DXC TECHNOLOGY

Authorised Reseller

Managed Service Provider

Tip sheet:

How security leaders can strengthen cybersecurity and meet compliance: With DXC Modern Workplace for Apple

Security leaders today face increasing threats, from AI-driven phishing attacks to complex ransomware tactics. These leaders must continually protect their organisations from breaches while ensuring compliance with rigorous regulations. For digital workplace services, managing security for remote and hybrid workforces introduces additional complexities, particularly as shadow IT and bring-your-own-device practices proliferate. Cybersecurity is not a set-and-forget discipline, and security leaders are constantly seeking ways to harden their security posture. Unfortunately, organisations across industries continue to face the consequences of vulnerabilities in digital products and services, especially when dealing with outdated systems and infrastructure complexity. To address these challenges, security leaders require robust, scalable workplace security solutions that safeguard the organisation from endpoint to cloud.

How DXC Modern Workplace for Apple helps overcome key security challenges

With the growing sophistication of cyberthreats and increasing regulatory demands, security leaders need digital workplace services that are both comprehensive and easy to manage. Here's how DXC Modern Workplace for Apple can help overcome these challenges:

1 Achieve end-to-end security

Comprehensive cybersecurity requires a multi-layered approach that addresses every aspect of the IT infrastructure. DXC offers a full range of workplace security solutions that cover endpoints, applications, cloud environments, and networks. With managed detection and response, threat and vulnerability management, and automated incident responses, DXC helps security leaders to defend against potential breaches.

Apple's Secure-by-Design principles complement this by embedding security into the core of its devices. Apple integrates hardware and software so security features like secure boot and FileVault encryption are automatically in place on all devices. With DXC's advanced security operations centres interpreting Apple's efficient logging and telemetry systems, organisations benefit from a security framework that spans from device to cloud. This helps reduce vulnerabilities, improves threat detection, and makes systems inherently resistant to security breaches.

2 Minimise risk from lost or stolen devices

With the shift to hybrid working environments, securing devices outside corporate networks is crucial. DXC's endpoint security management includes encryption, data protection, and remote wipe capabilities, providing security leaders with the tools they need to manage devices effectively. Whether employees are working from home or on the move, these features mitigate the risks associated with lost or stolen devices.

Apple's Activation Lock and FileVault encryption further strengthen this defence by ensuring that sensitive data remains protected and inaccessible to unauthorised users. With DXC Modern Workplace for Apple, organisations can reduce the risk of data breaches in remote and mobile work environments significantly.

3 Maintain compliance with global standards

Complying with local and international regulations is vital to avoid costly penalties and protect an organisation's reputation. DXC offers a comprehensive suite of cyber risk and compliance management services, providing audit trails, data governance, and continuous monitoring. Security leaders gain full visibility into their organisation's security landscape, letting them manage compliance more effectively.

Apple's built-in security features align with global compliance standards, so every device meets regulatory requirements from deployment. DXC's expertise in interpreting compliance frameworks, such as GDPR and CCPA, combined with Apple's Secure-by-Design architecture, helps organisations reduce the risk of non-compliance while maintaining a secure environment.

4 Simplify multi-platform security management

Managing a variety of devices across different operating systems can be complex. DXC helps streamline security management by offering cross-platform services, giving security leaders visibility and control over all endpoints. This approach ensures consistent security policies are enforced across all devices, from Mac to PC, and from mobile to cloud.

Apple devices integrate seamlessly with management platforms like Jamf and Microsoft Endpoint Manager, so organisations can apply security protocols consistently across the enterprise. With DXC managing this infrastructure, security leaders can manage multi-platform environments confidently without sacrificing security.

5 Strengthen security with zero-touch deployment

Deploying devices securely from day one is crucial to reducing vulnerabilities. DXC's zero-touch deployment service configures devices with the necessary security settings straight out of the box, removing the risk of configuration errors. This approach streamlines device rollouts, with security policies consistently applied right from the outset.

Apple Business Manager further supports this by automating the deployment process, also activating security protocols from the moment of first use. Together, this delivers a seamless, secure device deployment experience that enhances security and reduces risk.

The DXC Modern Workplace for Apple difference

Protecting an organisation from sophisticated cyberthreats while meeting compliance requirements is a top priority for security leaders. DXC offers a comprehensive portfolio of security solutions that safeguard IT infrastructure from endpoint to cloud, featuring proactive monitoring, advanced threat detection, and cross-platform management. These capabilities help organisations quickly detect and respond to threats, reducing the risk of breaches.

Apple's Secure-by-Design approach, with built-in hardware and software protections, adds an additional layer of defence. Features such as encryption, automatic updates, and secure boot decrease the likelihood of security incidents by up to 90 per cent for Mac users.[1] By combining these strengths with DXC's expertise, security leaders can build a resilient security posture that not only withstands current threats but also addresses future compliance challenges.

As an Apple Managed Service Provider, DXC provides Device Procurement Services, Apple Financial Services, Apple Professional Services, and Integrated Service Desk support with access to AppleCare for Enterprise and AppleCare OS Support. The combination of Apple's Secure-by-Design platform and DXC's expert analysis enhances cyber resilience, helping organisations meet regulatory frameworks and improve their cybersecurity stance across digital workplace services.

[1] Commissioned study by Forrester Consulting on behalf of Apple," The Total Economic Impact™ (TEI) of Apple, available at https://tei.forrester.com/go/Apple/TEI/?lang=en-us

Learn more about how DXC Modern Workplace can support your Apple technology, at:

dxc.com/au/mwp-apple

Get the insights that matter.
dxc.com/optin

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private, and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.