CrowdStrike: Modern antivirus and Endpoint Protection Software

CrowdStrike is an endpoint protection platform available to all University units. Endpoint protection is an enhanced version of antivirus software that includes additional features to address more sophisticated security threats.

During a period when faculty and staff are working remotely more often and do not routinely join the University network, it is more difficult to protect the University's devices. Attacks and vulnerabilities may happen at home, while traveling, or when a family member shares a computer. The capabilities of this CrowdStrike tool provide the University with another way to protect our community regardless of their location.

CrowdStrike is provided as a platform and service to the University, managed by IT Services. Individual unit IT partners each have their own cloud dashboard to manage CrowdStrike deployments for the devices they support. Each unit has access only to its devices and servers. The tiered architecture of the platform allows IT partners to see and respond to their own security issues while allowing IT Services Information Security the ability to detect and respond to threats across the University. (CrowdStrike is included the in the IT Allocation.)

Service features include:

- Support for modern Windows, Mac, and Linux operating systems
- A secure cloud dashboard that allows for easy management
- Contractual protections allowing CrowdStrike to be installed in environments with sensitive data, such as health information
- Protection against malware, ransomware, viruses, and other types of malicious software
- Coverage of gaps left by legacy antivirus
- Analysis of device file and network activity, without reading file or network content
- On-call expertise to proactively identify the most sophisticated types of attacks
- Ability to block malicious activity and alert on suspicious activity

To request this service: Contact unit IT staff.

Questions? See the CrowdStrike service FAQ