Enterprise Computer Protection and Threat Response
Stop cyberattacks before they happen

Overview

Enterprise computer protection and threat response—also known as endpoint detection and response—monitors, detects and responds to security threats across the network. It will help FSU better prevent, detect, investigate and respond to advanced threats.

Requirement

All FSU-owned desktops and laptops must run the enterprise computer protection threat response service provided by Information Technology Services (ITS). Systems not compliant with this requirement create an undue risk to the university and may be removed from the network.

Why the change?

Enterprise computer protection and threat response is a cybersecurity best practice that is required to renew the university's cyber insurance policy. The new defense suite will strengthen the overall security posture of FSU.

What does it do?

- Stops attacks before they happen
- Protects against malware, ransomware, cryptoware and includes vulnerability scanning
- Increases awareness of technology risks threatening FSU devices
- Improves ability to work with departments and individuals to mitigate risks
- Works on various operating systems including macOS, Linux and Windows 10 and 11
- Creates no adverse effects to computer performance

What do I do?

Personally-Managed Devices

For desktops and laptops that are not managed by ITS, please submit a case to ITS so we can work with you to configure your devices. fla.st/WJIDZA1L

ITS-Managed Devices

No action needed. ITS automatically configures computer protection and threat response on these devices.

More Information

fla.st/CMDOFZ7X

security@fsu.edu

FLORIDA STATE UNIVERSITY
INFORMATION TECHNOLOGY SERVICES