Tech Papers

Article Image
Click to Download

UEFI Networking and Pre-OS Security

Intel

Vincent J. Zimmer et al

White Paper
November 2011

External URL

Readers will get an understanding for the scope and objective of the Unified Extensible Firmware Interface (UEFI) specification and the UEFI technology's role as a foundation for pre-OS security and networking. This includes the platform boot process from local and remote media, assets to be protected, threats against those assets, and the various technologies that allow for their protection. In addition to a review of these technologies, forward-looking capabilities and approaches related to UEFI are discussed.


Give Feedback