# jamf PROTECT

# Protect Apple endpoints against Mac-specific threats

Gain unprecedented visibility into macOS.

amf PROTECT			
B Dashboards	1 ALERTS	🔍 Summary 💮 Processe	s (6) 😨 Files (0) 🚳 Binaries (5) 🚯 Users (2)
😧 Insights		2 esc (4697) • 1000 (4699	+ sh (734) + login (73) + lTern2 (759) + lTern2 (647)
Computers	Host: Collin Gordon's Mac 0   0   0   0   0   0   0   0   0   0	@ dscl (4697)	
		disci (4037)     Pid:	4697
Alerts	*	Pitt     Pitt	409) Autober/ded
🕰 Logs	Host: Collin Gordon's Mac 0 9 10 0 9 10 10 12 10 2019 3 01 25 AM GMT	<ul> <li>Process Arguments:</li> </ul>	dsci . read /Users/bradley dsAttrTypeNative:ShadowHat
		Name:	
Analytics	* + GatekeeperBlockedRevoked	<ul> <li>User:</li> </ul>	
	Host: Collin Gordon's Mac 0 0 10 00 10 10 1210209 30125 AM GMT	<ul> <li>Group:</li> </ul>	
* Plans			
+ Actions			
Deployments			
		<ul> <li>Process Start Time:</li> <li>Process End Time:</li> </ul>	10.23.2019 5:02:36 PM GMT 10.23.2019 5:02:36 PM GMT
Prevent		Process and time:     Parent Process:	suda (/usr/bin/suda)
	Hashdump Host: Johnny Smith's Mac 6 ● 5 ● 0 ● 2 ● 2 ●	Process UUID:	48887C89-238A-4083-8671-F2F075487296
Account		Sudo (4694)	
O Documentation	10.10.2019.201529.444.0417 10.4 LaunchAgent, PfladDisgulsedAsGoogle Host: Johnny Smith's Mac 5.5 .5 9 L 20 20 20 12.10.2019.20127.444.0417	<ul> <li>Pid:</li> </ul>	4694
		Path:	4694 Aardbir/audo
		<ul> <li>Process Arguments:</li> </ul>	
2 Admin		Name:	sudo
	B+ReverseShellPython Host: Johnny Smith's Mec. S ● 4 ● 0 ● 2 ● 2 ● 1210 2019 3:0120 AM GMT	User:	
		Group:	
	Spearphish     Host: Johnny Smith's Mac     20 20 00 20 20     1210 209 3.0119 AM GWT		
		Process Start Time:	Authorities: Software Signing + Apple Code Signing Cer 10.23.2019 5:02:35 PM GMT
		Process End Time:	10.23.2019 5:02.35 PM GMT
		Parent Process:	
	MacBook		
		Macbook	



The corporate security landscape is changing, and one size fits all security tools fail to provide the level of visibility needed to thwart today's sophisticated enterprise threats.

## Enter Jamf Protect – built for Mac to protect Mac.

Developed natively on Apple's architecture, Jamf Protect provides deep visibility into the activities and threats on macOS endpoints. With Jamf Protect's dashboards, real-time alerts, and extensive reporting on built-in macOS security frameworks like XProtect, Gatekeeper and MRT, you'll be the first to know when suspicious activities occur on your Apple computers.

"Jamf Protect was easy for us to deploy with Jamf Pro. It exposed us to a part of the Mac framework that we couldn't see before. It's been very actionable and easy to understand"

Dave McIntyre, Chief Information Technology Officer
 Build America Mutual



### Jamf Protect solves the unique challenges of macOS security:

#### **Detect and hunt Mac-specific threats**

Focus on understanding macOS activities, including those threats and attacks unique to Apple's architecture. Jamf's dedicated macOS security research provides deeper insights compared to Windows-first products.

### Enterprise visibility into native Apple security tools

Bring Apple's privacy commitment to the enterprise, by providing visibility of macOS' built-in security tools like XProtect and Gatekeeper that protect users from common malware.

# Controlled isolation and remediation through Jamf Pro

Manage and automate isolation, remediation, and cleanup of devices under attack with the same industry leading Jamf Pro that IT organizations already use to manage their macOS computers.

## Simple Jamf Protect management with Jamf Pro

Simplify security tool management by leveraging the same industry leading Jamf Pro that IT organizations already use to manage their macOS computers.

### Designed for macOS to minimize end user impact

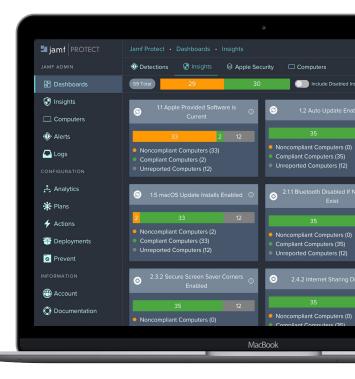
Keep employees productive, collaborative, and as engaged as Apple users expect while gaining insights necessary for IT and Security teams.

### **Endpoint compliance assessment**

Get quick insight into the security posture and endpoint configuration of all managed macOS endpoints.

#### Control your security data

Gain granular control over what data is collected by Jamf Protect, what is sent to Jamf's Cloud and/or sent directly into your existing SIEM.



### Unprecedented visibility. Real-time action. 100% Mac.



www.jamf.com

© 2002-2020 Jamf, LLC. All rights reserved

Interested in learning more about Jamf Protect? Contact **info@jamf.com** or your Jamf account executive.