



## Jamf Launches Jamf Executive Threat Protection to Defend Against Advanced Mobile Threats

April 20, 2023

MINNEAPOLIS, April 20, 2023 (GLOBE NEWSWIRE) -- Today, [Jamf](#) (NASDAQ: JAMF), the standard in managing and securing Apple at work, announced it has launched Jamf Executive Threat Protection, an advanced detection and response tool designed for mobile devices. The solution is built upon technology acquired in the ZecOps acquisition last September and provides organizations with an efficient, remote method to monitor devices and respond to advanced attacks, reducing investigation periods from weeks to minutes.

Apple began offering extreme protections for users who might be personally targeted by some of the most sophisticated digital threats with the introduction of Lockdown mode in iOS 16. Jamf Executive Threat Protection is designed to identify these sophisticated digital threats, going beyond traditional device management and endpoint security to extend visibility into attacks that target high-value users such as government officials, journalists, and high-ranking employees.

The end-user app collects system logs and device information which is analyzed to identify potential compromise. This provides users and organizations assurance that the integrity and security of their device remains intact and allows them to respond the moment a potential compromise is detected. Once a threat is detected, Jamf Executive Threat Protection provides organizations with a built-in remediation toolset to create a timeline of events, quickly resolve compromised devices, and restore device integrity with confidence.

The solution is designed for government agencies, media and entertainment organizations, highly regulated industries, executive security/protection, oil and gas, and the energy sector, with powerful features including:

- A collector that selectively collects information relevant to a mobile cyber investigation, while excluding private data such as messages, email, and photos.
- Advanced threat-hunting capabilities that allow analysts to explore device-level telemetry.
- Comprehensive analysis framework that detects mobile indicators of compromise (IOC) to enhance threat hunting and mobile threat intelligence.
- Automated creation of a timeline of suspicious events, indicating how and when a device was compromised.

This solution is powered by Jamf Threat Labs, which consists of highly skilled professionals in the fields of cybersecurity, data science, and threat research. Jamf Threat Labs analyzes security data from Jamf's extensive customer base to identify anomalies or possible device compromise and surfaces those actionable insights through Jamf's security products.

"Mobile devices have become an essential tool for modern workers, enabling productivity and connectivity on the go. However, with the rise of sophisticated mobile attacks, it's more important than ever to maintain the security of these devices to protect valuable data," said Dean Hager, Jamf CEO. "Jamf Executive Threat Protection offers a unique solution that goes beyond endpoint security to provide advanced detection and response capabilities, empowering organizations to stay ahead of targeted attacks and safeguard their most high-risk workers."

More information on [Jamf Executive Threat Protection can be found here](#).

### About Jamf

Jamf's purpose is to simplify work by helping organizations manage and secure an experience that end users love and organizations trust. Jamf is the only company in the world that provides a complete management and security solution for an Apple-first environment that is enterprise secure, consumer simple and protects personal privacy. To learn more, visit [www.jamf.com](http://www.jamf.com).

### Media Contact:

Natali Brockett | [media@jamf.com](mailto:media@jamf.com)

### Investor Contact:

Jennifer Gaumont | [ir@jamf.com](mailto:ir@jamf.com)