The Deepest Level of Visibility and Control for Enterprise iOS Devices

Securing enterprise mobile users anywhere

From the beginning, Apple designed iOS to be simple, intuitive, and powerful, with security built into its core. Through a combination of device encryption, privacy controls, and other security features, iOS provides the most secure and private mobile experience for businesses.

Securing devices is not the only concern—users also face a tremendous amount of risk on a daily basis. For example, how do you prevent users from clicking on phishing links in text messages and ending up on bad sites? Are users accessing enterprise data using the proper apps? Businesses need to protect users at all times and require visibility into what is happening on the devices from a risk and compliance perspective.

Apple and Cisco are partnering to deliver the deepest level of visibility and control for enterprise-owned iOS devices—enabling businesses to expand iOS adoption in new ways and helping to remove potential roadblocks due to security and audit concerns.

Benefits

- Single app to deploy
- Avoid impact to employees' mobile experience
- More easily meet compliance with improved visibility
- Protect users anywhere they travel

Use cases

Visibility

When investigating security events, businesses need complete visibility across all devices to understand what happened and determine the scope of the incident. Cisco Security Connector provides visibility into all traffic generated by the user, applications, and device. This allows enterprise teams to ensure iOS devices remain secure and compliant.

Control

Imagine an employee mistypes a domain and browses to “linkedim.com,” which has been set up as a phishing site. Or imagine the potential impact if a user clicks on a malicious link in a text message. Businesses need to protect mobile users from accidentally going to malicious sites where they could inadvertently enter sensitive information. Cisco Security Connector prevents users from connecting to malicious destinations at the earliest point, whether it’s through a DNS or IP address request, and provides protection over Wi-Fi and cellular connections.

For more information

Please visit https://www.cisco.com/go/security and https://www.cisco.com/go/apple for more information.

Cisco Security Connector solution overview

For the first time ever, businesses can gain visibility into network traffic on supervised iOS devices and block mobile connections to malicious sites—anytime, anywhere.

Cisco Security Connector is deployed via a Mobile Device Management (MDM) platform such as Cisco Meraki™ Systems Manager, IBM MaaS360 with Watson Unified Endpoint Management (UEM), VMware Workspace ONE Unified Enterprise Management (UEM) (previously AirWatch), and MobileIron on-premises Enterprise Mobility Management (EMM).

With the Cisco Security Connector, you gain the following:

- **Visibility:** Help ensure compliance of mobile users during incident investigations by rapidly identifying what happened, whom it affected, and the risk exposure.
- **Control:** Protect users from connecting to malicious sites on the Internet, both at a Domain Name System (DNS) and IP address level—whether on the corporate network, on public Wi-Fi, or on cellular networks.

Why Apple and Cisco are partnering

Apple and Cisco are accelerating digital transformation and providing the deepest level of visibility and control on iOS devices.

C45-741111-01 10/18