VMWARE ON VMWARE CUSTOMER STORY

VMWARE WORKSPACE ONE TRANSFORMS VULNERABLE SIGN-ON PROCESSES INTO A HIGHLY SECURE SSO SOLUTION

INDUSTRY

CLOUD COMPUTING AND PLATFORM VIRTUALIZATION SOFTWARE AND SERVICES

LOCATION

PALO ALTO, CALIFORNIA

KEY CHALLENGES

- Prevent unauthorized access to apps, regardless of device
- Implement sign-on security measures that colleagues will use effectively
- Reduce IT/help desk burden, especially with password reset requests

SOLUTION

VMware Workspace ONE®—incorporating VMware Identity Manager™, VMware Workspace ONE UEM, and VMware Horizon® View™—offers an easy-to-use SSO process that ensures industry-standard security at every step.

BUSINESS BENEFITS

- Enables easy-to-use app SSO regardless of access method (device, browser)
- Significantly enhances overall app security, systemwide
- Further reduces IT/help desk burden with users' self-service

Modern hacking advances combined with the proliferation of anywhere, anytime devices and user apathy about security left VMware apps vulnerable. VMware IT needed to find an alternative to the traditional sign-on process, one that offered superior security and end-user simplicity.

VMware, a subsidiary of Dell Technologies, provides cloud computing and platform virtualization software and services. It was the first commercially successful company to virtualize the x86 architecture. Today, VMware software powers the world's complex digital infrastructure. The company's various offerings provide a dynamic and efficient digital foundation to more than 500,000 customers globally, aided by an ecosystem of 75,000 partners.

The Challenge

Tens of thousands of colleagues at VMware access apps from a variety of devices on a daily basis, and that inadvertently created an unexpected security problem. The traditional sign-on process to access apps is vulnerable to modern day hacking. Once in, an attacker can potentially infiltrate the entire infrastructure. Making matters worse, each app requires a unique password—users either write them down or are otherwise lax with security—which creates vulnerabilities IT can't easily mitigate. For example, alternative software solutions (such as exponential passwords) have proven equally ineffective as colleagues either bypass them or ignore safeguards altogether.

The Solution

Given the gravity and complexity of this issue, VMware IT employed VMware Workspace ONE with VMware Identity Manager and Workspace ONE Unified Endpoint Management (UEM) to create a powerful single sign-on (SSO) solution that offers both top-flight security and remarkable ease of use.

Security from Every Angle

Workspace ONE offers colleagues an all-in-one location for every app they need, accessed via a single password across ubiquitous platforms (including Windows 10, iOS, Mac OS, and Android). The Identity Manager and Workspace ONE UEM components make mobile SSO a simple, effortless process as remote colleagues can seamlessly connect via any device without the hassles of logging in and configuring their applications. Required apps, profiles, and credentials are automatically loaded upon sign-in.

VMWARE FOOTPRINT

- VMware Workspace ONE
- VMware Workspace ONE UEM
- VMware Identity Manager
- VMware Horizon View

Dynamic entitlements enable administrators to enforce automated least privilege. Apps are appropriately and automatically added or removed without the need of IT intervention. And if a colleague is terminated or resigns, the system de-provisions their credentials either that day or within an hour depending on the size of the environment. Plus, conditional access via Identity Manager lets managers create several levels of access based on network, application, and other variables.

Ease of Use That People Actually Use

With all apps contained in a single location, colleagues no longer have to ask others for the right app URL. They can bookmark frequently used apps, allowing even faster access. Quick searches for non-regular resources (such as accessing seldom-used apps) are simplified, and these apps can be bookmarked from the search results, as well. And with tagging/categorization based on organization, colleagues can explore additional apps relevant to their job function. Virtual desktop access to VMware Horizon View is easy via Workspace ONE. The adaptive management capability offers users varied and appropriate authentication processes depending on their specific circumstances—everything from browser-only access (no device) to full device configuration/management by VMware IT, location, and network. The system always adapts to how colleagues want to access their apps while adhering to IT control policies.

Substantial IT and Help Desk Benefits

On the IT side, applications can be effortlessly pushed to colleagues, and an app catalog makes it simple to selectively install applications—all while automatically adhering to corporate rules and policies. Help desk personnel are less burdened with password reset requests, one of the largest issues they typically must manage in a large enterprise. This factor alone dramatically changed their productivity output as they can now focus on mission-critical issues.

But that's just the tip of the iceberg. IT deploys requirements and controls via Workplace ONE in numerous ways throughout the VMware ecosystem. These include BitLocker encryption and status, device enrollment trends, mobile application versioning for patching adoption/measuring of OS versioning rollouts, end-of-life (EOL) device discovery, Dell BIOS and application versioning (security and compliance), daily online trends, and Microsoft patches.

Stadium-Sized Success

Today, thanks to Workplace ONE, more than 25,000 colleagues (enough to fill a stadium) access nearly 800 applications and resources via more than 4.2 million launches a month from a wide variety of devices via SSO. Support calls to IT involving password resets have dramatically decreased, and overall colleague adoption rates have exceeded expectations. Best of all, IT met their major goal of empowering colleagues (and reducing overall IT burdens) via SSO adaptive management, all while ensuring privacy rules and safeguards are always enforced.

For more details on the VMware on VMware program go to
https://www.vmware.com/company/vmware-on-vmware.html.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com