# FIRMWARE SECURITY LEADER ECLYPSIUM RAISES $8.75M SERIES A

## MADRONA VENTURE GROUP, ANDREESSEN HOROWITZ AND INTEL CAPITAL INVEST IN ECLYPSIUM'S OVERSUBSCRIBED SERIES A ROUND

BEAVERTON, OR - 12/4/18 - **Eclypsium**, the industry's first enterprise firmware protection platform, announced today it has raised $8.75M in Series A funding. The new investment comes on the heels of rapid demand for Eclypsium's industry-leading platform that protects organizations from the foundation of their computing infrastructure upward, controlling the risk and stopping threats inside firmware of laptops, servers, and networking infrastructure. The round was led by Madrona Venture Group, with participation from existing investors Andreessen Horowitz, Intel Capital and Ubiquity Ventures. With the investment, Tim Porter, Managing Director at Madrona Venture Group, joins the company's board of directors.

"Firmware is in every device in the modern enterprise - from user devices like mobile phones and laptops, to the servers, switches, and networking infrastructure that power data centers and networks globally," said Yuriy Bulygin, Co-Founder and CEO of Eclypsium. "Firmware attacks are pervasive, persistent, and have the ability to permeate and compromise entire data centers, remaining undetected on thousands of devices. Eclypsium's mission is to find, stop and remove such attacks, which threaten the heart of every enterprise and organization today."

While the code and logic at the hardware tier has by and large been ignored for many years, a wave of new attacks like the **recent supply chain compromises** or the **LoJax UEFI exploit** have clearly shown that organizations can no longer afford to rely on "security by obscurity" when it comes to their hardware. The Eclypsium platform protects servers, laptops, and networking equipment against firmware attacks that allow attackers to subvert traditional security controls, persist undetected indefinitely, or even disable devices completely.

Over the course of beta testing the platform on thousands of devices earlier this year, Eclypsium found that organizations had little to no visibility into their firmware state, threats, and vulnerabilities. As a result, most devices are running outdated firmware with vulnerable configurations. Overall, Eclypsium found that the majority, over 77%, of the devices analyzed had outdated firmware, and nearly 100% of the devices tested were vulnerable to a known attack.

"Hardware and firmware-level attacks represent a glaring blind spot that is reshaping enterprise security," said Tim Porter, partner at Madrona Venture Group. "Eclypsium brings together a truly unique collection of talent and experience in firmware threat research and real-world mitigation. With years of experience in Intel's Advanced Threat Research team and McAfee, this team has been on the front lines of discovering new threats and analyzing the world's most sophisticated hardware and firmware attackers, and we are excited to be working with them on their next phase of growth."

"Since its inception, Eclypsium has established itself as one of the most prolific and significant research teams in the industry," said Martin Casado, General Partner at Andreessen Horowitz. "We are excited to continue to support the company on its critical mission to help the industry and customers achieve better visibility, protection and mitigation at the hardware layer across the entire lifecycle."

"Eclypsium's platform gives enterprises firmware and device visibility, trust and control, so they can remain confident in their underlying infrastructure," said Trina Van Pelt, Vice President, Intel and Senior Managing Director at Intel Capital.  "At Intel, security has long been one of our highest priorities, and in collaboration with Eclypsium we see an important opportunity to deliver key capabilities that can benefit the overall industry."

The Series A funding will be used to grow the team in all areas and support the rapid growth being driven by customers and prospects.

## LEARN MORE ABOUT ECLYPSIUM AND FIRMWARE SECURITY:

- Watch a **3-minute video** to learn how attackers use firmware level attacks to subvert traditional security, and how Eclypsium's platform helps detect, defend and mitigate

- Access **Eclypsium's firmware threat intelligence and research**

- Learn about the **hardware attack surface and how to defend it**

## ABOUT ECLYPSIUM

Eclypsium protects organizations from the foundation of their computing infrastructure upward, controlling the risk and stopping threats inside firmware of laptops, servers, and networking infrastructure. The Eclypsium enterprise firmware protection platform is built on decades of firmware threat research and real-world experience pioneering the open source project known as CHIPSEC. Eclypsium's solution proactively finds and manages firmware risk and protects from firmware-based threats at all of the key points in the hardware lifecycle, from deployment to operational use. Eclypsium is headquartered in the Portland, OR area. For more information, please visit **eclypsium.com** follow us on Twitter **@eclypsium**, or request additional information at **info@eclypsium.com**.

## CONTACTS

ZAG Communications for Eclypsium, Inc.
**zenobia@zagcommunications.com**
650.269.8315