# Phoenix FirmCare™

FIRMWARE SECURITY-AS-A-SERVICE PROGRAM

## What is Phoenix FirmCare?

Our security-as-a-service program monitors, rates, and reports firmware vulnerabilities. If a vulnerability is found, our team creates and delivers or helps source, custom patches to fix the problem.

This means that FirmCare provides the earliest and most comprehensive awareness of threats to your firmware security.

## How does it work?

### Monitoring and Scoring

Phoenix partners with the leading firmware security organizations such as Unified Extensible Firmware Interface Forum (UEFI), Internet Engineering Task Force (IETF), etc., to stay up to date on the latest vulnerabilities. The Phoenix Security Team follows a 1-10 scale to identify the urgency level of vulnerabilities, with “1” representing a low-level threat and “9+” as a critical threat. Based on the threat level, we will create a patch that works with customer requirements.

### Code Review

Phoenix FirmCare includes manual code review for standard patches to ensure the customer has ported in critical security patches for the standard codebase. This avoids the need to create any “high-risk” test tools that can escape into the wild.

### System Security Testing

Customers also benefit from a custom Phoenix System Security Test, which uses a remote file manager as part of the firmware. With the press of a hotkey during boot, a test server downloads test tools, runs them on the system, and uploads the results to the server for analysis. Phoenix generates a custom report from this data, revealing security gaps in the existing firmware.

### What devices are supported?

Phoenix FirmCare currently supports patch delivery for devices powered by processors, including:

- Intel
- AMD
- Arm
- Qualcomm
- Others in progress

phoenix technologies

## What do I get as a customer?

- **Constant monitoring:** Our team monitors the universe of firmware threats, tapping into Black Hat and DEF CON resources and other industry research entities.
- **Reports:** You can expect to receive reports on firmware threats weekly, monthly, or annually, depending on SLA, with suggested fixes for every identified vulnerability.
- **White hat hacking:** The Phoenix Security Team will mimic a hack on a target machine to uncover weak spots in existing firmware, then suggest fixes.
- **Penetration testing:** We have a test lab for handling penetration testing (pen testing) internally and at federal laboratories.

## What packages does Phoenix FirmCare offer?

| | Standard (SLA 1) | Enhanced (SLA 2) | Premium (SLA 3) |
|---|---|---|---|
| **Vulnerability notification** | 30 Days | 7 Days | 24 Hours |
| **Patch development, verification, & delivery** (for Phoenix code, open-source Phoenix code, or code from Phoenix Semiconductor Partners) | Based on contract, additional NRE charges may apply | Based on the threat level | Within 24 hours |
| **Access to Phoenix Program Manager & Customer Engineers** | ✗ | ✓ | ✓ |
| **Customer collaboration for other product vulnerability notifications** | ✗ | ✓ | ✓ |
| **Vulnerability support for non-Phoenix firmware** | ✗ | ✗ | ✓ |
| **White hat hacking & penetration testing** | ✗ | ✗ | ✓ |

### Want to learn more about Phoenix FirmCare?

Send us an email at firmcare@phoenix.com

phoenix technologies