Top 10 best practices for securing the cloud with Ivanti

In the Everywhere Workplace, enterprise computing architectures are rapidly shifting business apps and data to the cloud. Traditional security approaches, such as a network perimeter and locked-down endpoints, can no longer ensure the integrity of cloud data across the perimeterless enterprise. What's needed is an end-to-end, zero trust security framework that significantly reduces risk by giving IT complete control over business data wherever it flows across devices, apps, networks and cloud services.

This ten-point checklist is designed to help organizations understand essential best practices for designing a security architecture in a zero trust world so they can better protect cloud data across the perimeterless enterprise. Each organization should still conduct a separate analysis of their cloud architectures to identify potential security gaps and ensure the current deployment meets relevant industry compliance requirements. For instance, many organizations are subject to 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.

Security audit checklist

1. Enforce device encryption and password protection.Mobile devices are frequently lost or stolen.
   a. 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, organizations should also leverage multi-factor authentication (MFA) and biometrics like fingerprint or facial recognition to protect against unauthorized access.
2. Prevent business apps from sharing data with personal apps.
   a. 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. To prevent unauthorized data sharing, IT needs to enforce controls to prevent users from copying and pasting business content into personal apps, or from sending corporate files and email attachments to a personal cloud drive or email address. No business app on the device should be allowed to export data to a personal app.

3. Automatically delete business data from compromised devices.
    a. Mobile devices frequently fall out of compliance due to security issues like jailbreaking, rooting or malware. 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.
    a. 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 can send data from both business and personal apps through the corporate network, which can put personal privacy at risk. 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.
    a. 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 Office 365 alone is not adequate. This control is relevant for both the GDPR and NIST Cybersecurity Framework Category
    b. 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.
    a. 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 the Apple App Store or Google Play instead of through their company's internal enterprise app store.
    b. Though the app seems the same to the end user and runs on a secure device, IT can neither delete it nor control how it shares data. 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.
    a. 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.
    a. It is no longer just a Windows world. Most organizations support endpoints across a variety of operating systems. Older operating systems 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).
    a. 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).
    a. Any cloud-based security solution 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 confirm that their cloud-based security solutions have these certifications.

This ten-point checklist summarizes the best practices captured from thousands of real customer deployments. This guide is intended to inform security, compliance and legal policy definitions, but every organization must also consider industry regulations, geography and organizational risk tolerance before choosing and implementing a solution.

Using Ivanti for cloud security

Ivanti Unified Endpoint Management (UEM) provides the foundation for the industry's first end-to-end, zero trust enterprise security framework. Ivanti UEM puts mobile security at the center of your enterprise and allows you to build upon it with enabling technologies such as zero sign-on (ZSO) user and device authentication, multi-factor authentication (MFA) and mobile threat detection (MTD). Here's how our customers leverage Ivanti technology to address the checklist above:

Checklist # 1, 2, 3, 8

Enroll devices in Ivanti. Use Ivanti 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 Ivanti. Use biometrics for authentication if available. If a device falls out of compliance, automatically quarantine or selectively wipe business apps and data. When employees leave the organization, perform a complete factory reset on the device (if corporate-owned), or a selective wipe (if employee-owned).

Put business apps under management. Use Ivanti 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 Ivanti. 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 Ivanti to configure business apps so they only connect to on-premises services through the Tunnel per-app VPN. This separates business app traffic from consumer app traffic to ensure that personal data does not flow through the corporate network.

Checklist # 5, 6

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

Checklist # 7

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

Checklist # 9, 10

Don’t compromise on security certifications. We delivered the first solution to gain certification for the Common Criteria Protection Profile for MDM v2. Ivanti is also SOC 2 Type 2 compliant and has FedRAMP Authority to Operate (ATO). Modern security is evolving and Ivanti 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 enterprise organizations will need to pass either an internal or external security audit within the next few years. By building an end-to-end, zero trust security framework now, organizations can confidently meet compliance standards by protecting data in clouds, endpoints, and apps across the perimeterless enterprise. This audit checklist provides a starting point to help organizations meet regulatory requirements for GDPR, the NIST Cybersecurity Framework, and other compliance models. Organizations should seek out the expertise they need to fully analyze their infrastructure and ensure it meets both internal and external requirements.

To learn how Ivanti can help your organization deploy government-grade security across your cloud infrastructure, please contact us at www.Ivanti.com.

ivanti.com
1 800 982 2130
sales@ivanti.com