Image not found
https://it.ucsf.edu/sites/it.ucsf.edu/themes/custom/it_new/logo.png
it.ucsf.edu
Published on *it.ucsf.edu* (https://it.ucsf.edu)

Home > Endpoint Protection (Client Security)

Endpoint Protection (Client Security)

Sarah Mays on January 27, 2020

Client security applications, often referred to as "endpoint protection clients," are a crucial part of the defense of your computer system from malicious attacks and other security risks. Endpoint protection consists of anti-virus, anti-spyware, intrusion prevention, and client firewall. These components are the most important things to have installed in order to keep your computer safe.

Viruses, worms, and spyware can be transmitted via email, downloaded from websites, and even transferred from removable media suchs as cd's, disks, and thumbdrives. Since it has become increasingly difficult to know when one will be encountered, it is important that every computer connected to or participating in the UCSF network run an automatically updating anti-virus software package to help protect against these potential risks.
Anti-virus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account. Anti-spyware software prevents the installation of software that can be used to monitor or control your computer use to send you unwanted pop-up ads, redirect your computer to websites, monitor your internet usage, or even record your keystrokes. All of which could be used to theft of your personal and professional information.
A computer may be infected with viruses and/or spyware if your computer exhibits:

- slow downs, malfunctions, or displays repeated error messages
- won't shutdown or restart properly
- displays a lot of unwanted pop-up ads, or displays them even when you're not surfing the web
- displays web pages or programs you did not initiate
- sends e-mails you didn't write

Installing and maintaining client security applications on your computer can help protect your data and system from being compromised. UCSF policy requires that computers connect to, or participating in, the UCSF network have current anti-virus software installed, running, and updated on a regular basis. This will help ensure the UCSF network remains a stable and secure environment.

Symantec Endpoint Protection (SEP) for Windows computers

Symantec Endpoint Protection (SEP) is designed to detect, remove, and prevent the spread of viruses, spyware, and other security risks. The SEP client combines various client security technologies under a single application to help protect your computer without sacrificing performance. It provides your Windows computers anti-virus (AV), anti-spyware, intrusion prevention (IPS), proactive threat scanning, and personal firewall. SEP scans local hard disks, monitors file access, and monitors network traffic to detect potential threats and blocks any necessary access until the threat has been resolved.

In addition, the UCSF SEP client will automatically keep both the client software and security definitions (anti-virus and IPS) updated for the most complete protection.
SEP can be downloaded from the UCSF Customer Support Software Download site.
http://software.ucsf.edu/applications/sep.html [1]
[2]Additional help on Symantec Endpoint Protection can be found on our SEP Documentation page.

Symantec Endpoint Protection (SEP) for Mac OS X Intel computers

Symantec Endpoint Protection (SEP) is designed to detect, remove, and prevent the spread of viruses, spyware, and other security risks. The SEP client provides your Macintosh computers anti-virus (AV) and anti-spyware protection, intrusion prevention (IPS). SEP automatically scans local hard disks and monitors file access to detect the telltale signs of the presence of a virus and will warn the user and block access to the file until it can be cleaned.
In addition, the UCSF SEP client will automatically keep both the client software and security definitions updated for the most complete protection.
SEP for Mac can be downloaded from the UCSF Customer Support Software Download site.
http://software.ucsf.edu/applications/sep.html [1]
[2]Additional help on Symantec Endpoint Protection can be found on our SEP Documentation page.

Required Service Information

Symantec Endpoint Protection (SEP) [3]

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

Source URL: https://it.ucsf.edu/services/symantec-endpoint-protection-sep/additional/endpoint-protection-client-security

Links
[1] http://software.ucsf.edu/applications/sep.html
[2] http://software.ucsf.edu/sep
[3] https://it.ucsf.edu/services/symantec-endpoint-protection-sep