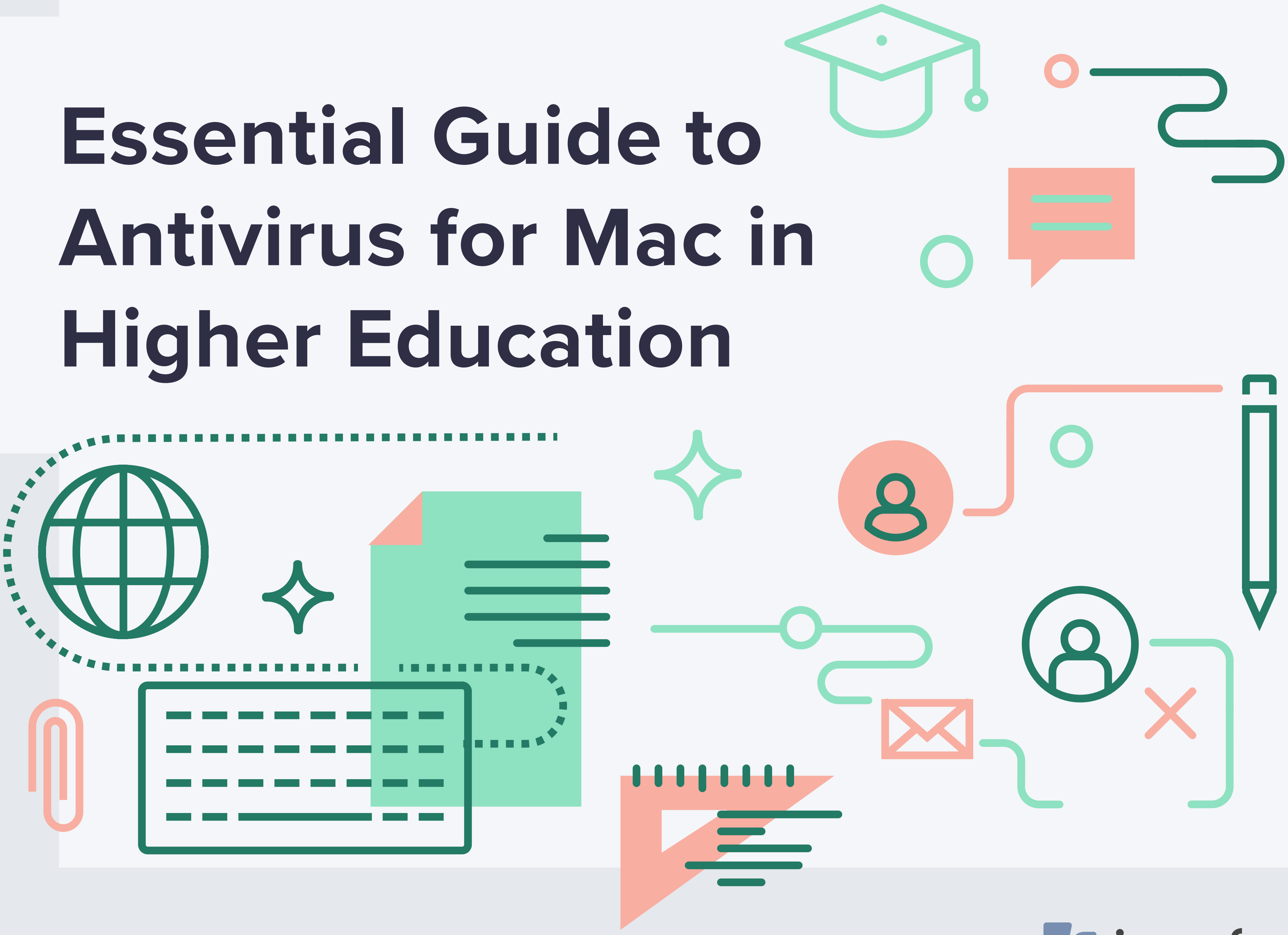
# Essential Guide to Antivirus for Mac in Higher Education



jamf

The state of malware for Apple devices has become a larger focus as the Apple ecosystem continues to find more footing within Higher Education.

Overall, Apple fares well considering that detections are on the rise across all computing platforms, while malware-specific detections appear to be in a lull compared to other, more targeted malware threat types.

Severe threats classified as malware — such as rootkits and ransomware — have decreased from prior years. Many of the larger frameworks of botnets have also fallen sharply despite several high-profile attacks last year. This is likely attributed to a shift in how devices are being used and where they're being used from. The global health crisis is the leading catalyst for this shift from corporate network environments, that are accessed locally by millions of users, to the work-from-home model that so many corporations have adopted in response.

In other words, the landscape has changed drastically. In response, malware authors and threat actors are adapting to these changes by modifying the scope and scale of the malware tools in their arsenal. By leveraging multiple threat types at once, attackers add complexity while increased reliance on automation allows targets to expand to include the collaboration tools that users are relying on to stay productive.

## In this e-book, we:

- Define Mac-focused antivirus (AV)
- Highlight how malware threats are increasingly affecting Mac users
- Explain why understanding these trends is so vital to securing private data
- Share what Jamf offers to ensure your Mac devices stay protected

# Mac-focused antivirus

Antivirus (AV) is a basic requirement for most institutional devices to provide baseline security. Apple includes a basic AV mechanism in macOS with XProtect, Gatekeeper and MRT. These tools, however, are sporadically updated, and organizations lack visibility into their actions. Institutions need sophisticated antivirus capabilities to prevent and quarantine Mac malware, far beyond what Windows-focused solutions are able to provide on macOS.

And they shouldn't wait until malware, adware or other unwanted software issues arise.

> They need to implement AV that effectively identifies and remediates Mac-specific attacks without spending precious resources looking for threats to Windows on a Mac. Effective, efficient and comprehensive Mac AV capabilities are essential to both security and device experience.

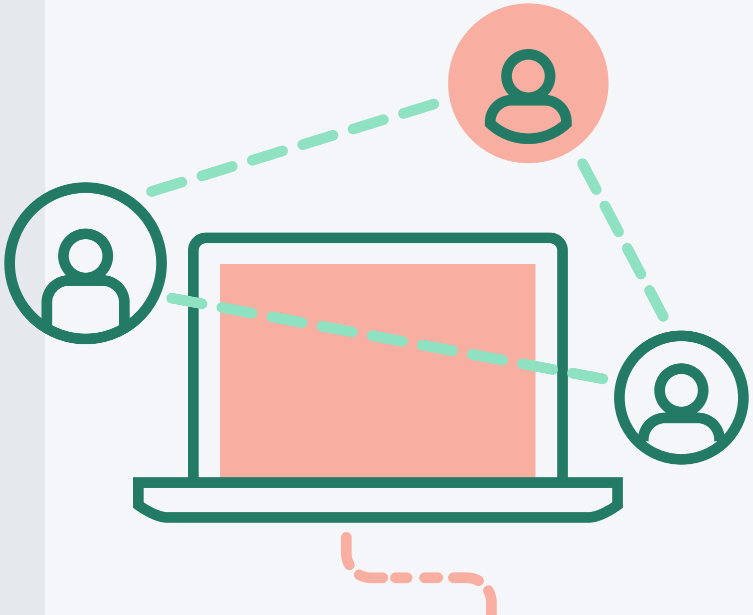
## A changing threat landscape

Taking the focus is a marked increase in phishing campaigns anchored around the crisis, feeding off the fears and concerns of individuals, particularly when it pertains to goods that have been in limited supply or affected by global shortages, including tech support scams. Coupled with this resurgence, a focal point for threat actors that has seen some of the largest gains in the wild is in the realm of information gathering.

## Online creeping

Adware, spyware, and a relative new kid on the block, stalkerware — are all types of malware used to obtain and exfiltrate data about computer users. The latter, stalkerware earned the nickname "online creeping" because it leverages all kinds of personally identifying data in real time.

**Examples like relaying GPS coordinates, decrypted message logging, and monitoring/recording phone calls are but a few of the many privacy concerns being violated, according to a report by Kaspersky Labs.**



# It’s chess, not checkers

When reviewing this information, it’s important to note that threat actors often play the long game, meaning that attack campaigns can last as long as they need to. They are not limited to getting a single piece of malware onto a device but may keep trying to gain access and leverage any existing footholds. This allows time to be on their side to make any changes necessary in their attack strategy or tools, gather as much intel as they would like, and ultimately allow any malware to embed itself more deeply into the affected systems.

It’s cyclical with each facet directly **impacting** and **feeding** the next.

# State of antivirus for Mac

Good news for Mac users is that overall malware detections on Mac devices, dropped by over 38% in 2020, according to a State of Malware Report for 2021 by Malwarebytes Labs.

Unfortunately, the education industry is often rated as the one of the least secure. This means universities must constantly work at advancing their security strategy and posture or risk succumbing to ever-evolving threats.

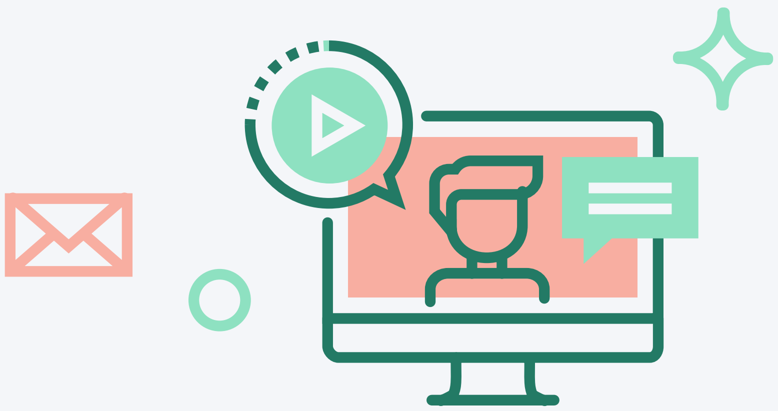
**Several factors affect this sea change, three main ones being:**

- Apple's continued market and Mac growth in higher education
- Users choosing Apple devices from student/faculty-choice programs or labs offering MacBook
- The global shift towards remote learning programs has expanded the demarcation line that used to divide the campus and home

# Don’t break out the party hats just yet

While the consumer users may see this downtick as a cause to celebrate, telemetry data collected from various sources indicate that devices used in the personal space are still subject to potentially unwanted programs (PUPs), with adware leading the charge.

This represents a different issue altogether than what is being seen on the education side, but for personal users of Mac products, PUPs and adware represent an attempt to target user’s personally identifiable information (PII) or a setup to something far worse down the road when malicious ads are delivered, private data is tracked or a sketchy app that claims it will clean your Mac is downloaded.



# Mix-and-match malware

One curious find that is sure to be just the tip of the iceberg centers around novel ways of implementing ransomware in attacks. While the last known novel ransomware targeting Mac was detected several years back, 2020 brought EvilQuest to the forefront (also known as ThiefQuest). This piece of malware has all the makings of ransomware except the encryption warnings and requesting for payment to decrypt files is merely subterfuge to mask its true intention: **persistent and targeted theft of personal and business data**.

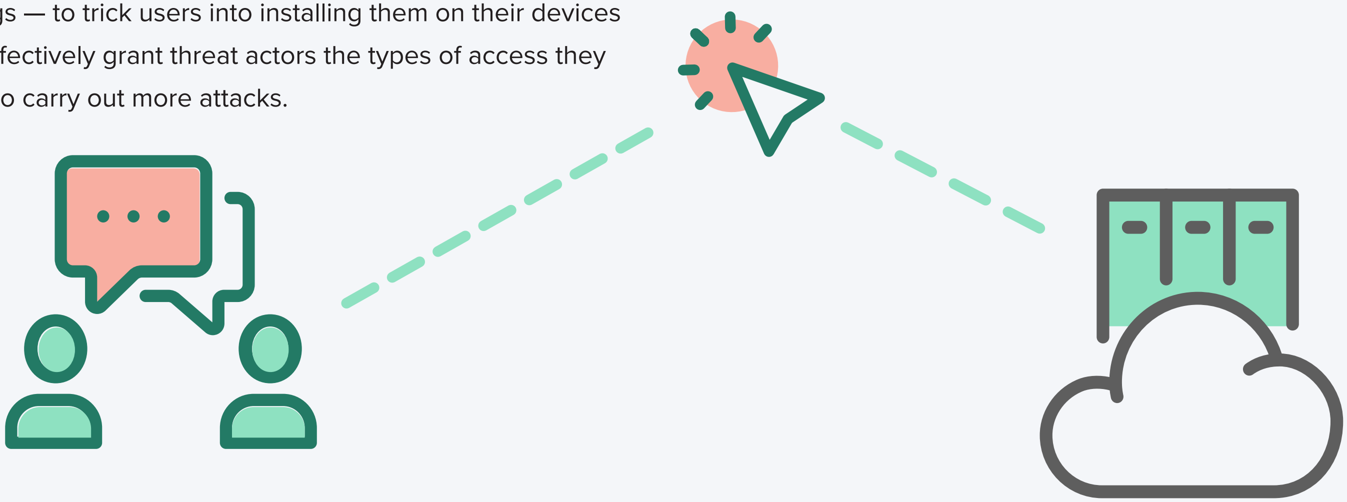
Malware such as this can evolve over time — just like regular software — to include additional features that cause more harm, while also increasing stealth to evade detection. It can even update itself to evolve after it has infected a device. EvilQuest has all the markings of being an ongoing story to watch for as it changes in the future.

# Old dogs *can* learn new tricks

Filed under the "annoying for now" category, adware-type malware is evolving as well. Given Apple's newer macOS releases that work to verify app signing before allowing apps to launch, some malware authors have gone to great lengths to think out of the box, so to speak, in order to gain access to the precious data on your system and to monetize the ads you see browsing the web.

Examples of these attack types can be duplicating the Safari app itself and modifying it by installing unauthorized extensions to track users. Or using configuration profiles — the same kind that are used by IT admins to manage device settings — to trick users into installing them on their devices and effectively grant threat actors the types of access they need to carry out more attacks.

It should also be noted that while adware is considered less dangerous, the combination of it being the most common malware threat among macOS while also showing the most advanced forms of innovation in how to infect systems — not to mention combined with the increasingly common ability to remotely add new malware payloads — makes it clear that adware could reach critical levels in its potential for destruction.



# Work smarter not harder

Unfortunately, there is no one solution that will resolve the escalating threats currently being faced. One of the key takeaways is that threats will not come from the same place each time. Threat actors are increasingly varying their tactics and target the devices and services that will yield the greatest results. One thing that the data asserts is that attackers are showing no signs of stopping.

What does this mean for everyone that relies on computers to live and work? In simple terms, security must be setup to defend, deflect, prevent or remediate any and all threats that come its way. Vigilance is an important part of the security equation, whether it stems from training users on how to spot common threat types, such as phishing attempts or not installing unknown software.

IT must also incorporate vigilant practices into its workflow to strengthen and uphold the security posture of the organization at all times. Reliance on detection software to locate threats based on known signatures or heuristics, which performs behavioral analytics to detect unknown threats before they happen helps provide IT with the insight necessary to understand where threats targeting their organization are not only coming from, but how to best protect against them.

Quick response and automation work hand in glove to respond to detected threats quickly while performing the heavy lifting to remediate any issues found is critical to be successful in this. Both help to minimize the attack surface and better manage risk efficiently while adding another layer to the defense in depth strategy.

After all, when we use Mac, it’s to get something done — probably not to scan through thousands of lines of application code looking for bugs in an app before we launch it, right? It’s in these moments that we remember that Apple strives to make its user experience exceptionally easy to navigate and to create something extraordinary. So, why shouldn’t security software follow those same guidelines?

# Jamf integration + support

Jamf Protect prevents malware and remediates malicious behavior through signature-based detection and behavioral analytics on Mac. With top-down, granular insight into devices IT departments can see what's affecting device performance from a security purview. Furthermore, when joined with Jamf Pro, centralized patch management and remediation are enabled to allow resolution of just about any issue that may arise. Lastly, pairing Jamf Pro and Jamf Protect along with Jamf Connect completes this highly secure trifecta by allowing for identity management by binding your Mac to institutional resources using cloud-based identity services for device and resource access — securing user's data by ensuring their devices are protected end-to-end.

A defense with an in-depth strategy that includes Apple's built-in tools and expands on them with the combined power of Jamf, will help you maintain effective Mac security that seamlessly integrates with the end-user experience while still providing all the relevant insight and analytics about their devices. This layered strategy allows IT to make the best decision where the protection of their devices and safeguarding of user's data is concerned.

> Jamf — the standard in Apple Enterprise Management — has the products and solutions that will help you enact the best security strategy for your institution and your users.

# Don’t just take our word for it.

Put AV and endpoint protection to the test.

When you’re ready to protect your Mac fleet against escalating security threats and known malware in the wild, and to remediate malicious behavior, request a free trial or contact your preferred Apple reseller.

jamf

Learn more about Jamf Protect and Mac endpoint protection on jamf.com

Request Trial

Or contact your preferred reseller of Apple hardware.