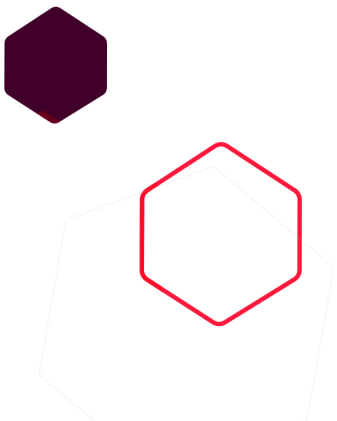
Software Supply Chain Security with immune Guard™

immune GmbH

April, 2022

PRODUCT BRIEF



MISSION

At the end of 2021, the German industry consortium Bitkom e.V. released a study with the headline "*German businesses under attack: losses of more than 220 billion euros per year*". To sum it up, here are the most shocking takeaways:

- The overall damage in cybercrime 2021 exceeded the COVID-19 pandemic costs
- Critical infrastructure is particularly under threat
- Company losses caused by malware incidents/breaches increased by 31% from 2020 to 2021

Aside from the significant risk of being targeted by a cyberattack, we see a global shift in the threat landscape. A hacker always tries to exploit the unseen security hole in your infrastructure. All components in a device come with embedded software called firmware. A new attack type has been born with the upcoming growth of firmware components in devices. The so-called "firmware implant" allows a new kind of stealthy malware resistant to Operating System reinstallation and hardware replacement that makes the recovery process expensive and sometimes impossible. In our product development at immune GmbH, we leveraged our extensive expertise in firmware security to protect against such threats.

Our mission, we help our customers by making their device fleet trustworthy and transparent. We believe usability and easy integration are necessary for a modern cybersecurity landscape. Therefore we created a solution to detect zero-day vulnerabilities and threats with a nearly zero false positive rate.

"We bring military-grade technology to our customers, which help them to enable SBOM and KRITIS standards"

Philipp Deppenwiese
CEO at immune GmbH

WHAT ARE WE TRYING TO SOLVE?

Hardware Security

Modern devices are distributed systems built from components developed and manufactured by many companies worldwide. Recently, hardware manufacturers created security modules to restrict and protect data exchange between these components. Until now, there was no product to tie the different hardware security features together to a comprehensive security solution for device's that does not depend on a particular vendor or set of vendors.

immue Guard binds the detection and protection of your device to a hardware security module inside.

Software Supply Chain

Fixing firmware vulnerabilities is complicated by the supply chain behind hardware manufacturing. Manufacturers often don't build firmware themselves; they buy pieces of firmware from 3rd parties. These 3rd parties often include software components from other hardware vendors like Intel or AMD. When a vulnerability in one of these widely used components is found, downstream vendors need to rebuild their firmware and update the affected devices. There is no effective communication established between firmware and hardware vendors to facilitate that. Additionally, vendors consider fixing security vulnerabilities a support request and may refuse to do so for out-of-support devices.

immue Guard makes the software supply chain of your device transparent to meet SBOM and KRITIS standards.

Growing Complexity of Firmware

The purpose of firmware is to drive the processors of a component like a network card and provide an interface to the operating system. Firmware has always been part of hardware development, but its size and complexity have grown exponentially in recent years. This complexity and the lack of technical security controls made firmware an attractive target for hackers. Several vulnerabilities in popular firmware components like UEFI have come to light that allows attackers to install and persist malware in firmware.

immune Guard continuously monitors your device's firmware components for potential threats or vulnerabilities.

WHAT CAN IMMUNE GUARD DO FOR YOU?

Close the gap between hardware- and software security

Endpoint security products don't protect against threats in firmware or the boot process. immune Guard uses existing hardware security like a Trusted Platform Module 2.0 to ensure the platform isn't tampered with before an EDR/EPP solution launch.

Discover insecure platform configuration and outdated firmware

immune Guard analyses firmware and provisioned hardware configuration of your devices and provides monitoring and risk assessment across the whole device fleet.

Protect your devices from firmware-based supply chain attacks

immune Guard computes cryptographic fingerprints of all code executed from the system's start to the operating system. This way, it detects manipulation of any software in the supply chain for an fast isolation of the tampered device.

Detect & respond to zero-day firmware vulnerabilities

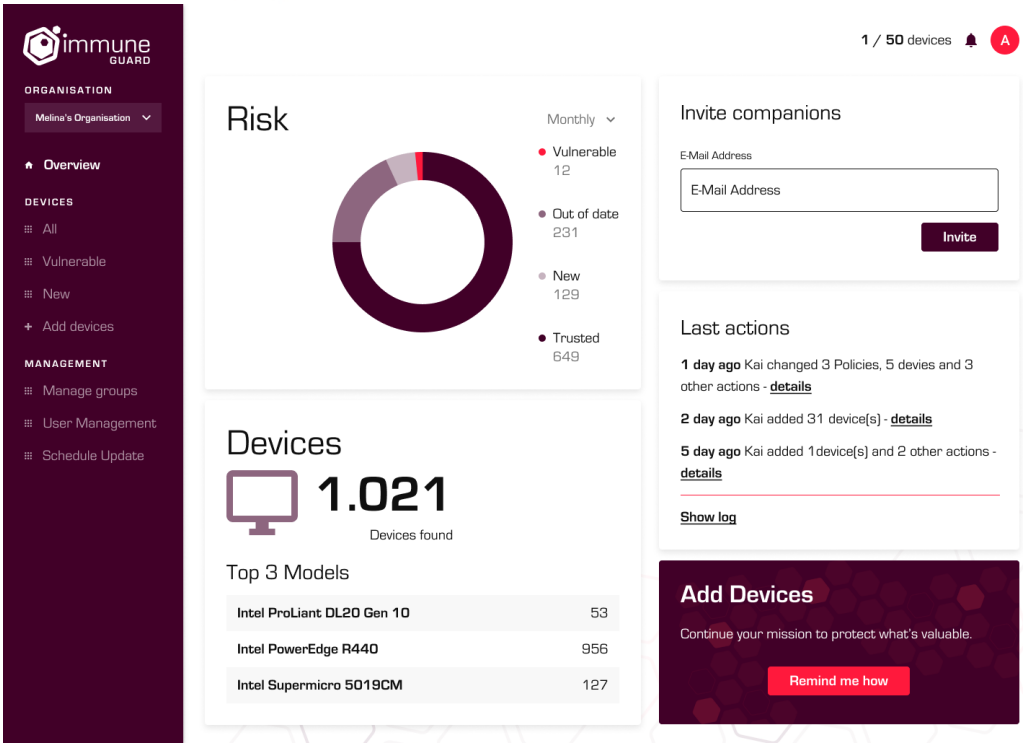
immune Guard performs in-depth introspection of firmware to find known and unknown threats and vulnerabilities. We also provide the industry-first firmware MDR solution (Managed Detection and Response).

immune Guard embraces the heterogeneous device landscape and can utilize security features from many hardware vendors. Our solution helps reduce costs by increasing device fleet transparency, protecting against unknown threats and supply chain attacks as one technology stack.

Enable SBOM and KRITIS standards for your device

Enterprises and governments must comply with several new regulations regarding the software supply chain and firmware compliance in specific. The U.S. Department of Commerce recently announced new rules for critical sectors on February 24th, 2022. Enterprises and Governments who fall under this act need to know their software supply chain, either by an assurance from the vendor or my self-assessment. In Germany and most other European countries, there are similar acts for critical infrastructure providers (KRITIS) who need to prove that IT devices are Bootkit-Free and Backdoor-Free! Here we can help. immune Guard analyzes the software supply chain from chip-level to the operating system. We combine vendor information with our artificial intelligence platform to discover any backdoor in the components. Companies and the government can easily comply with these new regulations by using the immune guard as an assessment service. We support the latest devices and also the existing legacy infrastructure. By implementing a self-assessment process for software & hardware, you open the door to a broader range of products that do a better job at a lower price.

HOW DOES OUR SOLUTION LOOK LIKE?

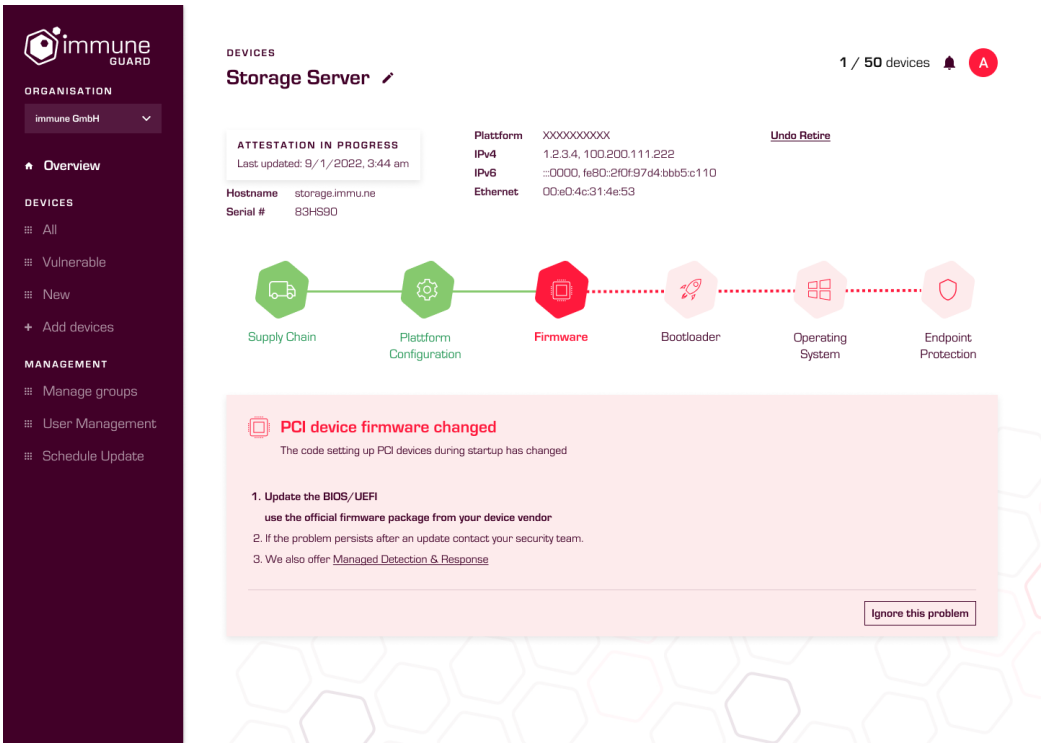


immune Guard provides a dashboard for your device to gain insights into your whole device fleet risk profile. This allows infrastrucure operators to quickly identify systems without outdated or vulnerable firmware, without the need for expert knowledge on all firmware components in the fragmented device landscape.

immune Guard helps you tightening your security by closing the protection gap between a device's launch and the operating system taking control. It does this by utilizing existing hardware, and firmware-based Trusted Computing solutions. The Trusted Computing Module in modern systems already records all executed code and associated data during startup, including the operating system core. After the start, the device sends these records together with an in-depth firmware report to immune Guard for analysis.

The firmware report includes versions of all running firmware components and their configuration. Suppose any modification of the device's startup code, a misconfiguration of the computing platform, or outdated firmware is found. In that case, we issue an alert via communication channels like email and SIEM solutions.

immune Guard is secure even if malware has infected the device it's running on. The recorded fingerprints are kept in a separate hardware security module which is tamper resistant. Malware cannot access the records or forge a report between the device and the our solution.



Requirements

The enrollment process of immune Guard requires either an internet connection (SaaS) or internal network access to a Private Cloud deployment (On-Prem). The device protection and threat detection requires one of the following security modules installed in your device:

- Discrete Trusted Platform Module 2.0
- Firmware TPM (PTT, fTPM)
- Microsoft Pluton

If none of the above modules can be used, immune Guard falls back to the Software TPM mode. In this mode, firmware analysis and monitoring are still functional but the system integrity can't be monitored. Customer with product integration and special security requirements can consult us for supporting our solution with their platform.

The immune Guard lightweight agent is open-source, so it can be reviewed and audited before added to your device. We support the following interoperability:

- Microsoft Windows Vista up to 11
- Linux from 3.x and all later

WHAT MAKES US DIFFERENT?

Firmware-based malware is out of the reach of today's EDR/EPP solutions as they are started with and run alongside the operating system. Additionally, because the firmware presents an interface to the operating system, malware can decide what information to expose through that interface and thus effectively hide from any operating system based scanning solution.

immune Guard...

- ... protects your device with security modules that record loaded code & data from chip-level to the operating system.
- ... comes as a lightweight agent and decides where to trust a system or not.
- ... immune Guard, with its technology, reduces the number of false-positive findings massively, and so does the cost of operation.
- ... provides in-depth firmware security assessments and secures your software supply chain.
- ... detects potential risks and zero-day security holes in your device.

To comply with specific rules for sensitive computing areas which require SBOM and KRITIS standards. We must focus on solutions closing the security gaps introduced by innovation and development over the last 30 years. As immune GmbH, protecting your foundation with our extensive supply chain and hardware security knowledge is our mission.

Get in contact
immune GmbH,
Kortumstrasse 19-21,
44787 Bochum,
Germany

E-mail: sales@immu.ne
Homepage: www.immu.ne
Phone: +49 234 545 00634