Andromeda
TECHNOLOGY SOLUTIONS

AndroForge™
“Your Daddy’s” Network Management Won’t Cut It Anymore

The “Why”

Microsoft’s original Active Directory system dates back to the 1990’s. It’s safe to say that the digital world looked and behaved quite differently back then
(Cloud Server?—what’s that?!)

Active Directory is Sooo Last Millenium!

The “What”

Andro-NetTM Manage is Andromeda’s bundled offering of Cloud-centric services for managing network environments. It is built around Entra ID and Intune applications—Microsoft's next-generation framework that supplants Active Directory and its now antiquated premises-centric network management.

Entra ID manages user identities and access control, while Intune is a Cloud-based service that manages and secures devices. Bundled together with Andromeda’s top-tier IT design and service support, Andro-Net provides secure access to organizational resources on a user-by-user basis across various wired and remote devices by verifying user identities and enforcing device policies.

Andro-Net allows seamless integration between identity management and device management

“Your Daddy’s” System With Traditional (AD-based) Network Management

- **Limited** (local) Admin access
- **Limited** to Windows platform
- **No** global management of users
- **No** centralized management of software
- **No** centralized management of company data
- **Lengthy, laborious, error-prone** process to swap devices and move/install software and data from old devices

Your System With AndroForge™

- **Cross-platform support** (Windows, macOS, iOS, Android, and even Linux)
- **Flexible device management** (wired/remote; desktops, tablets, laptops, phones, printers, ...)
- Native user authentication
- **AI-supercharged identity protection** detects suspicious login behavior and automates risk-based access decisions.
- Robust password management and setup (Self-Service Password Reset reduces IT support requests.)
- User **profile management with scalable permissions** for application/device access
- Physical device lockdown and remote wipe options
- Software policy rollout
- Definable secure borders where company data can live
- As much as **500% faster setups** for new users or devices!

AndroForge™ in Depth

Most modern companies operate as a hybrid business environment with remote and on-premises employees as well as remote office spaces consisting of both company-owned or personal devices. Rather than the old patchwork of user/device management allowed by the previous generation of network tools, AndroForge™ natively provides all these benefits:

01 Unified Endpoint Management (UEM)

- **Manage All Devices in One Place:** Allows you to manage company-owned and personal (BYOD) devices from a single Cloud-based platform.
- **Cross-Platform Support:** Works with Windows, macOS, iOS, Android, and even Linux.

02 Enhanced Security & Compliance

- **Zero-Trust Security Model:** Ensures every device and user is verified before granting access.
- **Conditional Access:** Expands network control by allowing/blocking access based on user, device, or location.
- **Remote Wipe & Selective Wipe:** Securely erases data from lost, stolen, or off-boarded employee devices.

03 Simplified Hybrid Work & Remote Management

- **No VPN Required for Management:** Employees can work from anywhere while IT administration retains full control over security.
- **Over-the-Air (OTA) Updates:** Deploys policies, security patches, and software updates remotely.
- **Remote Troubleshooting:** IT administration can monitor, support, and resolve issues without requiring physical access to devices.

04 Device Lifecycle Automation

- **Auto-pilot for Zero-Touch Deployment:** Set up new devices with pre-configured settings right out of the box.
- **Role-Based Access Controls (RBAC):** Assign different policies for remote vs. in-office employees.

05 Application & Patch Management

- **Manage & Deploy Apps Securely:** Control which apps employees can install and enforce security policies.
- **Automate Updates & Patch Management:** Keep systems secure with scheduled software updates.
- **Block Unauthorized Apps:** Prevent installation of risky software on company-managed devices.

06 Support for BYOD (Bring Your Own Device)

- **Separate Work & Personal Data:** Users can use their personal devices while AndroForge™ ensures company data remains secure.
- **App Protection Policies:** Protect corporate data within apps (e.g., Outlook, Teams) without full device control.
- **Compliance-Driven Access:** Allow access to company resources only if the personal device meets security policies.

07 Cost Savings & IT Efficiency

- **Eliminate On-Premise Infrastructure:** Cloud-based management reduces dependency on on-site servers.
- **Lower IT Support Costs:** Automated workflows reduce manual IT workload.
- **Scalability for Growth:** Easily onboard and manage new employees across multiple locations.

08 Compliance & Reporting

- **Enforce Security & Compliance Policies:** Ensure devices comply with industry standards (e.g., GDPR, HIPAA, ISO 27001).
- **Real-Time Reporting & Analytics:** Get insights into device compliance, security risks, and app usage.

09 Secure Identity and Access Management (IAM)

- **Single Sign-On (SSO):** Employees can access multiple applications (Microsoft 365, SaaS apps, custom apps) with a single login.
- **Multi-Factor Authentication (MFA):** Reduces the risk of account compromise by requiring additional authentication factors.
- **Conditional Access Policies:** Control access based on user location, device health, or risk level.

10 Enhanced Security for Remote Work

- **Zero Trust Security Model:** Verifies users explicitly before granting access.
- **Privileged Identity Management (PIM):** Reduces the risk of privilege misuse by enforcing just-in-time access.
- **Identity Protection:** Uses AI to detect suspicious login behavior and automate risk-based access decisions.

11 Seamless Integration with Cloud Apps

- **Microsoft 365 & Azure Integration:** Essential if your business relies on Microsoft services.
- **SaaS App Support:** Works with thousands of third-party apps like Google Workspace, Salesforce, and Slack.
- **Custom App Support:** Allows authentication into both internal and customer-facing applications.

12 Remote Workforce Productivity

- **Self-Service Password Reset:** Reduces IT support requests.
- **Adaptive Access:** Employees can work securely from anywhere, with automated risk-based authentication adjustments.
- **Cross-Platform Access:** Works on Windows, Mac, iOS, and Android.

13 Cost Savings & Scalability

- **Eliminates On-Premises Infrastructure:** No need for physical servers or VPNs for authentication.
- **Scales with Business Growth:** Easily add new employees or contractors with role-based access controls (RBAC).
- **Reduces IT Overhead:** Automates user provisioning and de-provisioning.

14 Compliance & Regulatory Support

- **Audit Logs & Monitoring:** Tracks login attempts, access changes, and security incidents.
- **Compliance Standards:** Supports regulations like GDPR, HIPAA, ISO 27001, and SOC 2.
- **Data Loss Prevention (DLP):** Helps protect sensitive data in cloud environments.

15 B2B & B2C Identity Management

- **External User Access:** Securely collaborate with partners and contractors using guest access.
- **Customer Identity Management:** Handles authentication for public-facing apps with social login options.

The Take-Away

If your modern business relies on Cloud services, includes some remote employees and needs a secure, scalable way to manage user and device access, **AndroForge™** is for you. It enhances security and IT efficiency, simplifies access and device management over a variety of operating system platforms, and integrates seamlessly with modern business applications.