Stand Strong Against Malware Threats

Join forces with CloudConnexions and secure your business with cutting edge malware defense.

Malware is involved in the majority of successful cyberattacks carried out today. It comes in many forms and can enter your network through force, deception, or a simple act of human error. Without a solid malware protection plan in place, it's only a matter of time before your organization is affected.

The Scourge of Malware

Hackers love malware for good reason. It's a simple, cheap, and readily-available way to initiate an attack. Moreover, malware is effective -- simply because it can be hidden nearly anywhere.

Malicious code can be delivered via all kinds of files, including videos, pictures, and applications. When someone opens or runs such a file, the malware hidden within is set into action.

Threat actors often create websites (or hijack legitimate websites) to set a malware trap for unsuspecting internet users. A website that is infected with malware can automatically download and install harmful files on a workstation or mobile device without your knowledge.

More often, malware is spread through email attachments. Someone on your network need only open an email attachment that is infected with malware to start a destructive chain of events that can lead to downtime, lost data, or worse.

Modern Malware Protection from CloudConnexions

Many years ago, malware could be readily avoided using simple signature detection techniques that were built into most antivirus or antimalware tools. These tools would simply look for known malware code and block or remove the suspicious files.

These days, malware and ransomware mutate and adapt too quickly for signature detection to offer reasonable protection. While the old methods can usually stop known threats, it's the constant influx of unknown malware that poses a problem.

This is why CloudConnexions uses advanced anti-malware tools to protect you and your data. Our solutions use predictive technology and cutting-edge behavioral analysis to identify suspicious code or application activity that could signal a malware intrusion. Our security experts can then evaluate the suspicious file(s) in quarantine, before it has a chance to impact your systems.

In the unlikely event malware does infiltrate your network or devices, our security team will respond quickly to counter the threat, minimize the spread, and remediate any damages.

Common Types of Malware

- Viruses - A specific type of malware that can spread between machines
- Ransomware - installs itself onto a victim's machine, encrypts their files, and then demands a ransom to return that data or unlock their machines
- Worms - Copy themselves from machine to machine, usually by exploiting a software security vulnerability
- Spyware - Captures and transmits personal information or use behavior
- Trojans - Malware disguised as legitimate applications
- Fileless malware - Challenging to detect because it does not rely on files and leaves no footprint