Screenly

Digital Signage Readiness Checklist 2026-2027

A checklist for security-minded, forward-thinking teams

Introduction

Digital signage players run on corporate networks, are often deployed in regulated or high-risk environments, and typically remain in place for years with minimal hands-on oversight.

From an IT perspective, digital signage should be evaluated like any other managed endpoint.

This checklist is designed for IT, security, and infrastructure teams to use during procurement reviews, security assessments, and internal due diligence.

Screenly

1- Secure Foundations: Architecture, Patching and Lifecycle

SECURE-BY-DESIGN ARCHITECTURE

Ask:
- Is the operating system purpose-built for embedded or IoT use?
- Is the OS security-hardened by default?
- Are devices locked down out of the box?
- Is secure boot supported and enforced?

Look for:
- Minimal OS with a reduced attack surface
- Kernel-level process isolation
- Devices designed to assume deployment on public or untrusted networks
- No open inbound ports by default

UPDATES, PATCHING AND END-OF-LIFE

Ask:
- How are security patches delivered?
- How frequently are OS and application updates released?
- Are updates automatic or manual?
- Are updates cryptographically verified, to ensure they cannot be altered in transit?
- Are OS end-of-life timelines clearly documented?

Look for:
- Automatic, transactional updates
- Signed updates with verification enforcement
- Updates that do not interrupt content playback
- Publicly documented EoL policies and mitigation strategies

2- Operational Security: Identity, Access and Vulnerability Handling

VULNERABILITY DISCLOSURE AND TRANSPARENCY

Ask:
- Is there a public vulnerability disclosure or bug bounty program?
- Is there a documented process for reporting security issues?
- Are security incidents publicly disclosed?
- Are third-party penetration tests performed?

Look for:
- Responsible disclosure with safe harbor
- Published advisories, changelogs, or postmortems
- Evidence of ongoing security review, not one-time audits

IDENTITY, AUTHENTICATION AND ACCESS CONTROL

Ask:
- How are devices uniquely identified and authenticated?
- Is certificate-based authentication supported?
- Is all management traffic encrypted in transit?
- Are role-based access controls available?
- Is multi-factor authentication supported?

Look for:
- Mutual TLS or equivalent device authentication
- Hardware-backed key storage where available
- Least-privilege access controls
- Auditable user and configuration changes

3- Network, Data and Compliance Considerations

NETWORK AND EDGE OPERATION

Ask:
- Can devices operate without constant cloud connectivity?
- What functionality is lost during a network outage?
- Are outbound connections minimal and documented?
- Does the platform require inbound access?

Look for:
- On-device content playback and scheduling
- Continued operation during outages
- Well documented network architecture and requirements
- No reliance on inbound network connections

DATA HANDLING AND COMPLIANCE READINESS

Ask:
- What data is collected, processed, or stored?
- Is personal data required to operate the platform?
- Where is data processed and stored?
- Which compliance frameworks does the platform align with?

Look for:
- Data minimization by design
- No dependency on personal data
- Support for SOC 2, GDPR, and EU CRA alignment
- Documentation suitable for audits and risk reviews

4- Longevity, Risk and Vendor Accountability

SOFTWARE TRANSPARENCY AND EXTENSIBILITY

Ask:
- Can you provide an SBOM to prove sound supply chain security protocols?
- How are third-party dependencies managed?
- Are dependencies regularly scanned for vulnerabilities?
- Can custom applications be deployed securely?

Look for:
- Inspectable application code
- Automated dependency and vulnerability scanning
- Secure sandboxing for applications
- APIs that do not weaken security controls

HARDWARE LIFECYCLE AND EXIT RISK

Ask:
- What is the supported hardware lifespan?
- What happens at hardware or software end-of-life?
- Can devices continue operating if the vendor relationship ends?

Look for:
- No forced hardware refresh cycles
- Clear decommissioning and migration paths
- Continued edge operation without cloud lock-in

SECURITY CULTURE, GOVERNANCE AND FUTURE READINESS

Ask:
- Does the provider publicly commit to secure-by-design principles?
- Have they signed CISA's Secure by Design pledge?
- Are they SOC 2 compliant or aligned?
- How are they preparing for the EU Cyber Resilience Act (CRA)?
- Do they publish security incidents or transparency reports?

Look for:
- Public security commitments and accountability
- Evidence of ongoing investment in security governance
- Clear regulatory readiness roadmap
- Transparency over time, not just certifications

Final Check

If a provider cannot clearly answer these questions, the risk is not just screen downtime.

It is security exposure, compliance debt, and long-term operational risk.

Digital signage should meet the same standards as any other endpoint deployed on your network.

Screenly - The Secure Digital Signage Company

WHY TEAMS CHOOSE SCREENLY

Most digital signage platforms can display content. Very few are built to meet the expectations of modern IT and security teams.

Screenly is designed from the ground up as secure signage infrastructure, ready to manage your fleet at scale.

SECURE BY DESIGN, NOT BY ADD-ON

- Purpose-built, minimal Linux-based operating system
- Kernel-level isolation using namespaces, cgroups, AppArmor, and Seccomp
- Secure boot and full device lockdown
- No open inbound ports
- No shell access, SSH, default credentials, or backdoors

AUTOMATIC, VERIFIABLE UPDATES

- Automatic OS and application updates
- Transactional, cryptographically signed updates
- Updates applied without interrupting playback
- Publicly documented OS end-of-life timelines and mitigations

STRONG DEVICE IDENTITY AND ENCRYPTION

- Mutual TLS (mTLS) for device authentication
- Private keys stored in TPM on supported hardware
- Full encryption for all device and management traffic

BUILT FOR THE EDGE

- Full on-device playback and scheduling
- Continued operation during network outages
- Minimal, documented outbound connections
- Architecture designed for public network exposure

TRANSPARENT, INSPECTABLE SOFTWARE

- Open source, inspectable signage applications
- Continuous vulnerability scanning of dependencies
- Secure sandboxing for applications

ENTERPRISE-GRADE BACK-END SECURITY

- SOC 2–aligned controls
- Ephemeral cloud infrastructure replaced every 24 hours
- Continuous vulnerability scanning
- Role-based access control and team isolation
- Two-factor authentication

SECURITY AS A COMPANY COMMITMENT

- Signatory to CISA's Secure by Design pledge
- Active preparation for EU Cyber Resilience Act requirements
- Public vulnerability disclosure and bug bounty program
- Published incident reports and security communications
- Regular third-party penetration testing

THE PRACTICAL CHOICE

For IT teams, the difference is not **feature** lists.
It is whether the platform behaves like infrastructure and whether the vendor demonstrates long-term security accountability.
For organizations that cannot afford security shortcuts, Screenly is the natural choice. To learn more, schedule a demo at sales@screenly.io.


Screenly