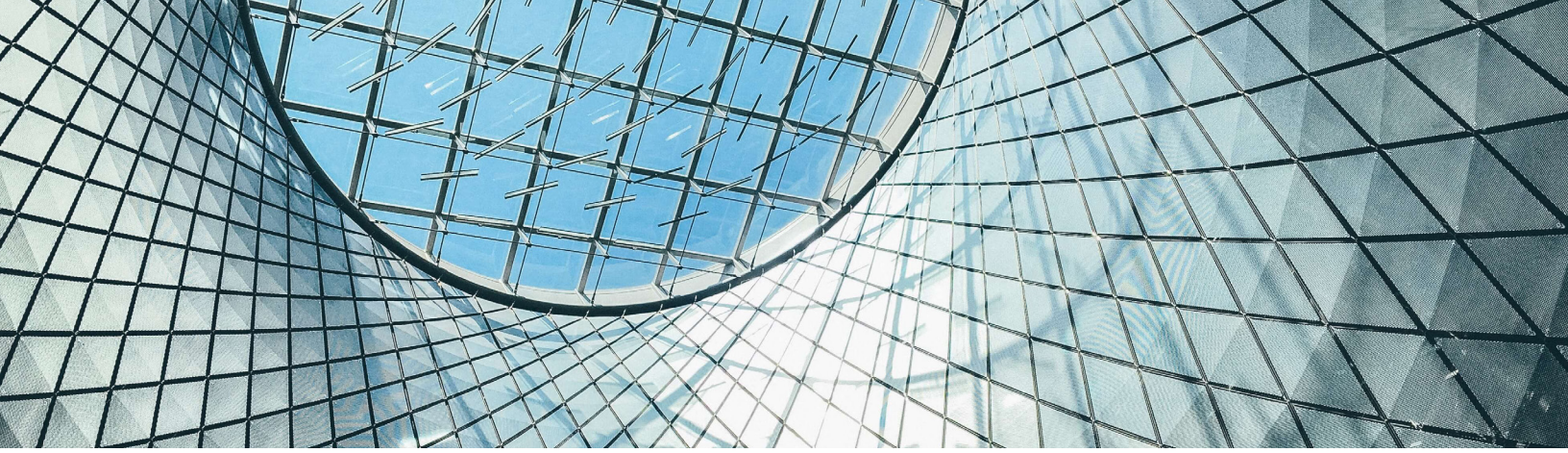

451 Research Market Insight Report Reprint

Coverage Initiation: Binarly aims to harden firmware supply chain for device, ecosystem trustworthiness

July 19, 2024

by Justin Lam

Easily overlooked between operating systems and computer manufacturers, firmware glues these layers together. Yet as computing increases in ubiquity and cloud services are increasingly abstracted from users, Binarly seeks to help product security teams build trust into their supply chains.

S&P Global
Market Intelligence

Introduction

Easily overlooked between operating systems and computer manufacturers, firmware glues these layers together. Yet as computing increases in ubiquity and cloud services are increasingly abstracted from users, Binarly seeks to help product security teams build trust into their supply chains.

THE TAKE

Binarly takes on one of the most difficult areas of security — low-level defects found in usually invisible layers of the computing stack, with the goal of providing software supply chain security to both upstream and downstream parties. In cases where source code is not always obtainable and distributions of firmware vary, Binarly looks to holistically build a full security understanding by looking at the binary's operation. By proving its capabilities beyond other application security approaches such as software composition analysis (SCA), Binarly looks to enhance vulnerability management, software bill of materials creation and SBOM validation for product security teams and enterprises alike.

Context

While many innovations in data security have evolved from more sophisticated discovery, classification and protection, questions arise about the underlying security of the systems collecting, processing or storing that sensitive data. Robust data security has long been associated with tight integration between software, firmware and hardware. Hardware security modules and Common Criteria standards have been evolving for the last 50 years. Among users, their applications and the clouds they run on, underlying devices and cloud computing resources must securely process their activities. Within the many billions of personal devices, PCs, internet of things/operational technology sensors, servers and network devices, firmware is a critical layer to defend. While most adversarial attacks occur through higher levels within application and operating system vulnerabilities, attacks stemming from lower levels within firmware or physical device vulnerabilities can be particularly devastating as they may completely subsume higher levels.

Binarly was founded in 2021 by Alex Matrosov, who currently serves as CEO. Prior to founding Binarly, Matrosov held information security and threat researching leadership positions at NVIDIA Corp., Cylance, Intel Corp. and ESET. Binarly has about 20 employees and has raised $10.5 million in early stage and seed investments led by Two Bear Capital, with participation and expansion from Acrobator Ventures, Blu Ventures, Canaan Management, Cisco Systems Inc., Emerging.vc, Liquid 2 Ventures, StoneMill Ventures and WestWave Capital. Binarly is currently based in Santa Monica, Calif.

Technology

Recent publicized firmware vulnerabilities such as LogoFAIL (CVE-2023-40238) showcase the possible dangers around vulnerable firmware. In particular, firmware often invokes other components; with LogoFAIL, the image parsing component that processes and displays a manufacturer's logo during the initial boot sequence was found to be vulnerable to an injected exploit that could compromise the PC's operating system and any detection from traditional endpoint technologies. A malicious firmware update in server environments via remote management tools such as Dell Technologies Inc.'s iDrac or Lenovo ThinkServer System Manager could propagate this vulnerability at scale. Firmware vulnerabilities like LogoFAIL do not necessarily alter the boot process or modify the firmware itself, thus avoiding detection or blocking from execution by built-in controls such as UEFI (Unified Extended Firmware Interface) Secure Boot. With firmware, underlying source code written in languages such as C, C++ or assembly is compiled into their finished binary form.

The Binarly Transparency Platform looks to help product security teams and enterprise security operations teams understand the risk and nature of firmware and software vulnerabilities. Binarly analyzes firmware and software packages and images to understand the direct and transitive dependencies within each component of code. The Binarly Transparency Platform reads in UEFI, BMC (Baseboard Management Controller), XIoT (extended internet of things) and container images.

The company says that Binarly Transparency Platform's unique focus on analyzing compiled firmware binaries enables it to identify vulnerabilities that may not be detected at the source code level. Binarly asserts that analyzing the full binary enables further analysis of dependencies. By better knowing the effective reach of each binary, any provided SBOM or any generated SBOM will have greater contextual depth. Other examples of Binarly examining greater levels of context include discovery of weak cryptographic assets. In some cases, firmware source code may not be available, so different approaches than other SCA are needed (e.g., in the case of LogoFAIL, the Binarly Transparency Platform's evaluation of all dependencies such as the execution of the vulnerable imagine parsing routine).

By providing this greater contextual depth, the platform's vulnerability management has significantly fewer false positives to reduce alert fatigue. Binarly provides a reachability analysis, helping teams understand the impact of any remediation. The platform also includes threat intelligence, which includes an AI chat interface to help assist vulnerability impact and blast radius.

The Binarly Transparency Platform is available at several tiers of functionality and is based on a freemium model.

Strategy

Binarly's focus on firmware naturally targets both enterprises and product security teams that have to attest to the hardware they manage or the devices they build. Deliverables such as SBOMs and supply-chain levels for software artifacts are increasingly needed for near-continuous evaluation. Seemingly obscure but severe vulnerabilities from Log4J, Heartbleed and liblzma (a component of the XY library used in OpenSSH) have placed open-source vulnerability management as the most cited pain point among application security practitioners, according to 451 Research's Voice of the Enterprise: Information Security, Application Security 2024 survey.

Supply chain security is a critical priority for enterprises; the murky ecosystem of firmware is especially difficult for product security teams looking to build on firmware they may receive upstream. For example, an IoT device designer may be using other components, each with its own drivers and firmware that must be integrated. Within the server market, major players such as Super Micro Computer Inc., Lenovo, Hewlett Packard Enterprise Co. and Dell may license UEFI firmware from independent BIOS vendors such as Phoenix, Insyde Software Corp. or AMI. Downstream from those server manufacturers, Binarly wants to add more visibility and context to these supply chains.

Product security teams that are responsible for secure, trustworthy devices are some of the key target customer profiles for Binarly at this early stage. Progressive enterprises that have been affected by other firmware or hardware vulnerabilities such as BlackLotus or SPECTRE are also candidates for target customers. Ultimately, Binarly would like to take its binary inspection approach and apply it beyond the world of firmware. The premium tier of the Binarly Transparency Platform enables scanning of container images.

Competition

Under the broad aegis of supply chain security, Binarly faces much direct and indirect competition. Indirectly, cloud providers, IoT/OT security and existing AppSec platforms place wallet share pressure on Binarly. IaaS approaches transfer firmware risks away from on-premises enterprises to cloud providers. Players like Tenable Holdings Inc. and Qualys Inc. have long operational track records for vulnerability management — their offerings are inherently sticky within their customers. Incorporating a new layer of vulnerability management from Binarly is an inherent challenge. Similarly, SCA players like Snyk analyze source code; given their foothold within CI/CD pipelines, they also take a look at the finished compiled and deployed packages, similarly to Binarly. For IoT initiatives, Microsoft Corp.'s acquisition of ReFirm extends endpoint detection and response functionality to the firmware level and was built into Azure Defender for IoT.

Directly, there is some competition. Eclypsium, founded in 2015 and having raised $64.5 million, has a focus on firmware and hardware security. ReversingLabs has raised more than $80 million. Eclypsium and ReversingLabs may be some of Binarly's most direct competitors, given their coverage of hardware and firmware security. Additionally, Nova Leah has been especially focused on medical devices and the specific challenges of that supply chain.

SWOT Analysis

STRENGTHS

The company's current focus on analyzing compiled firmware binaries for greater context and more accurate software supply chain risk management sets Binarly apart.

WEAKNESSES

While Binarly shores up its product-market-fit growth phase toward go-to-market-fit growth phases, distribution challenges will be difficult to overcome. Identifying common buying motions with existing supply chain security initiatives will need to be solidified.

OPPORTUNITIES

Firmware is a difficult layer to secure in the overall technology stack because it is mostly out of the traditional oversight of most detection and response tooling. The amount of firmware and the ubiquity of devices, servers and sensors create a wide addressable market. Specific markets for sophisticated product security teams embracing security-by-default, security-by-design principles may be the most ideal Binarly customer profile.

THREATS

Supply chain security is a fast-moving space, with well-funded or publicly listed vendors among vulnerability management, attack surface or even cloud-native application protection platform spaces. These indirect players certainly have the capital to directly pursue Binarly.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html