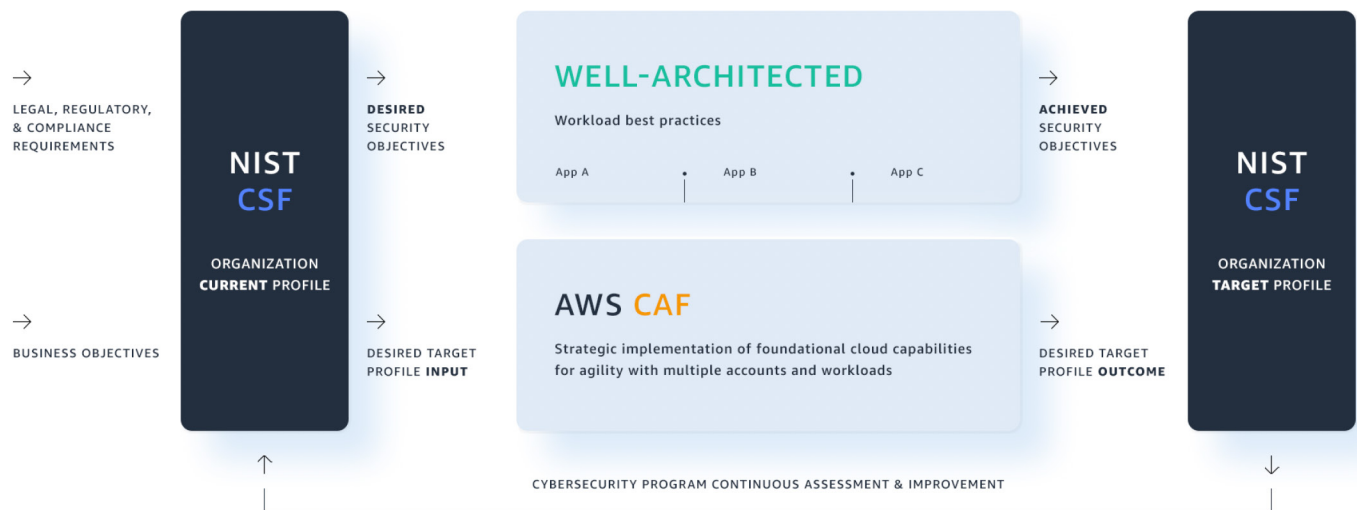


## Amazon Web Services

AWS complies with IT standards by Certifications and Attestations; Laws, Regulations, and Privacy; and Alignments and Frameworks. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. AWS customers remain responsible for complying with applicable compliance laws, regulations, and privacy programs. Compliance alignments and frameworks include published security or compliance requirements for a specific purpose, such as a specific industry or function.

ISO/IEC 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System (ISMS) which defines how AWS perpetually manages security in a holistic, comprehensive manner.

AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014. These certifications are performed by independent third-party auditors. Our compliance with these internationally recognized standards and code of practice is evidence of our commitment to information security at every level of our organization, and that the AWS security program is following industry-leading best practices.



AWS Cloud infrastructure and services have been validated by third-party testing performed against the NIST 800-53 Revision 4 controls, as well as additional FedRAMP requirements. AWS has received FedRAMP Authorizations to Operate (ATO) from multiple authorizing agencies for both AWS GovCloud (US) and the AWS US East/West Region. For more information, see the [AWS FedRAMP compliance](#) webpage.

## References

[AWS Compliance Programs](#)  
[AWS NIST Cyber Security Framework](#)  
[AWS FedRAMP](#)  
[Cloudflare ISO 27001](#)  
[Digital Ocean \(NYC1 and NYC2 - Data Centers\)](#)

# Useful Manager, Useful Support, and Data Integrity

## Useful Manager

Useful Manager is our hosted service that provides management and connectivity services to Useful servers and also hosts instances of Cloud servers.

The web interfaces of Useful Manager are all hosted on AWS with all security and logging services enabled (e.g. CloudWatch, CloudTrail, Amazon Inspector, AWS Config, and VPC Flow Logs).

- All user communication is HTTPS encrypted using Transport Layer Security (TLS).
- All interaction with Useful servers via the cloud is done through an encrypted proprietary protocol
- The Manager database is protected by a firewall which only allows LAN access from the application server
- All data communication between browser and Cloud server is validated to prevent injection attacks
- Session expiry is set for both cloud sessions and remote access sessions
- All user passwords are stored in a database that is twice-hashed, and users receive email notifications of password updates
- All user passwords are stored in an encrypted format. Useful requires a 2-factor authentication for login from each new IP address (password + emailed token)
- All content is hosted on Amazon S3 with private access, which communicates with servers via an internal endpoint (AWS S3 Gateway)

Useful employs a centralized system of diagnostics and alerts to proactively identify any problems.

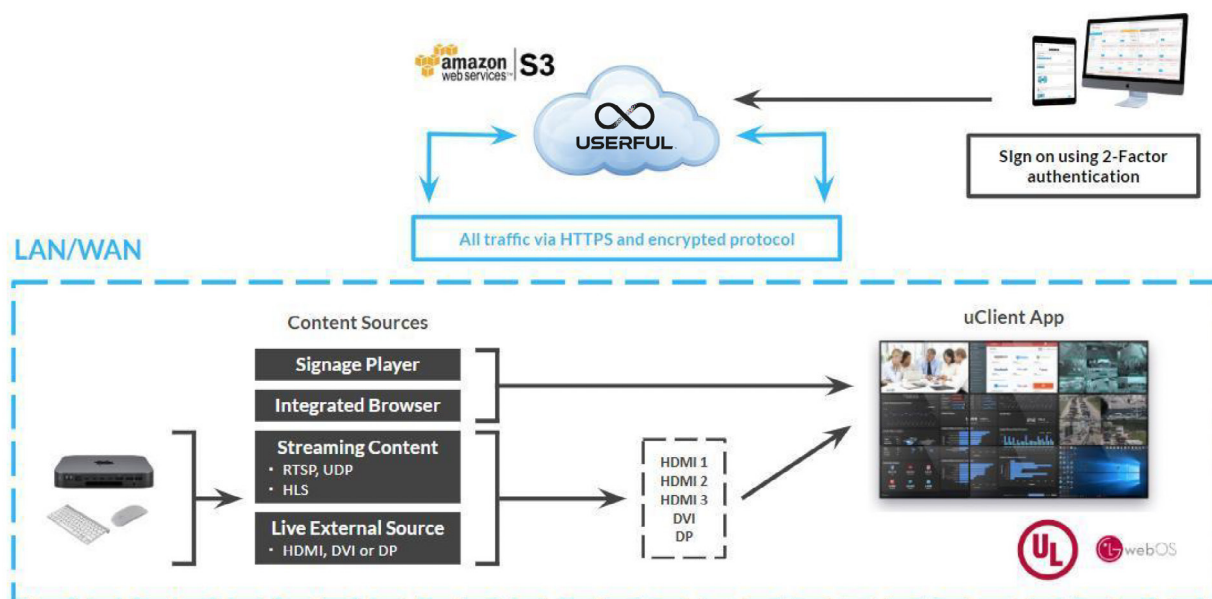
- Useful Manager utilizes a “defense-in-depth” (multi-layered bidirectional) approach to security. This layered and segmented approach allows for the compartmentalization of systems, meaning that a partial compromise does not result in data loss or exposure to additional compromise.

## Useful Cloud Servers

Useful Cloud is a video wall and display management solution that works directly with smart displays allowing customers to run video walls of unlimited size and resolution from the cloud with no additional hardware needed. Useful's uClient app is installed on each webOS smart display or Useful uClient Adapter. Each device synchronizes with the others within the local area network and connects to an assigned Useful Cloud server hosted in Manager.

All communication between AWS servers and the Useful uClient app is via HTTPS and all interaction is done through an encrypted proprietary protocol. Devices need to be able to connect to the Internet via outbound access on TCP port 443. For customers who want access to Useful's optional USB camera feature for observing what is playing on displays in real-time via the cloud, they need to ensure their firewall also allows outbound access on port 3478.

With Useful Cloud, uClient devices talk to each other using the local area network for video synchronization via TCP ports 14725 and 14726. Customers with tightly controlled networks must ensure nothing is blocking local area network traffic on these ports.



## Userful Servers

Any Userful server with the ability to connect to the Internet with outbound access on TCP port 443 and UDP port 3478 to the listed destinations will maintain an active connection with Userful Manager using secure HTTPS, provided the server is powered on.

With or without an active Userful subscription, Userful Support staff can use this connection to deliver instant support to a Userful system. They may also use it to activate the remote VPN connection for unrestricted administrative (root) access to the server for support and maintenance purposes.

## System Access

Userful Support staff are subject to background checks and will abide by the following conditions unless consent is specified by the end-user.

Userful staff members:

1. Will never duplicate, transmit, compromise, remove, corrupt, or otherwise alter user content or resources.
2. Are not able to view user passwords, and will never alter login credentials.
3. Will never intentionally harm or disrupt a production system, taking all precautions to test corrective actions on internal resources before deploying fixes to live environments.
4. Will strive to schedule previously agreed-on system updates and software fixes in off-hours to avoid service disruptions.

Userful Manager connectivity is not required for the operation of the Userful product and can be prevented with relevant network design or firewall rules.

Members of the Userful Engineering Team have similar access to Userful Manager for development and testing purposes, however, all staff are subjected to the same screening backgrounds as Support staff, and will never enter an end user's system for any reason unless their assistance with a complex, escalated issue is sought by the Support member, in conjunction with either (or both) the Support Manager or Product Manager's involvement and consent.

## Data Storage

All data in Useful Manager is stored in an AWS EBS volume separate from the connection server, protected by a firewall that only allows access from that server.

By default, the following data is stored in Useful Manager:

- The user's login credentials - email address and password
- Synchronization information for Useful servers
- Licensing information for the Useful server, including contact email address, Billing Name,
- Useful Sales Order#, Useful Invoice#, System ID, and Issue and Expiry Dates

Administrators can make use of an optional configuration backup function, which would save some information to Manager if enabled:

- Stored URLs, usernames, and passwords from web browser, VNC, or RDP sources
- Network addresses of RTP or RTSP network video sources, if configured
- File names of content playlists (content files are not stored)
- File names and paths of any custom commands running Linux applications using the Program Runner source
- Names of created presets and layouts

Useful supports hardware and software clients.

All Useful clients should be placed on a subnet or VLAN separate from the primary corporate network, as long as an interface from the server is also connected to this network and the client devices can access the Internet for app and firmware updates.

Zero Clients can be run on a subnet or VLAN that is entirely isolated from everything but the second interface on the server.

## uClient

Useful's uClient is a cross-platform app with versions for Android, LG WebOS 4.0+, and Samsung smart displays (in development).

The app is either downloaded and installed or comes pre-installed on the device, and automatically starts when the device is powered on using the capabilities of its platform to deliver content from Useful servers.

When used with a server and live sources, uClients receive RTSP streams directly from the servers and decode and play those streams on their respective screens in real-time. No data is stored or saved, aside from the hostname of the server that the device is currently connected to. When paired with a Cloud server, either some or all of the media content being played is downloaded directly to the internal storage of the device itself and then subsequently played using the device's own media playback capabilities.

Useful servers can deliver a hybrid of the two models with the new "Forward & Store" model where content for video walls is "chopped" up along bezel lines, with each piece sent to its respective display and played locally in sync with other displays. This means that each display has only the piece of the file that is assigned to it downloaded to its local storage.

Updates to the uClient app are delivered directly from Userful's servers. The app requires local storage access, but nothing else. uClient collects the following information from its device:

- MAC address of network adapters (wired and wireless, though it cannot set network settings).
- IP address and subnet mask
- Make and model of the device
- Firmware version (LG) or Android version (Android)

## Userful uClient Adapter

WebOS was the first product in its category to undergo UL Certification (Software Cybersecurity for Network-Connectable Products). WebOS 4.0 has a broad range of built-in security and security features for the enterprise including, TLS V1.2 for HTTPS, WPA2, RootCA, Proxy interface, ability to disable network ports, sandbox file system, restrict API access, and check file integrity. It uses self-signed certificates for HTTPS in the local network.

uClient installs on WebOS and is granted access only to local storage and media playback capabilities, all of which are handled through supported APIs.

## Userful Zero Clients

A Userful Zero Client is a simple ASIC-powered device that synchronizes USB and video signals over the local network to a server. The device itself stores no data or operating system and contains only very limited firmware. If removed from the premises, no data is retained whatsoever. Data transmitted to the Zero Client is not encrypted, however, the protocol is not an industry standard and all video data is transmitted in JPEG format, so personal data or credentials are never transferred to or from the client, except where they are used as public kiosks with keyboards and mice attached.

Userful Zero Clients can not connect to Userful Cloud servers.



# Network Security

Attackers equipped with internal knowledge of client devices and their operation could potentially use packet sniffers to read any information between your Useful servers and client devices, though most of this information will be useless. To remedy this vulnerability, follow standard network security guidelines and isolate the connection between the server and devices. Locking down unauthorized device access to the network would provide additional security.

When running a Useful system, it is a good idea to use a secure network environment. This includes:

- A basic firewall that prevents most internet-originated attacks.
- A network that does not allow public connections. This can include public wifi or any network where a malicious user can gain access to a system on the network.

Risks of an insecure network include:

## Network Disruptions (DOS)

Network clients can be rendered inoperable without sufficient network connectivity. Some of the network services running on the server are susceptible to a DOS (denial-of-service) or DDOS(distributed-denial-of-service) attack. A malicious user with access to the network could temporarily disrupt the system with a targeted attack. They will most likely be remedied with a reboot providing the attack has been stopped. Your firewall or IPS should be able to identify and remedy this threat before it gets out of hand.

## Network Snooping

By default, all local network access to the Useful Control Center (UCC) including keyboard and mouse activity of the clients is accessible on the LAN. HTTPS access to UCC can be configured after the initial setup. Any activity taking place should be considered susceptible to being read by a third party including any passwords entered at login or when resetting a password, etc. Using a keyboard and mouse directly plugged into the Useful server is the most secure way to access the Useful Control Center to configure Useful, though not all functions of UCC are supported in this way.

## Network Access

Full administrative access is available via the network (SSH, UCC). This is enabled by default as it is a useful feature to end-users and Useful support staff. The level of security is limited by the strength of the passwords chosen and the accessibility through the local firewall.

## Userful's Remote Support Feature (VPN)

The Useful VPN is a feature that allows authorized Useful support and development team members to remotely access the Useful systems with full administrative privileges. Generally, permission is requested before enabling the VPN, but Useful can enable it remotely. All Useful employees are subjected to background checks so it's highly unlikely that any employee would do significant harm to either your Useful system.

# Software and Role-Based Access Control (RBAC)

## Administrator Account

As part of the initial configuration process, an Administrator user account is created, with full application and OS-level access.

We recommend using secure password practices including ensuring administrator passwords are at least 8 characters in length and avoiding the use of just words and adding capital letters, symbols, and numbers to your password to increase the complexity of it.

If you are reimaging your appliance yourself by downloading the ISO from our website, we have an MD5 sum for the ISO located on the download page of Userful and we recommend that you compare the hashes as an additional security precaution.

The Userful host does not use encryption to store files on the hard drive by default, but you can achieve this through the same methodology that you would use for stock CentOS 7, or by re-installing the server with encryption enabled before configuration using the included install media.

## Role-Based Access Control

The Administrator account created during the initial setup of the system can be complemented with a set of user accounts that are created from, and exist only within the Userful application.

Creating Users and Groups within the Userful Control Center allows the Administrator to delegate responsibilities and access levels to other users of the system without exposing any part of the underlying OS.

Users can be assigned to Groups with granular permissions and restrictions. To provide a few possible examples:

- Full read/write access to all display and content source applications, but no access to user management or system operations
- View-only access to monitor content live on the displays or video wall
- Access only to the Command & Control application, with no access to the Control Center at all
- User management only tasks

RBAC user accounts can also be integrated into existing LDAP, Active Directory, and SAML-based corporate authentication systems.

# Conclusion

Cyber Security is of the utmost importance to Userful and Userful's customers. To learn more or to ask any follow-up questions, please contact Userful directly.

<https://www.userful.com/contact-us>

Tel: +1.403.289.2177

Toll-Free (within North America): +1.866.873.0091

[info@userful.com](mailto:info@userful.com)



## Appendix A:

### Example Questionnaire, Decisions Control Room Deployment

Question	Response
If the solution has any components hosted within a cloud environment, does the cloud environment align with the Customer approved Cloud Reference Architecture?	Userful Manager pertains to p. 14 of the included Security Packet document as an entirely vendor-hosted Manager system.
Do you have mechanisms in place to support the availability of the solution or service in the event of an outage or degradation of service (e.g. back-up or redundant infrastructure, failover or high-availability configurations, etc.)?	Redundancy is provided through the use of backup “failover” servers, a second server with identical specifications that is designated as a live-failover system in the event of server hardware failure. Spare client devices are provided, however, these are rarely if ever needed as clients have no moving parts. Settings can be centrally backed up and restored.
What environments are used to develop, test, and operate this solution?	Development languages include C, C++, Java, Python, and shell scripting. The development, test, and deployment platform is based on Red Hat Linux. The (optional) Userful Manager interface is developed in javascript using a node.js-based framework.
Has the solution owner created design documentation that itemizes the transmission, processing, accessing & storage of all sensitive non-public (SNP) data? Solutions with sensitive non-public (SNP) data must have sufficient architecture and data flow documentation.	See <b>Architecture Overview</b> diagram, p. 5. In the majority of use cases, Userful servers do not access SNP data in using means that would be classified as a risk.
Are Customer approved cryptographic algorithms (minimum AES-128 bits for symmetric encryption; ECC-256 bits or RSA-2048 bits for asymmetric encryption) used to encrypt Sensitive Non-Public data en queue, in transit, or at rest? If your solution does not transmit, process, access, or store sensitive non-public (SNP) data then you may mark this as N/A.	Whether SNP data is or is not used within the system will entirely be determined by which content the Customer chooses to display. In the context of in-transit or enqueue data (as it pertains to the projected use case of Userful), security would be provided by the HTTPS connection between the web browsers running in Userful (admins can choose between the latest stable versions of the Firefox and/or Chrome browser) and their destination web server. SNP data is not directly queued or transmitted over the local network, except as VNC should the optional Interactive Viewer functionality be used. Admins can disable the Interactive viewer if desired. Any traffic from the Userful server through Userful Manager (including the VNC connection for the interactive viewer), is encrypted via HTTPS.

If the solution contains sensitive non-public (SNP) data, is there a deep packet Data loss prevention (DLP) system monitoring the perimeter of the solution? If your solution does not transmit, process, access, or store sensitive non-public (SNP) data then you may mark this as N/A.	Userful does not transmit SNP data directly over the Internet. Use of the Interactive Viewer functionality through Useful Manager transmits VNC data (screen content) over the Internet, this can be avoided by either disabling interactive viewer or restricting local access to the server.
Does the solution provide input and output validation, including appropriate bounds checking?	End-users are only interacting with video wall content and Useful does not contain any end-user-facing database entry aspects.
What mechanisms will be used for users to authenticate to the solution for application usage and administrative purposes?	Manager authentication uses SSL. For systems that are not connected to Useful Manager, Local LAN authentication is also possible and supports HTTPS.
What mechanisms will be used for applications to authenticate to the solution for application usage and administrative purposes?	API calls sent through Useful Manager are encrypted with SSL. API calls can also be sent within the local network unencrypted. No customer data is accessible directly via the API.
Are access control methods in place to enforce segregation of duties? Segregation of duties and best practices restrict users from approving their access to applications and systems. If so, please explain.	<p>Userful Manager allows an administrator to utilize two access levels for new administrator accounts. The lower level account has restricted access permissions (e.g., cannot add new users), but still has administrative control over the Useful server.</p> <p>Local access control is restricted through a granular series of role-based access permissions using user/group functions to restrict access to relevant assets, as determined by the Customer's administrator.</p>
Do all components of this solution require unique credentials (i.e. username and/or tokens) for each user?	Userful Manager logins are unique to each user. Local access is also possible if required through a shared login, though the use of discrete user accounts is encouraged.
Have all default accounts been disabled or renamed upon installation?	There are no default users or accounts in existence at the time of unboxing.
Have all default passwords been replaced?	There are no default credentials in Useful, user credentials must be created by the administrator as part of the initial configuration.
Are all keys and tokens rotated at least once per year?	Password reset policies are not automatically enforced, but passwords can be rotated or reset at any time by the administrator.

Are user account roles and access re-evaluated annually and with every job change? If not, please elaborate.	User control in Manager is handled by the designated administrator(s), including account activation and deletion. Management of the local login is done manually.
Are you using Customer approved security algorithms, key lengths, key management, authentication, access control, methods, and techniques? Please specify those that are used.	Access to Useful systems is granted only when given by the Organization's administration, either by account creation through Manager or local access. Individual user accounts can be created and managed through Useful Manager, removing the use of shared accounts. Active users associated with the Organization can be easily listed by administrators in Useful Manager. No default passwords exist in Useful, administrators are free to implement their password policies when creating new users. Any non-interactive accounts must be enabled by default. Only Organization administrators may access system logs in any fashion.
Do failed login attempts provide a generic error message (e.g. "The credentials are incorrect") as opposed to a specific error message (e.g. "The username was not found")?	For Manager login, generic error messages are provided. For local logins, the username is pre-populated by default. The error "Invalid username or password." appears if an invalid password was entered. The pre-populated username can be changed if required.
Are all encryption keys managed with the approved Customer key management solution (SafeNet KeySecure)? If encryption keys are not used within the solution, please select N/A.	The Useful Manager service manages its own encryption keys; local access does not require encryption keys but importing HTTPS certificates is supported.
Are all certificates validated appropriately? This includes checking the validity (i.e. it has not expired and has been signed by a trusted Certificate Authority) and revocation status of a certificate using Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP).	The Useful Manager service, when communicating with individual Useful servers, manages its encryption keys entirely internally and Useful controls all aspects of signing and maintaining these keys.
Please specify the version(s) of SSL/TLS used within the solution?	SSL 2, SSL 3, TLS 1.2













Are privileged logins, such as 'Administrator' or 'root,' required to use strong authentication with a unique user account before assuming administrative privilege? If so, please explain how.	The user created during setup can set their credentials. There are no criteria in place for strong password authentication, users are encouraged to create secure passwords.
Do all sessions time-out or lockout within thirty (30) minutes of user inactivity?	2 hours, unless "Keep Me Logged in" is checked, in which case the login is indefinite.
Are security event logs available for all applications and systems in this solution that will store, queue, transmit, or process data?	Beyond the base Useful OS itself, 3rd party applications in use on the system will be the Chrome and Firefox web browsers. Any security incidents originating from these applications will be logged on the websites they access.
Do security event logs meet the requirements outlined in the Customer approved Security Event Logging Standard?	Userful Manager logs valid logins and password changes. Last-login time is visible to administrators.  The local Useful system logs are displayed in a built-in Activity Log center.
Are security events logs from this solution forwarded to the Customer's centralized security information and event management (SIEM) solution?	Not currently.
Are all components of the solution synchronized with a consistent, centralized time service, such as Network Time Protocol (NTP)?	Yes, Useful uses NTP to maintain date/time synchronization.
Is there a plan for reporting security incidents to a Customer-authorized incident management and response team?	Administrators are given the tools necessary to investigate security incidents via the Activity Log.
Is a change management process followed for all changes to applications and systems included in this solution? This includes security updates, bug fixes, and feature enhancements.	System updates released by Useful are managed by the end-users at their discretion. Changelogs are available as part of our public documentation. Notifications of new releases are emailed to stakeholders before release.
Do the solution's applications and systems use a Customer approved operating system build? If not, please specify any changes or deviations from these builds.	Userful's base OS is a derivative of Red Hat Enterprise Linux.



Are all unnecessary system and network services disabled within the solution?	We removed regularly compromised software and ports from the default OS configuration when creating the Userful product, thereby restricting possible attack vectors. Apache, FTP, PHP, Flash, and Samba are examples of services that are not included. Userful only uses required ports and services to operate. The base OS image has been locked down so that no unnecessary software or services are installed.
Are any insecure network ports or protocols utilized by the solution? Insecure protocols may include FTP, NFS v3 or older, RCP, SSL, SMB/CIFS v2 or older, SNMP or Telnet	FTP access can optionally be enabled but is disabled by default. The list of open ports on a default Userful install is available in this document.
Does the solution discard invalid or malformed network packets that could potentially cause a Distributed Denial of Service (DDoS) attack? If your application or system is not Internet-facing, you may answer this with a N/A	See the firewall rules, described above in this document.
Do all components of your solution utilize a host-based firewall? If yes, please specify which components use the host-based firewall and what host-based firewall access control lists (ACL) are used?	DNS Discovery




















## Appendix B:



### Example Checklist, Engage Digital Signage Deployment








Section 1: Data Access and Controls	Complete
Prevent access to organization-defined security-relevant information except during secure, non-operable system states.	
The component inventory must be consistent with the authorization boundary of the system and is subject to annual review. All components within the authorization boundary of the system must be verified either as part of the system or recognized by another system as a component within that system.	
Users must understand their responsibilities for protecting Sensitive, Confidential, or Regulated data and the consequences for mishandling such data.	
When employing multifactor authentication for remote access to information systems, ensure that it complies with the Customer Authentication Standard.	
Approved devices remotely connecting to the organization network must have a VPN client installed, with an organization-issued VPN certificate.	
Implement adequate security measures (e.g., virus, malware, and spam protection, firewall, intrusion detection) on client computers before allowing VPN remote access.	
Implement adequate security measures (e.g., virus, malware, and spam protection, firewall, intrusion detection) on client computers before allowing VPN remote access.	
Virtual desk applications shall be securely configured to minimize the ability of users to copy data.	
The information system shall use automated functions to monitor and control remote access methods.	
Systems shall log all remote access occurrences, including both end-user and administrator activity user credentials, date/time, and duration of connection at a minimum).	
Route all remote accesses through managed network access control points. Limiting the number of access control points for remote accesses reduces the attack surface for organizations.	
The ISO shall authorize the execution of privileged commands and access to security-relevant information, e. g. logging into a firewall device for administrative functions. Remote access under these conditions shall be authorized only for compelling operational needs and the agency shall document the rationale for such access. Such actions shall be logged and audited.	







Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; Authorize the connection of mobile devices to organizational systems.	
The Customer shall establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, whether owned by the Customer or the employee.	






<b>Section 2: Governance</b>	<b>Complete</b>
Encryption is required for all mobile devices that contain Customer Sensitive, Confidential, or Regulated Information.	
Develop policies governing the use of external information systems and resources including the type and classification of data that can be stored outside of the Customer.	
Establish terms and conditions for contracting with external information resources providers.	
Limit connections to and use of external systems to only those required for business operations.	
Establish and document terms and conditions via Interconnection Security Agreements (ISAs).	
<ul style="list-style-type: none"> <li>a. Approve and manage the exchange of information between the system and other systems using Interconnection Security Agreements;</li> <li>b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and</li> <li>c. Review and update the agreements annually.</li> </ul>	
Authorize all connections from internal/organization information systems to other information systems outside of the Customer through the use of system connection agreements and monitor/control the system connections on an ongoing basis.	
All Interconnection Security Agreements must be approved by the Authorizing Official and the Information Security Officer.	
Customer must have a procedure for authorizing internal information resource connections.	
For any system categorized as moderate or high, the System Security Plan (SSP) will identify the types of personally owned equipment that may be internally connected with organizational information systems and networks, compliant with Customer mobile device security policies.	





<p>a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and</p> <p>b. Review and update the baseline configuration of the system:</p> <ul style="list-style-type: none"> <li>b1. Annually;</li> <li>b2. When required due to a major system change; and</li> <li>b3. When system components are installed or upgraded</li> </ul>	
Information Resource Technology (IRT) assets must comply with the Customer Information Security Minimum Configuration Baseline Standard.	
Define, document, approve and enforce physical and logical access restrictions associated with changes to the system.	
<p>Limit personnel authorized to make changes to the infrastructure based on their job responsibilities, and approve individuals before granting access.</p> <p>a. Establish and document configuration settings for components employed within the system using approved common secure configurations derived from sources defined in Stds.2-3 that reflect the most restrictive mode consistent with operational requirements;</p> <p>b. Implement the configuration settings;</p> <p>c. Identify, document, and approve any deviations from established configuration settings for all configurable system components based on explicit operational requirements; and</p> <p>d. Monitor and control changes to the configuration settings following organizational policies and procedures.</p>	
<p>The Customer must</p> <ul style="list-style-type: none"> <li>• establish mandatory configuration settings for information technology products employed within the information system;</li> <li>• configure the security settings of information technology products to the most restrictive mode consistent with operational requirements;</li> <li>• document the configuration settings; and</li> <li>• enforce the configuration settings in all components of the information system.</li> </ul>	
All configuration baselines implemented in a production environment must be coordinated with and approved by Customer Information Security.	
<p>To resolve configuration conflicts among multiple security guidelines, follow the latest (current) guidance from the highest applicable source in the Customer hierarchy as follows:</p> <ol style="list-style-type: none"> <li>1. Customer Information Security Configuration Baselines</li> <li>2. The Center for Internet Security (CIS);</li> <li>3. NIST National Checklist Program (NCP) Repository;</li> <li>4. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG);</li> <li>5. National Security Agency (NSA) STIGs;</li> <li>6. Vendor Configuration Baselines.</li> </ol>	
Configure information systems to provide only essential capabilities.	








Provide timely responses, as defined by the CISO, to informational requests for organizational configuration Overall Status: and posture information.	
The component inventory must be consistent with the authorization boundary of the system and is subject to annual review. All components within the authorization boundary of the system must be verified either as part of the system or recognized by another system as a component within that system.	

<b>Section 3: Users and Data Integrity</b>	<b>Complete</b>
<p>Provide contingency training to system users consistent with assigned roles and responsibilities:</p> <ul style="list-style-type: none"> <li>a. Within 60 days of assuming a contingency role or responsibility;</li> <li>b. When required by system changes; and</li> <li>c. Annually thereafter.</li> </ul>	
<p>Train personnel in their contingency roles and responsibilities concerning the information system and provide periodic refresher training.</p> <ul style="list-style-type: none"> <li>a. Conduct backups of user-level information contained in any component of the system at a frequency set following the systems recovery point objectives;</li> <li>b. Conduct backups of system-level information contained in the system following the recovery point objective (RPO) as defined in the contingency plan (see CP-02);</li> <li>c. Conduct backups of system documentation, including security- and privacy-related documentation when created or received, when updated, or as defined in the contingency plan, System Security Plan (SSP), or both when both are available; and</li> <li>d. Protect the confidentiality, integrity, and availability of backup information.</li> </ul>	
Conduct backups of system-level information (including system state information) and critical user-level information contained in the information system and protect backup information at the storage location.	
Backups, including remote and cloud-based backups, must be compliant with Customer requirements for encryption and protecting data at rest.	
Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	
Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resource system may grant that user access.	
Each system's identification and authentication mechanisms must comply with the Customer Identification and Authentication Standard.	






Implement multifactor authentication for access to privileged accounts.	
<p>For access to privileged accounts,</p> <ul style="list-style-type: none"> <li>a. implement multifactor authentication following the Customer Identification and Authentication Standard.</li> <li>b. Selecting an identifier that identifies an individual, group, role, service, or device;</li> <li>c. Assigning the identifier to the intended individual, group, role, service, or device; and</li> <li>d. Preventing reuse of identifiers for at least a year for individuals, groups, roles, services, or devices.</li> </ul>	
Sensitive Personal Information, to include SSNs and parts of SSNs, must not be used as system identifiers. Identifier management must ensure that any access to, or action involving, personally identifiable information (PII) is attributable to a unique individual.	
<p>Manage system authenticators by:</p> <ul style="list-style-type: none"> <li>a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;</li> <li>b. Establishing initial authenticator content for any authenticators issued by the organization;</li> <li>c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;</li> <li>d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;</li> <li>e. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;</li> <li>f. Changing default authenticators before first use</li> <li>g. Changing or refreshing authenticators at the frequency defined in the Customer Identification and Authentication Standard;</li> <li>h. Protecting authenticator content from unauthorized disclosure and modification;</li> <li>i. Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and</li> <li>j. Changing authenticators for group or role accounts when membership to those accounts changes.</li> </ul>	
<p>Organizations must manage information system authenticators by:</p> <ul style="list-style-type: none"> <li>a. Defining initial authenticator content;</li> <li>b. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and</li> <li>c. Changing default authenticators upon information system installation.</li> </ul>	
<p>This control applies only to systems that use a memorized secret (passphrase, PIN, etc.). For all requirements concerning the use of memorized secrets, see the Customer Authentication Standard.</p>	










<p>a. Screen individuals before authorizing access to the system; and</p> <p>b. Rescreen individuals following rescreening conditions defined in Human Resources policies and procedures, and, where rescreening is indicated before access is granted for any new or changed role.</p>	
<p>Customer must screen individuals requiring access to organizational information and information systems before authorizing access.</p>	
<p>Customer is responsible for defining all information classification categories except the Confidential or Regulated Information category, which is defined in Subchapter A of this chapter and establishing the controls for each.</p>	
<p><b>Section 4: Vulnerability Detection and Mitigation</b></p>	<p><b>Complete</b></p>
<p>Involve the Senior Official for Privacy, or their designee, when conducting the security categorization process for information systems containing personally identifiable information (PII) or sensitive personal information (SPI).</p> <p>a. Scan for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system are identified and reported;</p> <p>b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:</p> <p>b1. Enumerating platforms, software flaws, and improper configurations;</p> <p>b2. Formatting checklists and test procedures; and</p> <p>b3. Measuring vulnerability impact;</p> <p>c. Analyze vulnerability scan reports and results from control assessments;</p> <p>d. Remediate legitimate vulnerabilities following an organizational assessment of risk;</p> <p>e. Share information obtained from the vulnerability scanning process and control assessments with the Customer IT Operations team, help eliminate similar vulnerabilities in other systems; and</p> <p>f. Employ vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.</p>	
<p>Customer's Information Resources Manager shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than October 15 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or Data processing of the agency or a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.</p>	





<p>Customer's information resources manager shall provide an electronic copy of the vulnerability report on its completion to:</p> <ul style="list-style-type: none"> <li>• The Department of Information Resources;</li> <li>• The state auditor;</li> <li>• Customer's Executive Director; and</li> <li>• Any other information technology security oversight group specifically authorized by the legislature to receive the report.</li> </ul>	
<p>Separate from the executive summary described by Subsection (b), the Customer shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request.</p>	
<p>Conduct scans according to the Scan Frequency table: Target Scan Type Scan Frequency All external-facing systems Un-Credentialed Scan Once per 24 hours Workstations Credentialed Scan Once per week Servers Credentialed Scan Once per week Internal-facing networked assets (other than workstations or servers)Credentialed Scans Once per month All internal-facing networked assets, Un-Credentialed Scan Once per month.</p>	
<p>Remediate legitimate vulnerabilities according to the Remediation Responses below, timeline beginning from the date of identification by a vulnerability scanner:</p> <ol style="list-style-type: none"> <li>1. High Baseline: <ul style="list-style-type: none"> <li>(a) Critical Risk: 3;</li> <li>(b) High Risk: 14;</li> <li>(c) Moderate Risk: 30;</li> <li>(d) Low Risk: 90.</li> </ul> </li> <li>2. Moderate Baseline: <ul style="list-style-type: none"> <li>(a) Critical Risk: 3;</li> <li>(b) High Risk: 14;</li> <li>(c) Moderate Risk: 30;</li> <li>(d) Low Risk: 90.</li> </ul> </li> <li>3. Low Baseline: <ul style="list-style-type: none"> <li>(a) Critical Risk: 14;</li> <li>(b) High Risk: 30;</li> <li>(c) Moderate Risk: 90;</li> <li>(d) Low Risk: 180.</li> </ul> </li> </ol>	

<p>Internet-Facing Vulnerability Response Time (Calendar Days)</p> <p>For each baseline, the critical, high, moderate, and low-risk response times are as follows:</p> <ol style="list-style-type: none"> <li>1. High Baseline:             <ol style="list-style-type: none"> <li>(a) Critical Risk: 14;</li> <li>(b) High Risk: 30;</li> <li>(c) Moderate Risk: 90;</li> <li>(d) Low Risk: 180.</li> </ol> </li> <li>2. Moderate Baseline:             <ol style="list-style-type: none"> <li>(a) Critical Risk: 14;</li> <li>(b) High Risk: 60;</li> <li>(c) Moderate Risk: 90;</li> <li>(d) Low Risk: 180.</li> </ol> </li> <li>3. Low Baseline:             <ol style="list-style-type: none"> <li>(a) Critical Risk: 30;</li> <li>(b) High Risk: 90;</li> <li>(c) Moderate Risk:</li> </ol> </li> </ol>	
<p>False positives should be identified as such in the log. Where possible, scanners should be tuned to exclude a newly identified false positive, but no further remediation action is required.</p>	
<p>Utilize an up-to-date SCAP-compliant vulnerability scanning tool.</p>	
<p>The network and host-based vulnerability scanner shall provide the following capabilities:</p> <ul style="list-style-type: none"> <li>• Identify active hosts on networks.</li> <li>• Identify active and vulnerable services (ports) on hosts.</li> <li>• Identify vulnerabilities associated with discovered operating systems and applications.</li> </ul>	
<p>Where possible, use tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.</p>	
<p>For dynamic application security testing.</p> <ol style="list-style-type: none"> <li>a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: security and privacy controls as defined in Customer Information Security and Privacy Controls Baseline Standard and Service Level Agreements (SLAs);</li> <li>b. Define and document organizational oversight and user roles and responsibilities concerning external system services; and</li> <li>c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: processes, methods, and techniques as specified in contracts, SLAs, and the Continuous Monitoring Program.</li> </ol>	
<p>Customer must require that providers of external information system services employ adequate security controls following the standards described in SA-9 and monitor security control compliance.</p>	



<p>Ensure that Service Level Agreements include:</p> <ul style="list-style-type: none"> <li>• Service definitions;</li> <li>• Delivery levels;</li> <li>• Security controls, including third-party personnel security, information classification, transmission, and authorization;</li> <li>• Aspects of service management, including monitoring, auditing, impacts to the organization's resilience, and change management; and</li> <li>• Issues of liability, reliability of services, and response times for the provision of services.</li> </ul>	
Section 5: Development Practices and Penetration Testing	Complete
<p>Require the developer of the system, system component, or system service to perform penetration testing:</p> <ol style="list-style-type: none"> <li>At the following level of rigor: organization-defined breadth and depth to include, at a minimum, the system components to be scanned and the vulnerabilities checked; and</li> <li>Under the following constraints: constraints defined in Stds. 1, 2, &amp; 3 below. " <ul style="list-style-type: none"> <li>Std.1 – Customer, when implementing an Internet website or mobile application that processes any sensitive personal information or confidential or regulated information, must subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.</li> <li>Std.2 – Require advanced coordination and formal authorization for all penetration testing on systems in the production environment. Authorization must include the scope of test including, but not limited to, system components and planned actions.</li> <li>Std.3 – Reporting on penetration testing should include the defined list of targets provided (IP addresses, protocols, services or applications, etc.); the specific commercial, public, and proprietary tools used; and, if applicable, evidence of successful exploitation or illustrations of exploitability where vulnerabilities exist.</li> </ul> </li> </ol>	
<p>Sensitive, confidential, or regulated information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted.</p>	
<p>Storing sensitive, confidential, or regulated information on portable devices is discouraged. Confidential or regulated information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-Customer-owned computing device.</p>	
<p>Customer may also choose to implement additional protections, which may include encryption, for other data classifications.</p>	
<ol style="list-style-type: none"> <li>Identify, report, and correct system flaws;</li> <li>Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;</li> <li>Install security-relevant software and firmware updates within periods defined following the release of the updates; and</li> <li>Incorporate flaw remediation into the organizational configuration management process.</li> </ol>	

Customer must identify, report, and correct information system flaws.	
<b>Section 6: Vulnerability Remediation</b>	<b>Complete</b>
<p>a. Customer shall, with available funds, identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. Customer shall include in the plan:</p> <ol style="list-style-type: none"> <li>1. Procedures for reducing the agency's level of exposure concerning information that alone or in conjunction with other information identifies an individual maintained on a legacy system of the agency</li> <li>2. The best value approach for modernizing, replacing, renewing, or disposing of a legacy system that maintains information critical to the agency's responsibilities;</li> </ol> <p>b. A plan developed under this section, along with any information or communication prepared or maintained for use in the preparation of the plan, is confidential and is not subject to disclosure</p>	
Review available published sources and alerts identifying software flaws.	
Where feasible, test newly released security-relevant patches, service packs, and hotfixes in a test environment.	
Patches, service packs, and hotfixes not implemented in enterprise or specific systems must be documented in the risk register.	
Monitor systems to verify that security releases have been installed and are functioning correctly.	
<p>a. Implement signature-based, non-signature based, or both types of malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;</p> <p>b. Automatically update malicious code protection mechanisms whenever new releases are available following organizational configuration management policy and procedures;</p> <p>c. Configure malicious code protection mechanisms to:</p> <ol style="list-style-type: none"> <li>c1. Perform periodic scans of the system at least daily and real-time scans of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed following organizational policy; and</li> <li>c2. Block and quarantine malicious code and send an alert to administrators in response to malicious code detection; and</li> </ol> <p>d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.</p>	
The information system must implement malicious code protection.	
Security Officer shall establish a security strategy that includes perimeter protection.	

The Department of Information Resources will provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize State information resources as specified in Chapters ##### and #####, Government Code. Perimeter security controls may include some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router.	
Configure systems to address all applicable monitoring objectives following the Information Security Program Plan, including but not limited to: — <ul style="list-style-type: none"><li>• Impact of security changes to the information system;</li><li>• Unauthorized use of the system;</li><li>• Information system attacks; and</li><li>• Identified specific types of transactions of interest.</li></ul>	
a. Designate individuals authorized to post information onto a publicly accessible system; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information before posting onto the publicly accessible system to ensure that nonpublic information is not included; and d. Review the content on the publicly accessible system for nonpublic information quarterly or as new information is posted and remove such information if discovered.	
Develop policies governing the procedures to post information on publicly accessible information systems.	
If sensitive, confidential, or regulated information is discovered on a public site, the information must be handled according to the organization's incident management policies and procedures.	