BEST PRACTICES:

THREAT PREVENTION Basics

jamf

What do bicycles, a statue of a horse, helicopters, and an eyebrowless portrait of a woman have in common? Leonardo da Vinci, of course! This quintessential Renaissance polymath created some version of these items, requiring him to have a hand in painting, sculpting, mathematics, physics, engineering and more.

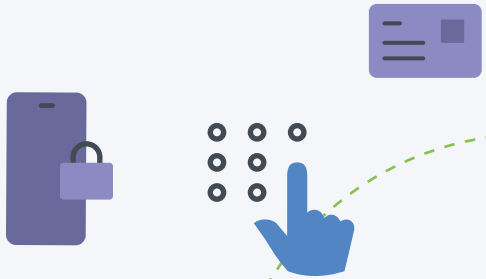
For organizations with limited resources, it can feel like you have to be the “Renaissance man” of your company: executive, manager, IT professional, accountant and so on. At Jamf, we can’t do your taxes, but we can help you learn the high-level aspects of threat prevention as well as what you need to keep in mind for best practices when assessing your threat prevention strategy.

What is threat prevention?

Threats come from a variety of sources and methods. They can look like an attachment in an email, a text or call to log in to your bank account, websites that look *almost* familiar or like nothing at all, like in the case of devices running outdated software with security vulnerabilities.

Threat prevention works behind the scenes to:

- Protect from known ransomware, trojans and other malware
- Use artificial intelligence to identify unknown threats
- Alert you of suspicious activity
- Block phishing attacks and malicious websites
- Monitor and log the health of your devices



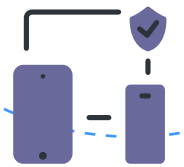
Does my organization need threat prevention?

Short answer: yes! It's true. Regardless of the size of your organization—if you have company data, it needs to be protected. Your organization *will eventually* be the victim of cybersecurity exploitation, at least targeted, so it's important to reduce the risk of this happening and the impact an attack would leave on your organization.

Getting started with threat prevention

Preventing threats means protecting your devices and your network. A great place to start is **ensuring your devices are up to date**—outdated operating systems and applications with unpatched vulnerabilities make it that much easier for bad actors to get into your systems.

Implementing an antivirus and endpoint detection and remediation (EDR) tool further enhances your security posture. Antivirus works in the background to **identify known threats** by recognizing suspicious activity, information in files that indicates malware, malicious websites and IP addresses, and more. EDR goes beyond this by **using artificial intelligence (AI) and machine learning (ML) to identify threats** that are not well known—cyber attacks are evolving into more sophisticated and complex threats each day, so comparing to a database of known threats isn't enough.



Maybe this sounds like too much to tackle—we're here to offer you a solution. Jamf offers device management solutions to keep your devices up to date while giving you transparency into their compliance with security policies. And our security software defends your devices from known and unknown threats without burdening the user. Whether you have Jamf for your management or security solutions, keep these best practices in mind:

1. Require devices and software to run the most up-to-date operating systems (OSs) and that apps are managed, verified and updated.

2. Don't simply rely on the most secure out-of-box hardware. Protect your Apple fleet and users with an Apple-focused endpoint protection solution.

3. Let technology work *for* you, and incorporate AI and ML into your security strategy with EDR.

Want to learn more? Our Threat Prevention for Beginners e-book takes a deeper dive into threat prevention tactics and solutions.

Or if you're ready, you can give our software a try.

jamf

www.jamf.com

© 2002–2023 Jamf, LLC. All rights reserved.