VALCARI

VIEM

Valcari's

Integrative

Endpoint Management

VIEM allows remote, hybrid or in-office employees to work securely from any device anywhere.

VIEM is critical to uniformly manage all endpoint devices for onboarding or daily activities on a single console from the cloud.

700 12th St. NW
Suite 700-97388
Washington, DC 20005
T. (720) 842-9902
E. solutions@valcari.net

VIEM

Valcari‘s Integrative Endpoint Management

WHY?

The Current Environment

Coronavirus has transformed how we work and the technology we use every day in the workplace. The shift has required employees to remote work or a hybrid work situation. Remote work or hybrid work is not going away but will be an integral part of the modernized workforce in the future. This has required an increase in a company's security perimeter not only in its physical location, but wherever an employee is accessing a company's data or infrastructure.

Why VIEM?

Anyone can purchase a UEM, EMM, MDM software package and start to implement its configurations. But what makes Valcari different is.... You are getting a company that has over a decade of experience with mobility and can evaluate your business needs and integrate a UEM with your current business operations with minimal interruption to end users with Government-level secure configurations your company needs. Valcari can do it faster, with more security and at less of an expense than hiring more IT employees because mobility is what we do!

Valcari's Integrative Endpoint Management

Capabilities and Benefits

- Digital workspace platform that is intelligence driven. Will securely and simply deliver and manage any application on any device while integrating app management, access control, multiplatform management of endpoints.
- Choose to: bring your own device (BYOD), choose your own device (CYOD); company-owned, personally enabled (COPE) device; or company-owned, business-only (COBO) device.
- Reporting - Gain control access and in-depth visibility by generation of custom reports and automated remediation actions.

Onboarding

- Gain a seamless, out-of-the-box experience for employees by eliminating laptop imaging with configuration settings on the endpoint management.
- Configure and manage dynamic smart groups, which consider user attributes, and device information which updates automatically as those change.
- In under an hour, you can onboard a new employee with all devices and apps without the need for help desk calls or tickets.
- From anywhere in the world and within minutes from the cloud you can provision a new corporate laptop right out of the box.
- Automate your traditional onboarding and laptop and mobile device configurations.
- Delivers real-time application lifecycle management.
- Bridge legacy enterprise client-server apps to the cloud.

VIEM

Valcari‘s Integrative Endpoint Management

Authentication

- Single Sign-On (SSO) capabilities and support for multifactor authentication simplifies application and access management.
- Password-free access by leveraging device trust and biometric timeout settings for authentication.
- Leverage new and existing forms of third-party authentication by authentication brokerage.
- Endpoint compliance with conditional access
- Zero-trust security
- Passwordless user authentication
- Passwordless multi-factor authentication uses device-as-identity for a on-premise application or single cloud.
- Transform employee onboarding with a unified app catalog.

VIEM

Valcari‘s Integrative Endpoint Management

Automation & Efficiency

- Across your entire digital workspace environment gain insights and automation capabilities.
- Leverage OS management interfaces by shrink-wrapped device provisioning to self-configure smartphones, tablets, and laptops for instantaneous enterprise use.
- Can enable devices to receive patches for vulnerabilities quickly through the operating system vendor, which leaves the app management and configuration to IT.
- Admins have the power to distribute files directly to users, groups, devices, and more across external cloud storage providers and internal repositories to ensure the most up-to-date information is given to employees.
- Receive notifications and contextual actions on mobile devices
- View your entire digital workspace environment in one place that aggregates and correlate devices, application, and user data.
- Enterprises can now automatically update, install, remove software packages, and provide scripting and file management tools
- Create an automated workflow for applications, scripts, files, software, and commands to install on laptops.
- Configure installation on demand or during enrollment.
- Set packages to be installed based on conditions, or a defined schedule.
- Deploy software updates automatically and let users be notified when those updates occur.
- App analytics and automation
- Configure and enforce data policies and access across all devices, applications, and locations in one place.

Employee Experience

- Flexible management designed to increase adoption for even the most ardent privacy-sensitive employee.
- Unified onboarding and catalog in a single destination for employees. Ability to access optional Hub Services1 such as Notifications, Home, and People.
- Simple to manage integrated contacts with email and calendar.
- For employees on the go there is a consumer-simple, enterprise-secure email application.
- Secure collaboration on content. Users can edit, share, markup and create securely from Share-Point, Google Drive, DropBox and more.

Legacy

- Deliver any application from the latest cloud apps to legacy enterprise apps.

Security

- Reduce data leakage by advanced email attachment security.
- Control access on a per-application basis to mobile, Mac, Windows, virtual apps, and Chrome.
- Automate access decisions and keep your business data safe by analyzing authentication context such as network location, target app, device state, user group, and authentication method.
- Enforce policies through your policy engine by using UEM technology.
- Enforce IT policy compliance on blacklisted and whitelisted apps, jailbroken devices, and open-in app restrictions.
- Based on user behavior, companies can automate access control policies, apply the latest security patches, and quickly identify out-of-compliance devices.
- Connect end users automatically with corporate resources such as VPN, per-app VPN, Wi-Fi, with advanced options for certificate authentication for secure connectivity to back-end systems.
- Administrators can remotely monitor and manage all devices connected to your enterprise.
- Without device management, secure employee business apps and contractor devices.
- Secure web browsing – Protect both data-at rest and data-in-motion.
- Create secure tunneling and custom bookmarks so users can safely and quickly access company information.

Security (Cont.)

- Mobile app containerization – Choose from an environment of integrated apps and in-house mobile apps that provide an additional layer of security.
- Derived Credentials – By utilizing personal identity verification (PIV) and common access cards (CAC) your company creates an environment of two-factor authentication.
- Per app VPN – Without requiring any user interaction, you can allow access to corporate resources behind the firewall by creating policies that authorize specific mobile apps access.
- Trust Engine – Provide adaptive access control by utilizing a combination of various signals such as device, network, app, geographic region, and user.

Any Device.
Anywhere.
Securely.

700 12th St. NW
Suite 700-97388
Washington, DC 20005
T. (720) 842-9902
E. solutions@valcari.net

www.Valcari.net

VALCARI