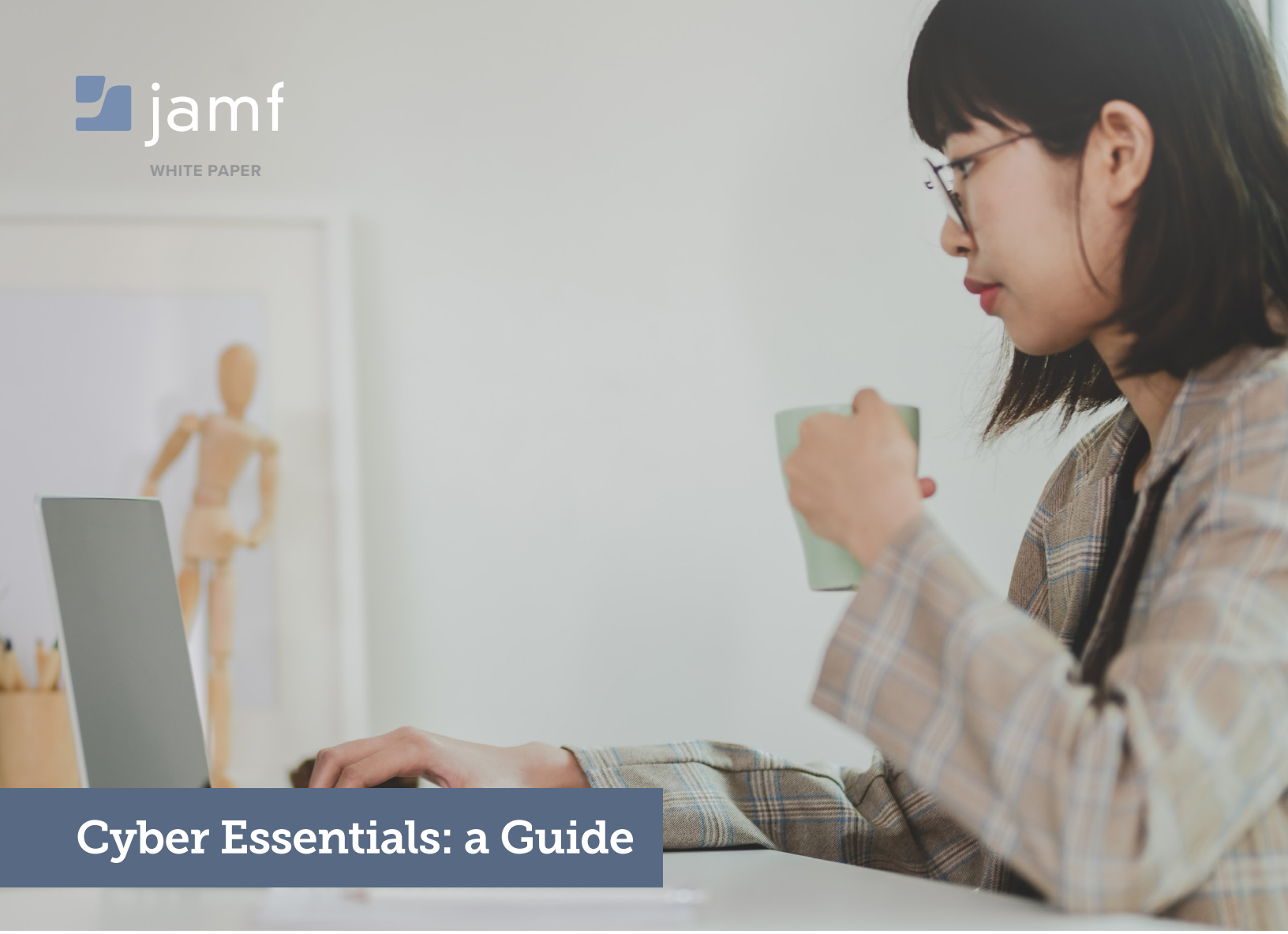
jamf

WHITE PAPER



Cyber Essentials: a Guide

Company and user data is constantly at risk of cyberattacks. This guide from Jamf — the Apple management experts — will show you how to protect your organisation against the most common cyberattacks.

To see more about Jamf Pro's security features and recommendations, visit:
www.jamf/com/security

Why is Cyber security important?

Security of company data and devices is receiving more and more attention, given the growing number and severity of security threats. When it comes to cyber security, we believe a company is only ever as good as its software. Breaches and security vulnerabilities can disrupt user privacy, sensitive company data, user experience and much more. A cyberattack of any kind is guaranteed to hit pause on business as usual until the breach is resolved. This means valuable time and resources are invested into fixing a security threat which was preventable in the first place. Ensuring company- and employee-owned devices and data is encrypted, compliant and stays private should therefore be a priority for IT.

Why should my organisation actively take measures to protect its cyber security?

The vast majority of cyberattacks are the equivalent of a thief simply trying your front door to see if it's open, and following a security plan helps to mitigate this risk. Adopting the recommendations in this guide can:

- Reassure clients and customers that your organisation is working to secure their technology infrastructure and their data against cyber attacks
- Attract new business who value organisations that take cyber security seriously
- Allow you to seek government contracts requiring cyber security certifications
- Build a relationship with a trusted IT supplier

What attacks can we prevent?

Your security plan should address the most common internet-based threats to cyber security: particularly attacks that use widely available tools and demand little skill. You should work to prevent:

- Hacking: exploiting known vulnerabilities in internet-connected devices, using widely available tools and techniques
- Phishing: attempting to trick users into installing or executing a malicious application through email or other means
- Password-guessing: manual or automated attempts to log onto a system from the internet by cracking passwords

How can Jamf help?

Whatever your level of participation in best practice guidelines for security, Jamf can help. Jamf Pro and Jamf Connect have existing built-in functionality that will achieve most, if not all, best practice guidelines.

If you're new to Apple security and just want the basics, please see our e-book **Apple Device Security for Beginners**.

Requirement #1: Firewalls

Ensure that only safe and necessary network services can be accessed from the internet.

Organisations should routinely:

- Change passwords to difficult-to-guess, complex passwords
- Prevent access to the administrative interface from the internet, unless the interface is protected by one of the following controls:
  - A second authentication factor, such as a one-time token
  - An IP whitelist that limits access to a small range of trusted addresses
- Block unauthenticated inbound connections by default
- Ensure inbound firewall rules are approved and documented by an authorised individual
- Remove or disable permissive firewall rules quickly
- Use a host-based firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

Implement firewall best practices with Jamf

We've got you covered! Jamf Pro offers settings that accomplish these best practices in the security and privacy payload of a Jamf Pro configuration profile, which is pushed out to all managed Macs:

- Enable Firewall
- Block all incoming connections such as file sharing, screen sharing, Messages Bonjour and iTunes music sharing
- Control incoming connections through the Connection Setting dropdown for specific apps — requiring app name, bundle ID and connection setting before allowing the app
- Enable stealth mode: ignore attempts to access the computer from the network by test applications using ICMP, such as Ping
- Configure managed devices to automatically connect to a VPN when conditions are met, offering more secure network access

And Jamf Connect offers simple provisioning of users from a cloud identity service during an Apple provisioning workflow, complete with multi-factor authentication.

For a deeper, more technical dive into information on the application firewall and configuring it with Jamf Pro, please take a look at these developer resources:

Apple's Developer Configuration Profile Reference, Firewall Payload

Apple KB - OS X: About the application firewall

Jamf Pro Administrator's Guide, Computer Configuration Profiles

jamf | CONNECT

You can see more details on Jamf Connect here:

https://www.jamf.com/resources/product-documentation/jamf-connect-transform-provisioning-and-identity-management/

Best Practice #2: Secure Configuration

Ensure that only safe and necessary network services can be accessed from the internet.

Computers and network devices best practices

Companies should routinely:

- Remove and disable unnecessary user accounts
- Change any default or guessable account passwords
- Remove or disable unnecessary software
- Disable any auto-run feature which allows file execution without user authorisation
- Authenticate users before allowing internet-based access to sensitive data

Implement computer and network best practices with Jamf

Jamf Pro can help administrators implement these best practices through configuration profiles, policies and scripts to disable, report or quickly remediate. For example:

- To ensure the guest user account is disabled permanently, a Jamf administrator may deploy a configuration profile with the login window payload to all managed devices.
- Using Smart Groups, administrators can disallow certain types of users with a scripted payload. Jamf Nation, the largest online community of Apple-focused admins and Jamf users, contains a wealth of information, sample scripts and user-led troubleshooting.
- Automated reports provide administrators information on local user accounts, if needed, and user-initiated enrolment settings can be set in Global Management or retroactively using the management accounts payload.
- Administrators may disable Bluetooth and restrict or disallow apps.
- When configuring enrolment settings, a Jamf administrator may enable randomised passwords or enforcement of complex passwords through the user-initiated enrolment option.

For more detailed information on administering account passwords with Jamf Pro, please see these technical resources:

Jamf Pro Administrator's Guide, Administering the Management Account

Jamf Pro Administrator's Guide, Administering Local Accounts

Jamf Pro Administrator's Guide, User-Initiated Enrolment Settings

Password-based authentication best practices

This best practice is meant to protect against brute-force password guessing by using at least one of the following methods:

- Lock accounts after too many attempts
- Limit the number of guesses allowed within a certain time frame
- Set requirements for password length and complexity
- Have a password policy that clearly explains to users strong and secure password practices

Implement password-based authentication best practices with Jamf

Jamf Pro offers the ability to set all of these preferences in a configuration profile. Jamf Pro administrators can also create password blacklists for common, easily guessed passwords. With Jamf Connect and Jamf Pro, users can take advantage of single sign-on and multi-factor authentication for even stronger password protections.

Local accounts with NoMAD or mobile accounts with Active Directory are also in luck: Jamf Connect works smoothly with NoMAD for an even more secure experience.

For information on how they work together, please see this infographic that lays it all out: **https://www.jamf.com/resources/infographics/understanding-macos-catalina-and-jamf-connect/**

Best Practice #3: User Access Control

Organisations should ensure that user accounts are assigned to authorised individuals only, and that applications, computers and networks are only accessible to users who actually need them.

This means organisations should:

- Have a user account creation and approval process
- Authenticate users before granting access to applications or devices
- Remove or disable user accounts when no longer required
- Use administrative accounts to perform administrative activities only
- Remove or disable special access privileges when no longer required

Implement access control best practices with Jamf

Jamf's available restrictions to the System Preferences through the configuration profile, restrictions payload or simple removal of administrative access when no longer needed will cover these issues, and the well-managed **Self Service** option ensures that no one has access to areas or apps that they don't need.

To remove users and accounts, administrators deploy a simple policy removing these accesses, accounts or users.

Best Practice #4: Malware Protection

Organisations should restrict execution of known malware and untrusted software to prevent harmful code from causing damage or accessing sensitive data.

Malware protection best practices

- Anti-virus and other security software must be kept up to date — automatically or in an established workflow at least daily
- The software must be configured to scan files and web pages automatically upon access
- The software must prevent connections to malicious websites on the internet
- Only approved applications are allowed on devices
- All code of unknown origin must be run within a 'sandbox' that prevents access to other resources unless permission is explicitly granted by the user

Implement malware best practices with Jamf

Jamf's security features are built in. With software deployment via a policy and automatic updates of all software, you can rest assured that all anti-virus and other security software is always up to date. If the anti-virus software your organisation uses does not automatically scan files upon access, a Jamf script or policy can get the job done. And, of course, all macOS devices already have Apple's built-in **XProtect**.

Additionally, with Jamf Pro's configuration profiles, administrators may set security and privacy payloads through gatekeeper settings, deploy certificate transparency payloads, restrict apps to a specific whitelist and more.

On top of Apple's built-in sandbox, disallowing apps from sharing key features, Jamf Cloud's servers also have a sandbox for greater security. And as if all of this weren't enough, administrators may add additional security features for protecting against malware through a personal privacy policy control configuration profile.

Best Practice #5: Patch Management

This best practice ensures that devices and software are not vulnerable to known security issues for which fixes are available.

Software should be:

- Kept up to date
- Licensed and supported
- Removed from devices when no longer supported
- Patched within 14 days of an update being released

Implement patch management best practices with Jamf

Administrators can use Jamf Pro's patch management feature to track and patch software on managed devices: patch management automatically patches software on managed devices after an administrator uploads a package, associates it with a patch version and creates a patch policy.

Jamf's patch server may provide software titles, or customers may wish to integrate an external patch source managed by themselves or a third party. Software title information includes supported OS versions.

Software can be easily uninstalled with a policy configured for uninstall or by removing the device from the scope of the Mac App Store record.

Conclusion

Jamf makes it easy to implement and follow best cyber security practices.

To put these security features to the test, request a **Free Product Trial**.