

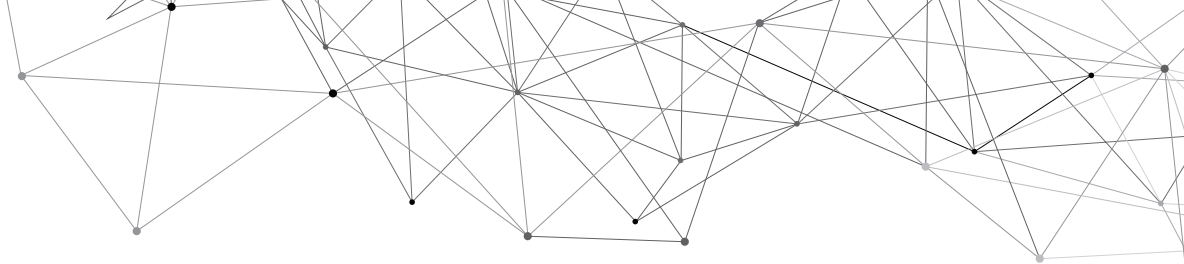
Binwalk Product Comparison

Binwalk products from ReFirm Labs are the industry standard for device vulnerability management, with more than 50,000 users worldwide. Choose the right Binwalk solution for your organization and protect the connected devices on your attack surface.

| Feature | Open Source | Teams | Enterprise | Description |
|--|-------------|-------|------------|--|
| File System Extraction from Binary Firmware Images | ✓ | ✓ | ✓ | Extract embedded file systems from a wide variety of binary firmware encoding schemes |
| Build and run locally from Github | ✓ | | | Open source, community supported |
| Web File System Access | | ✓ | ✓ | Full access to extract file system via web, including searching, downloading individual files or entire system |
| Enhanced Extraction | | ✓ | ✓ | Faster, broader file system and extractor support |

Detailed Security Analysis

| | | | | |
|--|--|---|---|---|
| Cryptographic Analysis | | ✓ | ✓ | Identify embedded cryptographic materials including public/private keys and certificates |
| Password / Accounts | | ✓ | ✓ | Find hard coded accounts & passwords, weak passwords |
| SBOM | | ✓ | ✓ | Deliver Software Bill of Materials listing open source components and licenses |
| Security Checklist | | ✓ | ✓ | Find known backdoors, exploits and malware using ReFirm's private signature database |
| Known Vulnerabilities | | ✓ | ✓ | Identify known open source vulnerabilities with remediation suggestions |
| Continuous Monitoring | | ✓ | ✓ | Ongoing notifications as new vulnerabilities are disclosed in firmware already in the platform |
| Binary Hardening | | ✓ | ✓ | Analysis of compiler settings for all executables to conform to secure coding best practices |
| Potential Zero – Day Exploit Detection | | ✓ | ✓ | Find buffer overflow and command injection zero-days using automated static & dynamic reverse engineering |



| Feature | Open Source | Teams | Enterprise | Description |
|-------------------------------|-------------|-------|------------|---|
| Firmware Comparison | | | | Show changes to firmware & security analysis results to focus security assessments & spot regressions |
| Policy / Compliance Reporting | | | | Interpret security analysis results against common or custom security policies and standards |

Reporting

| | | | | |
|----------------------------|--|--|--|--|
| Detailed Web Report | | | | Downloadable in PDF |
| Shared Links | | | | Share analysis results with password protected, time to expiration links |
| Data Export via JSON / CSV | | | | Download individual results in JSON or CSV format |
| Full RESTful API | | | | Integrate with automated workflows |
| Command Line Interface | | | | Integrate with automated workflows |

Security Features

| | | | | |
|------------------------------------|--|--|--|---|
| Two-factor Authentication | | | | Supports standard one-time password solutions like Google Authenticator |
| Enterprise SSO | | | | Integrate with cloud SSO providers, or Active Directory (on-premise deployment) |
| Single-tenant Deployment | | | | Isolated tenant hosted by ReFirm Labs |
| On-premise / Air gapped deployment | | | | Meet organizational IP / security requirements with 100% on-premise deployment |
| Organizations / Groups | | | | Isolate firmware by organization / suppliers |

Support / Licensing

| | | | | |
|-------------------------------------|--|--|--|--|
| Community Support | | | | |
| Email Support | | | | |
| Support via Dedicated Slack Channel | | | | Direct access to ReFirm Labs' support and development team |
| Custom Enterprise License Agreement | | | | |