Workforce Application Infrastructure

Best Practices for Building Effective Digital Workplaces

Executive Summary

Workforce Application Infrastructure focuses on technologies that enable, manage, and secure applications and devices used by employees to enhance productivity, collaboration, and security within an organization. It emphasizes the integration of desktop applications, mobile device management (MDM), endpoint security, and identity security to create a cohesive infrastructure for workforce operations.

It serves as the backbone for modern enterprise IT environments, ensuring that the workforce—whether on-site, remote, or hybrid—can access the tools they need securely and seamlessly across diverse devices, including desktops, laptops, tablets, and smartphones.

Introduction **3**
Managing a Distributed Workforce 3
Application Delivery and Management **5**

Introduction

Workforce Application Infrastructure refers to the integrated set of technologies, systems, and processes that enable organizations to deliver, manage, and secure applications and devices used by employees to drive productivity, collaboration, and operational efficiency.

It serves as the backbone for modern enterprise IT environments, ensuring that the workforce—whether on-site, remote, or hybrid—can access the tools they need securely and seamlessly across diverse devices, including desktops, laptops, tablets, and smartphones.

This bridges critical components such as desktop applications, mobile device management (MDM), endpoint security, and identity security to create a cohesive ecosystem that supports the digital workplace.

Managing a Distributed Workforce

At its core, Workforce Application Infrastructure addresses the challenges of managing a distributed and dynamic workforce in an era of digital transformation.

It enables organizations to deploy applications efficiently, maintain device compliance, protect sensitive data, and ensure secure access to resources while supporting employee productivity and user experience.

This infrastructure is particularly vital in environments where employees use a mix of company-owned and personal devices (BYOD), requiring robust solutions to balance flexibility, security, and scalability.

Key objectives of Workforce Application Infrastructure include:

- **Application Accessibility:** Ensuring employees can access critical applications (e.g., productivity suites, collaboration tools, or industry-specific software) on any device, anywhere, with minimal friction.
- **Device Management:** Centralizing the oversight of devices through MDM or Unified Endpoint Management (UEM) to enforce policies, manage updates, and ensure compliance.

- **Security and Compliance:** Integrating endpoint security (e.g., antivirus, encryption) and identity security (e.g., single sign-on, multi-factor authentication) to protect against threats and meet regulatory requirements.
- **Scalability and Automation:** Supporting large-scale deployments and ongoing management through automated tools, reducing IT overhead and enabling rapid adaptation to workforce changes.
- **User Experience:** Providing a seamless and consistent experience across devices and platforms, enhancing employee satisfaction and productivity.

Workforce Application Infrastructure is particularly relevant in the context of modern workplace trends, such as remote work, cloud adoption, and the increasing use of mobile devices.

It encompasses subcategories like Application Delivery and Management, which focuses specifically on deploying and managing applications across devices, as well as broader frameworks like Digital Workplace Platforms or Secure Access Service Edge (SASE) that integrate application delivery with network and security services.

By aligning these components, Workforce Application Infrastructure empowers organizations to create a secure, efficient, and flexible environment that supports their workforce's evolving needs.

Application Delivery and Management

Application Delivery and Management systems to deploy, configure, update, and manage applications across devices including desktops, laptops and mobile in an organization. It ensures that applications are accessible, secure, and optimized for workforce productivity.

Key aspects include:

- **Application Deployment:** Distributing and installing applications on devices, often through centralized platforms like Mobile Device Management (MDM) or Unified Endpoint Management (UEM).
- **Application Management:** Ongoing tasks like updating, patching, and configuring applications to ensure compatibility and performance across devices.
- **Cross-Device Compatibility:** Ensuring applications work seamlessly on different operating systems (e.g., Windows, macOS, iOS, Android).
- **Security Integration:** Incorporating endpoint and identity security to protect applications during deployment and use.
- **Automation and Scalability:** Using tools to automate deployment and manage applications at scale, reducing IT workload.