Microsoft Endpoint Manager

Flexible mobile device and app management that let employees work the way they choose.

Modern workplace demands a new approach to management and security, and more alignment across productivity tools. End users now have the flexibility to work from anywhere on any device, and IT is still responsible for security of all corporate data, wherever it lives. Only Microsoft provides the most complete and most secure device management for the modern workplace and helps organizations realize fastest time to value from their Microsoft 365 investment. Microsoft Endpoint Manager is the industry-leading solution that enables users and protects data across mobile devices, PC desktops and mobile applications.

- Microsoft provides the best platform to manage Windows as a service for IT organizations, and to help realize the promise of cloud-based endpoint management
- Extends the value of existing management infrastructure by attaching the power of Microsoft 365 cloud for automation and intelligent security insights
- Ensures security and compliance at all levels, starting with the device itself, and responds in real-time to the ever- changing threat landscape with integrations between Microsoft Endpoint Manager, Azure Active Directory and Microsoft Threat Protection

How Aruba ClearPass Policy Manager integrates with Microsoft Endpoint Manager for collaborative network access control at the device level

What about those other devices, sitting on the same network, right next to the Microsoft Endpoint Manager managed client? Introducing Aruba ClearPass. When integrated with Microsoft Endpoint Manager, ClearPass incorporates Microsoft Endpoint Manager's endpoint derived content for device level scrutiny before trust or access are applied. A known "dirty" device or a device that is outside of corporate policy compliance can now safely be remediated or handled, even before it attempts to login with potentially falsified credentials or a spoofed account.

CUSTOMER BENEFITS

- Device Level Scrutiny - ClearPass uses Microsoft Endpoint Manager supplied device-level context to make network and application level access authorizations.
- Stops Bad Actors Fast – If not trusted at the device level, ClearPass can deny access, or provision with a custom policy to protect the other users and devices on the network.
- Industry-adopted authentication, authorization, directory resources, and certificate management services across any wireless or wired deployed network infrastructure.

Learn More

Case Study

https://www.arubanetworks.com/en-in/resources/ust-global/

Contact

https://www.arubanetworks.com/me/company/contact-us/contact-us-form/

The Microsoft Intelligent Security Association (MISA) is an ecosystem of independent software vendors that have integrated their security solutions with Microsoft to better defend against a world of increasingly sophisticated, fast-moving threats.

aka.ms/MISA

Member of Microsoft Intelligent Security Association

Microsoft