vmware

Is Your Security Strategy Built for Anywhere Work?

Protect apps and data while improving employee experience

Endpoints: the good, the bad and the ugly

Endpoints are the gateways to your business. However, allowing the increased access your employees want can increase your risk.

Bad actors are working to gain access to corporate assets, and employees face myriad threats:

- Phishing email, SMS, and WhatsApp messages
- Pretexting and impersonations
- Malicious content
- Zero-day threats, device and application vulnerabilities
- Machine-in-the-middle attacks

Most of these threats involve the human element. It's no surprise that **82 percent** of reported breaches involve humans, according to Verizon.[1]

82%

The ability to work from anywhere, on any device, is key to employee satisfaction.

However, IT faces tough choices when it comes to protecting remote and hybrid employees.

Limit employee access to resources

- Allow access only to corporate devices
- Grant access only to select applications
- Allow only email communications
- Prohibit the use of public WiFi

Require lots of actions on the part of users

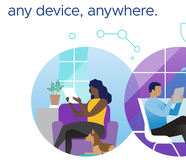
- Multiple logins and re-verification of identity
- Login and connection over a corporate VPN

Because these

"choices"

negatively impact employee experience, they don't feel like choices at all.

There is a better way. VMware Workspace Security enables end users to securely access any app, on any device, anywhere.



It's also part of a successful Zero-Trust strategy, starting with **segmented conditional access**, achieved by authenticating users at the endpoint and segmenting their access to resources via automatic, seamless per-app tunneling.

A series of connections that automatically secure traffic per application—*only when the application is in use.*

One big pipe connecting to your corporate network

How segmented conditional access works:

- Verify the integrity of a user and their device.
- Grant secure access to on-premises apps, SaaS apps, intranet sites, or virtual desktops.
- Individual per-app tunnels are dynamically configured as needed.
- End users conveniently access all their resources from one place via passwordless single sign-on (SSO).

If a user is out of compliance with policy-defined thresholds for security, conditional access policies can be instantly applied. For example:

- A user working at odd hours or at an unconventional location may need to supply additional authentication via a token or other phishing-resistant form of multifactor authentication.
- A user attempting to access high-security applications from an insecure device may be prompted to add additional security to their device or leverage a virtual desktop session for access.

The simplicity of management and security integrated into a single platform

Easily configure conditional access via the Workspace ONE platform.

- Connect with multiple identity providers (IdPs).
- Use phishing-resistant MFA built into Intelligent Hub or bring your own MFA solution.
- Configure secure policies for managed corporate-owned devices and unmanaged personally owned devices.
- Provide end users a single app—Workspace ONE Intelligent Hub—to authenticate, access work apps and resources, and view security status and alerts.

Automatically detect and respond to threats to improve compliance and scale remediation efforts.

- Detect advanced threats across desktops and mobile devices including iOS, Android and Chrome OS.
- Feed security information from Workspace ONE UEM and VMware Trust Network partners into the machine learning–powered Workspace ONE Intelligence platform.
- Create adaptive policies and auto-remediate threats via Workspace ONE Unified Endpoint Management (UEM).
- Address smartphone risk with advanced mobile threat protection that integrates with Workspace ONE UEM.

Interconnect management and security teams and technologies.

- Keep stakeholders in the know with topline reports with drill-down detail, rich context, and insights that inform orchestration.
- Create policies that trigger automated remediation if issues are found.
- Leverage Workspace ONE Intelligence to analyze risk and automate tasks with Workspace ONE UEM and third-party platforms, including ITSM solutions.

Get started

To learn more about how VMware Workspace Security can protect your anywhere organization, visit vmware.com/go/workspacesecurity or talk to your sales representative.

[1] Verizon. "2022 Data Breach Investigations Report." Gabriel Bassett, C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup. 2022.