MobileIron

Cloud Best Practices: Audit Checklist for Endpoint Security

This 10-point checklist outlines best practices for designing a security architecture that protects cloud data at the endpoint. Enterprise computing architectures have changed fundamentally in the last ten years, as employees consume an ever-growing collection of business cloud services through mobile apps. The traditional security approach of network perimeter and locked-down endpoints is not suitable for this app-to-cloud model of modern work.

Cloud service providers, in general, take a structured and comprehensive approach to securing their data centers and mitigating the risk of a data breach. However, once the data leaves the service provider and resides on an end user's mobile device, that data can be easily compromised or lost unless appropriate security controls are in place.

Many organizations will have to undergo internal or external security audits to test how well they are protecting business data both in the cloud and at the endpoint. The U.S. NIST Cybersecurity Framework (www.nist.gov/cyberframework) and the European Union General Data Protection Regulation (GDPR - www.eugdpr.org) are two of the frameworks likely to influence audit criteria.

This checklist is intended to provide a starting point rather than an exhaustive audit. Each organization should still conduct its own analysis and define its own controls, but gaps between your current deployment and this checklist might indicate escalated levels of risk.

MobileIron

info@mobileiron.com

www.mobileiron.com

Security Audit Checklist

1. Enforce device encryption and password protection

Mobile devices are frequently lost. Enforcing device encryption and the use of passwords can protect data from easy access when the device is no longer in the possession of the owner. Encryption is a requirement under the Health Insurance Portability and Accountability Act (HIPAA) in the United States and under the GDPR if appropriate for the risk. If the device supports it, also use biometrics like fingerprint or facial recognition to make unwanted access more difficult.

2. Prevent business apps from sharing data with personal apps

Mobile operating systems allow the sharing of data between apps on the device. For example, end users can receive document attachments in business email and then open those documents in other apps, like PDF readers or document editors. Once an app opens a document, the app can then store or transmit that document outside the control of IT. This is a very common vector of data loss. No business app on the device should be allowed to export data to a personal app.

3. Automatically delete business data from compromised devices

Devices frequently fall out of compliance due to security issues like jailbreaking, rooting, malware, or out-of-date firmware. Remediation actions should be automated and not require manual IT intervention. If the compliance issue is severe, business data should be automatically deleted from the device. Closed-loop compliance, from detection through remediation, is essential for risk mitigation. The longer a compromised device contains business data, the greater the risk of breach. To preserve privacy, IT should be able to delete the business data on the device without deleting the personal data.

4. Tunnel business traffic without tunneling personal traffic

Just as checklist item #3 requires the separation of business and personal data on the device, this item requires a similar separation in the network. A device-wide VPN will send data from both business and personal apps through the corporate network. A per-app VPN, on the other hand, can be configured to send only the traffic from business apps through the corporate network, thereby protecting that traffic while preserving the privacy of the end user's social media feed and other personal communications.

5. Stop unauthorized devices from accessing business cloud services

Most organizations run business cloud services from multiple vendors, such as a productivity suite from Microsoft and a CRM solution from Salesforce. If an unauthorized device gains access to any of those services, it can download data from that service to the device. That data is now outside the control of IT. This often happens when an end user downloads a business app to a personal device for convenience. Business data should never be on a device unless IT can delete apps and control data sharing on that device. IT must be able to apply these security controls across all its business cloud services, regardless of vendor. Securing only Office 365 is not adequate. This control is relevant for both the GDPR and NIST Cybersecurity Framework Category DE.CM-7 ("Monitoring for unauthorized personnel, connections, devices, and software is performed") because it prevents unauthorized devices from accessing business data.

6. Stop unauthorized apps from accessing business cloud services

To protect data, IT must be able to ensure that both the device and the app accessing the cloud service are secure. If the device is secure but the app is not, data will be lost. A common example is when end users download business apps directly from consumer services like Apple's App Store or Google Play instead of through their company's internal enterprise app store. Though the app seems the same to the end user and runs on a secure device, IT can neither delete it nor control its data sharing. IT must be able to stop unauthorized apps from accessing any business cloud services, not just Office 365. This control is relevant for both the GDPR and NIST DE.CM-7 because it prevents unauthorized software (apps) from accessing business data.

7. Detect and remediate zero-day exploits

The prior controls mitigate the risk of data loss. However, bad actors are always discovering new hardware, software, and behavioral vulnerabilities to exploit. Ongoing machine learning-based analysis of device, app, and network threats combined with the ability to remediate at the endpoint allows IT to respond to new threats quickly.

8. Provide rich security controls for Android, iOS, macOS, and Windows 10

It is no longer just a Windows world. Most organizations support endpoints across a variety of operating systems. Older operating systems, like Windows 7, have legacy security tools, but modern operating systems, like Android, iOS, macOS, and Windows 10, have evolved to endpoint architectures that support unified, cross-platform security solutions. IT should choose a solution that provides rich controls that fully leverage the native security frameworks of these different operating systems.

9. Certify for device security (Common Criteria Protection Profile for MDM)

Common Criteria is an international standard for computer security certification. The Protection Profile for Mobile Device Management (MDM) sets requirements on how to apply security policies to mobile devices in order to process enterprise data and connect to enterprise network resources. Common Criteria is often a requirement of government institutions and high-security organizations. IT should choose a security solution that has this certification.

10. Certify for cloud security (SOC 2 Type 2 and FedRAMP)

If the security solution IT deploys is itself cloud-based, it should have a Service Organization Controls (SOC) 2 Type 2 report with a detailed description of the auditor's test of operations and compliance controls. This test assures the effectiveness of controls relating to the security, availability, processing integrity, confidentiality, and privacy of the provider's systems. FedRAMP Authority to Operate (ATO) is a formal United States certification that recognizes that the provider has also passed the federal risk management process for security requirements. IT should choose a security solution that has these certifications.

This 10-point checklist is a distillation of best practices we have seen across MobileIron customers. It is intended as one input into your security, compliance, and legal policy definition process. We expect each organization will develop the guidelines best-suited for its industry, geography, and organizational risk tolerance.

Using MobileIron for Cloud Security

MobileIron is a government-grade cloud and endpoint security platform. Here is how our customers leverage MobileIron technology to address the checklist above:

Checklist # 1, 2, 3, 8

Enroll device in MobileIron: Use MobileIron to install a configuration profile on the device that allows IT to take the security actions necessary to protect business data.

Set security policies: Set the appropriate password and encryption policies in MobileIron. Use biometrics for authentication if available. If a device falls out of compliance, automatically quarantine or selectively wipe it. When employees leave the organization, do a full wipe on the device if corporate-owned or a selective wipe if employee-owned.

Put business apps under management: Use MobileIron to distribute business apps through the Apps@Work enterprise app store or Managed Google Play. When installed, these apps are managed through policy controls set in MobileIron. That means IT can prevent data sharing between business and consumer apps and delete the apps over-the-air when necessary. This puts enterprise data under the control of IT without compromising the privacy of personal data on the device.

Checklist # 4

Deploy per-app VPN: Use MobileIron to configure business apps so that they only connect to on-premises services through MobileIron Tunnel per-app VPN. This separates business app traffic from consumer app traffic, so that excess personal data does not flow through the corporate network.

Checklist # 5, 6

Allow only trusted devices and apps to access cloud services: Use MobileIron Access to block unmanaged, unauthorized, or non-compliant devices and apps from authenticating to cloud services like Office 365, Salesforce, ServiceNow, Workday, etc. MobileIron Access is a multi-cloud, multi-identity, standards-based solution that extends across the many cloud services and identity providers in an enterprise.

Checklist # 7

Detect and remediate zero-day threats: Use MobileIron Threat Defense to monitor for suspicious device, app, and network activity. When an issue is uncovered, trigger MobileIron policies to take the appropriate remediation action, like user notification, device quarantine, or data wipe.

Checklist # 9, 10

Don't compromise on security certifications: MobileIron was the first solution to gain certification for the Common Criteria Protection Profile for MDM v2. MobileIron is also SOC 2 Type 2 compliant and has FedRAMP Authority to Operate (ATO).

Modern security is evolving and IT professionals sometimes ask if Microsoft Intune can fully support this checklist. We do not think it can, especially for checklist items # 3, 4, 5, 6, 7, 8, 9, and 10. MobileIron is committed to a multi-OS, multi-cloud, and multi-identity security architecture that supports the best-of-breed technology choices of modern enterprises.

Summary

Most organizations will face a security audit of some type, either internal or external, over the next few years. The goal is the same – protect data from both malicious compromise and well-intentioned loss – but the mechanisms to do so are very different between traditional and modern security architectures. A structured audit checklist can provide a starting point for the people, process, and technology investments that will enable an organization to quickly and securely tap into the innovation of cloud services.

In any cloud deployment, endpoint security must stay top-of-mind to satisfy the GDPR, the NIST Cybersecurity Framework, and similar compliance models. Modern apps on modern endpoints are how employees consume cloud services, but data will be lost if those endpoints and apps are not secure. How much data is lost will depend on how quickly organizations implement an end-to-end, multi-cloud security solution like MobileIron as they move to Microsoft Office 365, Salesforce, ServiceNow, Workday, and beyond.