

Topics

1. What Is Endpoint Detection and Response (EDR)?
2. What Is the Difference Between EDR vs. MDR?
3. What Are the Key Benefits of Managed EDR for a Business?
4. How to Evaluate and Choose a Managed EDR Provider for Your Business
5. Essential EDR Features: What to Look for in a Solution
6. What is Endpoint Security?
7. What is Managed EDR? Why Your Business Needs It
8. EDR vs. Antivirus: What's the Difference?
9. Essential EDR Features: What to Look for in a Solution
10. Top Managed EDR Solutions
11. Endpoint Security for Linux: What You Need to Know
12. **Endpoint Security for Mac: What You Need to Know**
13. What is Mobile Endpoint Security?

You heard it here: Macs aren't immune anymore

What is endpoint security for Mac?

Which security software is best for Mac?

Does Defender for Endpoint work on Mac?

XProtect: Apple's built-in perimeter wall

Some Mac security strategies that actually work

Structural stress points: The enterprise Mac security dilemma

Cracks in the foundation: Future threats to Mac security

Huntress is your blueprint for Mac endpoint protection

Endpoint Security for Mac: What You Need to Know

Published: May 23, 2025

By:  **Brenda Buckman**

Key Takeaways:

- Mac malware is on the rise, but antivirus software is insufficient on its own.
- Strong Mac endpoint security needs layered defenses with real-time threat detection and behavioral monitoring.
- Use tailored, multi-layered solutions, like Microsoft Defender for Endpoint and Huntress Managed EDR, to fit your organization's risk and compliance needs.

Macs are no longer the untouchable strongholds they once seemed. [Endpoint security for Mac](#) has become a key focus in the blueprints of modern enterprise security architecture. While [antivirus](#) is a necessary foundation, it's no longer enough to support the entire structure. They're like a beautiful façade on a house built in an earthquake zone. They look secure, but the fault lines are shifting.

Security pros now need to reinforce every Mac like a house in an earthquake zone—tested, hardened, and stress-proofed for today's seismic threats. Malware designed to target Mac devices is becoming more advanced and threatening. In fact, [macOS infostealer detection surged by 101% between the last two quarters of 2024](#). There's no doubt that it's time to confront the reality head-on and rethink how Macs fit into your security strategy.

[Try Huntress for Free](#)

[Get a Free Demo](#)

You heard it here: Macs aren't immune anymore

The tough reality many organizations face is that the long-held myth that Macs are invincible has created serious blind spots in corporate security blueprints.

Primary risks targeting macOS:

- ✓ Malware specifically designed for macOS, including sophisticated adware and advanced spyware
- ✓ Social engineering campaigns that exploit user trust in Apple's perceived polished reputation
- ✓ Info-stealers that silently harvest credentials and sensitive data
- ✓ Supply chain attacks targeting Mac-specific software builds and update channels

Think of it this way: Cybercriminals used to walk past the Mac house on the block because it looked secure and didn't have much inside. Now that enterprises have moved valuable assets into those homes, attackers have adapted and learned how to bypass the alarm system.

This shift means you can't rely on Apple's default defenses, and you need a new strategy to secure every corner of your Mac environment.

What is endpoint security for Mac?

[Endpoint security](#) for Mac is the full architectural plan for protecting Mac devices.

Modern Mac endpoint security includes:

- ✓ Real-time threat detection
- ✓ Behavioral analytics
- ✓ Automated incident response
- ✓ Vulnerability management

You can't put all your faith in signature-based AV tools. Today's solutions use advanced behavioral analytics and real-time monitoring to spot suspicious activity.

Which security software is best for Mac?

When choosing the best antivirus for Mac, you need to understand that traditional antivirus alone isn't enough. Today, the best solutions combine an endpoint protection platform ([EPP](#)) and endpoint detection and response ([EDR](#)). These solutions give you real-time behavioral [monitoring](#), forensic tools, cross-platform threat visibility, incident response, and system and network activity insights.

But the best solution? It's the one built to your specs. A high-security Swiss bank vault needs different materials than an artist's loft. So, whether you're managing 1,000 Mac endpoints or just five, your protection strategy should reflect your risk model and compliance needs.

Does Defender for Endpoint work on Mac?

Yep, Microsoft Defender for Endpoint supports macOS. This is a big deal because it signals a shift in how cross-platform security is wired into enterprise environments. It brings enterprise-grade detection, auto-investigation, and response tools tailored for the Mac wing of your estate.

But here's the rub: Even with a strong solution like Microsoft's, relying solely on EDR means you still need to manage it yourself, hire macOS threat experts, and monitor around the clock. That's just not sustainable for most organizations. The most effective Mac endpoint protection strategies combine multiple complementary technologies and expert-managed support for continuous, layered defense. [Huntress Managed EDR for macOS gives you those layers.](#)

XProtect: Apple's built-in perimeter wall

Apple's XProtect is always running quietly in the background with no switches to flip or toggles to set. It checks files as they're downloaded, opened, or modified using a combination of malware definitions, system heuristics, and other built-in protections.

To support overall macOS security:

- ✓ Keep macOS fully updated so all security components work properly
- ✓ Allow Apple's background security updates to stay current with the latest protections
- ✓ Use XProtect as part of a broader layered strategy and not your only line of defense, but depending only on XProtect is not enough.

Some Mac security strategies that actually work

Treat Mac security like maintaining a historic building. The structure might be solid, but you still need to retrofit it to withstand today's environmental pressures. Apple gives you great bones, but it's on you to bring in the right contractors and tools.

Core elements of Mac security

- ✓ We repeat—enable automatic security updates for macOS.
- ✓ Enforce least privilege access.
- ✓ Monitor logs and network traffic for anomalies.
- ✓ Deploy comprehensive [EDR solutions](#) like [Huntress Managed EDR](#).
- ✓ Conduct [regular security assessments](#) and pen tests.

Structural stress points: The enterprise Mac security dilemma

When you're managing an office tower (your business), and not a single-family home (your personal laptop), security complexity grows fast. Businesses deploying Macs at scale face challenges most people never encounter:

- ✓ Diverse configurations
- ✓ Policy compliance
- ✓ Cross-platform integration with Windows tools
- ✓ Ensuring Macs don't become the weakest floor in your office tower

For this, you need to rely on Mac-specific engineers with purpose-built solutions to tie your security architecture together, 'cause [Macs need security](#), too.

Cracks in the foundation: Future threats to Mac security

Attackers are evolving. Fast. Think about these:

- ✓ [APT](#) groups, like North Korea's state-sponsored [Lazarus Group](#), are now building Mac-specific toolkits
- ✓ Social engineering campaigns exploit Apple's safe brand perception
- ✓ Supply chain attacks target Mac software distribution channels, like the [3CX desktop app attack](#) that reached thousands of victims at once

The Mac security stack is being tested in real time, and only layered, resilient designs will hold.

Huntress is your blueprint for Mac endpoint protection

Comprehensive Mac endpoint protection means you're not just leaning on Apple's design but strengthening it with steel reinforcements. You need enhanced visibility, intelligent threat detection, and rapid response systems that are beyond default settings.

This doesn't mean replacing Apple's protections. It means augmenting them. With [Huntress Managed EDR](#), you get that full suite, enterprise-grade protection tailored for macOS but

designed to protect every wing of your infrastructure. See how Huntress helps secure [macOS environments with purpose-built endpoint detection and response](#).

The stakes are high, and Macs are no longer side players. They're central fixtures in enterprise infrastructure, and if they aren't secured with the same intensity as Windows systems, you're building on sand. [Book a demo](#) with Huntress to secure your foundation before the cracks appear.



Brenda Buckman

[Read More >](#)

[Continue Reading](#)

What is Mobile Endpoint Security? >

Protect What Matters

Secure endpoints, email, and employees with the power of our 24/7 SOC. Try Huntress for free and deploy in minutes to start fighting threats.

[Try Huntress for Free](#)



Platform

Huntress Managed Security Platform
Managed EDR
Managed EDR for macOS
Managed ITDR
Managed SIEM
Managed Security Awareness Training
[Book A Demo](#)

Solutions

Phishing
Compliance
Business Email Compromise
Education
Finance
Healthcare
Manufacturing
State & Local Government

Why Huntress?

Managed Service Providers
Value Added Resellers
Business & IT Teams
24/7 SOC
Case Studies

Resources

Resource Center
Blog
Upcoming Events
Support Documentation

About

Our Company
Leadership
News & Press
Careers
Contact Us

