Chris Chevalier product@chrischevalier.com

Data Protection Case Study

Device Control, Application Control, and FIPS 140-2 Certification

Executive summary

Led the product direction and delivery of enterprise-grade Data Protection solutions, including Device Control and Application Control, deployed on more than two million endpoints across commercial and government environments. Modernized product capabilities, improved reliability and OS coverage, and successfully achieved NIST FIPS 140-2 certification, enabling expansion into additional regulated and government markets. Automated white-labeling to enable larger scale partner opportunities.

Context and objectives

- **Product domain:** Endpoint data protection, device control, application control, encryption, and policy enforcement
- **Customer base:** Large enterprises, government agencies, and regulated industries
- **Business drivers:** Strengthen data protection posture, meet government procurement requirements, expand market reach, and reduce operational friction
- **Constraints:** Diverse market segments, multi-OS support requirements, strict cryptographic standards, aggressive certification timelines
- **Success criteria:** Achieve FIPS 140-2 certification, improve stability and OS parity, reduce support escalations, and deliver customer-requested enhancements

Role and scope

- **Title:** Group Product Manager – Endpoint & Data Security
- **Scope:** Owned product strategy, roadmap, backlog, and cross-functional execution across four global engineering teams
- **Responsibilities:** Product management, product ownership, certification program leadership, customer research, and cross-functional alignment with Sales Engineering, Support, and Marketing

Problem statement

Enterprise and government customers required stronger data protection controls, consistent OS coverage, and validated cryptographic implementations. Device Control and Application Control

needed modernization to meet evolving security expectations, reduce operational issues, and qualify for government procurement through FIPS 140-2 certification. Non-governmental organizations required ease of administration.

Approach and strategy

- **Discovery:** Analyzed customer requirements, government procurement criteria, support escalations, and competitive gaps
- **Prioritization:** Balanced certification requirements, customer impact, and engineering feasibility
- **Roadmap:** Sequenced modernization work, certification preparation, and customer-driven enhancements to minimize disruption to existing deployments

Execution and key activities

- Directed product strategy and execution for Device Control and Application Control across millions of endpoints
- Led the FIPS 140-2 certification program, coordinating engineering, QA, external consultants, and certification labs
- Defined and delivered product changes required for certification, including cryptographic module updates and documentation
- Improved OS parity and supportability across Windows, macOS, and Linux environments
- Managed integration of third-party technologies to accelerate delivery and meet aggressive timelines
- Partnered with Support to identify and resolve recurring customer issues, reducing escalations and improving reliability
- Delivered enhancements enabling MSP/MSSP white-labeling and expanded market reach
- Provided training and enablement for Sales, Support, and Customer Success teams

Technical architecture and modernization areas

- **Core capabilities:** Device access control, encryption enforcement, data exfiltration filtering and contextual limiting, application whitelisting/blacklisting, policy management
- **Modernization focus:**
    - Cryptographic module updates for FIPS 140-2
    - OS parity improvements

    - Supportability enhancements and logging improvements
    - Integration of third-party components for iOS MDM support
- **Operational improvements:** Reduced support escalations, improved policy enforcement reliability, and strengthened compliance posture

Deliverables and artifacts

- Certification documentation package for FIPS 140-2
- Updated cryptographic modules and supporting engineering changes
- Product requirements, acceptance criteria, and release notes
- White-labeling automation and onboarding templates for MSP/MSSP partners
- Training materials for Sales, Support, and Customer Success
- Updated product architecture and OS support documentation

Results and metrics

- **Certification:** Achieved NIST FIPS 140-2 certification, enabling expansion into government and regulated markets
- **Scale:** Supported more than two million deployed endpoints across global customers
- **Operational impact:** Reduced support escalations through modernization and improved OS parity
- **Market impact:** Opened new revenue channels through certification and white-labeling capabilities

Challenges and mitigations

- **Strict certification requirements:** Partnered with external experts and certification labs to ensure compliance
- **Legacy architecture constraints:** Sequenced modernization work to minimize customer disruption
- **Multi-OS complexity:** Coordinated global engineering teams to align capabilities across platforms
- **Customer onboarding friction for MSP/MSSP:** Automated white-labeling and created standardized onboarding templates

Lessons learned and next steps

- Certification programs require early alignment across engineering, QA, and external partners
- Incremental modernization reduces risk and accelerates delivery
- Strong documentation and repeatable processes improve long-term maintainability
- Next steps: Expanded OS support, enhanced policy analytics, and improved partner onboarding automation