Endpoint Management

Overview

Endpoint management is an industry term for the practice of providing a secure and stable environment for a community of connected devices including computers, tablets, and phones. A key goal of endpoint management is to ensure those endpoint devices are secure and protected from exploitation. Franklin OIT leverages two key tools to facilitate endpoint management for college-supported endpoint devices: Ivanti LANDesk and JAMF. Information about these tools, along with frequently asked questions, is published on the following pages:

- Ivanti (LANDesk)
- JAMF FAQ

Why is endpoint management necessary?

Franklin OIT works in concert with EITS to provide security on our networks, and we have different roles but the same goal: to protect data available through the endpoints associated with our clients.

EITS’ role

EITS uses tools that monitor the network for bad actors who have successfully attacked a computer on the network and will inform Franklin OIT if the endpoint is in our area or range of the network. Repairing compromised devices after they are exploited is considered a reactive approach to maintaining endpoint security.

EITS also proactively monitors the network for known vulnerabilities. This means that an endpoint may not have been compromised yet, but it is susceptible to attack because either the version of the operating system or the version of an installed software package is vulnerable to attack. It’s important to proactively patch, or update to a newer version of software when available to maintain a secure environment. Patching the vulnerability secures the endpoint and effectively remediates the threat.

Franklin OIT’s role

Franklin OIT takes a proactive role in Endpoint Management. We use several tools which allow us to maintain an inventory of computer endpoints, along with installed software, to identify vulnerabilities and track our progress in patching them. We use tools that automatically update computer operating systems and application software to newer, more secure versions. If there is a particularly nefarious vulnerability, referred to as a zero-day, we can look at the inventory to see what endpoints are affected and target them for upgrades. This is why we use tools like Ivanti and JAMF to keep inventories of computers and installed software versions. These tools gather specific and limited information used to inform Franklin OIT’s endpoint security strategy and allow us to rapidly respond to security threats by targeting affected endpoints in our inventory.

What are Ivanti and JAMF?

Collectively, Ivanti and JAMF are Endpoint Management Tools that help a large organization like the Franklin College of Arts and Sciences manage many thousands of endpoints. We talked about how these tools help us keep our devices secure through regular patching above, but they also help us manage settings and preferences to ensure compliance with the strict security requirements needed in an enterprise environment – one where many computers and associated devices share a common network. Although your computer may not contain sensitive or restricted data, if left unmanaged, it could provide an entry point on the network to other systems that do have sensitive or restricted data.

Additional information and responses to frequently asked questions about each tool is available here:

- Ivanti (LANDesk)
- JAMF FAQ

How does endpoint management help me?

Some features and preferences of modern computer operating systems that are useful in the home environment are not suitable for the enterprise environment where many devices interact. These computer use policies are set by USG, EITS and Franklin OIT and are designed to keep the institution’s data and networks safe. Franklin OIT uses endpoint management tools to adhere to these policies and configure computers to meet those standards. Achieving a reasonable security balance requires sacrificing some level of convenience, but Franklin OIT always strives to balance this tradeoff to achieve the highest level of security while maintaining the highest level of convenience.

External Resources

- USG IT Handbook
- EITS IT Policies, Standards, and Guidelines