Optoma | Experience more

Security White paper

Version 2024.8

This white paper outlines the comprehensive security framework implemented across the Optoma suite of products, ensuring the safeguarding of customer data against a broad spectrum of threats. In an era where data security is paramount, Optoma commits to the highest privacy and safety standards, using the latest technologies and protocols to secure devices, applications, networks, and cloud infrastructures. Our end-to-end security approach is designed to exceed industry standards, providing peace of mind for our users.

Table of Contents

Introduction

In recognising the critical importance of data security for , Optoma has developed a multifaceted security strategy to defend against diverse threats, ensuring the integrity, confidentiality, and availability of sensitive information. Our security measures span the entire product ecosystem, from individual devices to cloud-based services, aligning with rigorous security standards to support your organisational security objectives. This document provides an overview of Optoma's security capabilities, including our robust encryption practices, secure access controls, and comprehensive risk mitigation strategies.

Application Level Security

At the application level, Optoma employs stringent security protocols to thwart unauthorised access and mitigate risks:

- **Authentication:** We mandate the use of strong password policies and device authentication mechanisms to maintain a fortified security posture for user access.
- **Permission Control:** A sophisticated permission management system ensures only verified users can access device functionalities. This framework restricts unauthorised access and offers customisable permission settings for granular control.
- **Security Testing:** Continuous security assessments are conducted to identify and rectify vulnerabilities, reinforcing our commitment to maintaining robust security defences.

Device Level Security

Optoma prioritises device security through various measures designed to protect against threats:

- **Encryption:** All data stored on devices is encrypted using state-of-the-art algorithms

- **Access Control:** Multiple layers of access control, including security locks and screen lock mechanisms, prevent unauthorised device interactions.

- **Data Wipe:** A secure data deletion feature allows forerasure of sensitive information, ensuring data privacy and protection.

Network Level Security

Optoma's Products incorporate various security protocols to mitigate network-related security risks. These protocols are designed to ensure the integrity and confidentiality of data as it traverses wireless and wired networks.

Enterprise-Grade Authentication

- **Encryption Protocols:** Optoma prioritises protecting data transmitted over Wi-Fi networks by implementing robust encryption protocols, notably WPA2. This level of encryption is pivotal in preventing unauthorised entities from intercepting and deciphering sensitive data.

- **WPA2-Enterprise with 802.1x Authentication:** For Wi-Fi networks, the standard has evolved to embrace WPA2-Enterprise, supplemented with 802.1x authentication. This setup provides a more secure authentication mechanism, ensuring only authorised users can access the network. Optoma supports various Wi-Fi protocols, including the advanced security features offered by WPA2 and WPA2-Enterprise with 802.1x authentication.

- **WPA3-Enterprise:** Builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections. Use Multiple Extensible Authentication Protocol (EAP) methods, include minimum 128-bit Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication (AES-CCMP 128) and minimum 256-bit Hashed Message Authentication Mode (HMAC) with Secure Hash

Algorithm (HMAC-SHA256) .

(*) Applied models: IFP52+, IFP53, IFP32, FP

Encrypted Data Transmission

- **Implementation:** All data exchanged between Optoma devices and those connected through Wi-Fi or Ethernet undergo encryption. This is facilitated through the use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols.

- **TLS and DTLS Protocols:** These protocols are instrumental in offering robust encryption for data in transit, thereby safeguarding sensitive information against unauthorised access and interception.

  1. **TLS (Transport Layer Security):** A cornerstone cryptographic protocol that provides communication security for securing HTTPS connections.

  2. **DTLS (Datagram Transport Layer Security):** Tailored for datagram-based applications, DTLS ensures secure communication free from eavesdropping, tampering, or message forgery. It extends the principles of TLS to support scenarios where the underlying transport is less reliable.

VPN Support

Functionality: Optoma devices come equipped with Virtual Private Network (VPN) support, adding an essential layer of security for data transmitted over Wi-Fi networks. VPNs encrypt the entire communication channel between the device and the VPN server, effectively protecting data from interception and unauthorised access.

Cloud Level Security

Optoma's cloud infrastructure is secured with industry-leading security services from Azure and AWS to protect sensitive data. Our cloud solution architecture is designed with a defence-in-depth strategy, leveraging the strengths of both platforms to ensure comprehensive data protection and compliance with an extensive array of security standards.

- **Azure Security Integration:** Utilising Microsoft Azure's robust security features, Optoma benefits from a multi-tenant platform that supports enhanced security, operational management, and threat mitigation practices. Azure's infrastructure offers exceptional protection against exploits, malware, and sophisticated attacks. Significantly, Azure maintains an expansive compliance portfolio, including ISO 27001:2022, ISO 27017:2015, ISO 27018:2019, ISO 20000-1:2018, ISO 22301:2019, and ISO 9001:2015, alongside the highest CSA STAR certification.

- **AWS Security Services:** AWS's Virtual Private Cloud (VPC) ensures secure service operation, including stringent security rules and IAM role configurations.

- **Compliance Frameworks:** Optoma's cloud solution adheres to critical security and compliance frameworks, providing a secure environment for customer data. These frameworks include:

  - □ National Institute of Standards and Technology (NIST) 800-53
  - □ NIST Cybersecurity Framework (CSF)
  - □ NIST 800-171
  - □ System and Organization Controls (SOC) II
  - □ Centre for Internet Security (CIS) Critical Controls v8.0
  - □ ISO 27001
  - □ North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
  - □ Payment Card Industry Data Security Standard (PCI-DSS) v4.0
  - □ Department of Defence Cybersecurity Maturity Model Certification (CMMC)
  - □ Health Insurance Portability and Accountability Act (HIPAA)

Additional Security Measures:

- **Secure Connection:** Our platform employs TLS 1.2 encryption for all connections, ensuring the privacy and security of your data during transmission. This encryption acts as a vital barrier against eavesdroppers and hackers, who may attempt to intercept data in transit.

- **Data Encryption:** We go a step further by encrypting all data stored in the cloud using industry-standard algorithms. This layer of encryption is crucial for protecting sensitive data against potential breaches, ensuring that even in such events, your data remains accessible and secure.

- **Multi-Factor Authentication (MFA):** Access to cloud services is fortified with multi-factor authentication, a security measure requiring multiple authentication methods from independent categories of credentials. MFA ensures that only authorised personnel can access sensitive data, significantly reducing the risk of unauthorised access.

- **Data Redundancy:** To guarantee high availability and mitigate the risk of data loss, data is redundantly stored across multiple locations. This redundancy ensures that sensitive data is always accessible when needed, providing a reliable safety net against data loss scenarios.

Verification and Compliance Process

Optoma engages in a robust verification process to validate the integrity and efficacy of our security measures. This multifaceted approach ensures our products not only meet but exceed industry standards for security, offering our clients the highest assurance of data protection.

1. **Third-Party Audits:** Our products and services undergo exhaustive audits conducted by independent, third-party security firms. These evaluations are designed to identify potential vulnerabilities and assess the effectiveness of our existing security measures. The insights gained from these audits enable us to continually fortify our defences against evolving cybersecurity threats.

2. **Code Reviews:** Regular, comprehensive reviews of our codebase are a cornerstone of our security strategy. These reviews are conducted by security experts who scrutinise our code for vulnerabilities, adherence to best practices,

and overall security hygiene. This proactive measure ensures our products' resilience against known and emerging threats.

3. **Vulnerability Testing:** We employ ongoing vulnerability testing to discover and address potential security weaknesses pre-emptively. This proactive approach allows us to mitigate risks before they can be exploited, ensuring our solutions' ongoing security and reliability.

4. **Penetration Testing:** Penetration testing, or "ethical hacking," is pivotal in our verification process. Skilled security professionals simulate cyberattacks under controlled conditions to evaluate the effectiveness of our security measures. These tests help us identify and rectify vulnerabilities, enhancing our defence mechanisms against cyber threats.

(*) Applied to: Display Share, Whiteboard, My Account and OMS.

Compliance Management and Review Processes

General Data Protection Regulation (GDPR): Optoma's Product adheres to GDPR principles and prioritises safeguarding customer data, reflecting our deep commitment to privacy and data protection. If a user wishes to delete their account, our comprehensive procedure is as follows:

- **Identity Verification:** Initially, we verify the user's identity when making the deletion request. This critical step ensures the request's legitimacy, protecting against unauthorised attempts to access or alter user data.

- **Data Deletion:** Upon confirming the user's identity, we delete the user's data from our databases. This includes removing personal information, transaction history, and any other data linked to the user's account, ensuring their privacy is thoroughly respected and maintained.

- **Data Anonymisation:** When data cannot be entirely deleted due to legal or other binding obligations, we anonymise this information. By doing so, the data is stripped of any personally identifiable information, ensuring the user's privacy remains intact even when data retention is required by law.

- **Record Keeping:** We maintain a detailed record of each deletion request and the subsequent actions taken. This documentation is crucial for transparency and accountability, providing a clear audit trail in the event of regulatory inquiries or audits.

California Consumer Privacy Act (CCPA): Compliance with the CCPA reflects our dedication to safeguarding the privacy and rights of California residents, offering transparency, control, and accountability in the handling of personal information.

Product Security and Telecommunications Infrastructure (PSTI): Compliance with the PSTI Act covers the following three main security features:

- **Devices will not be allowed to have universal default passwords:** This makes it easier for consumers to configure their devices securely to prevent them being hacked by cyber criminals
- **A vulnerability disclosure policy**: This means manufacturers must have a plan for how to deal with weaknesses in software which means it's more likely that such weaknesses will be addressed properly
- **Disclose how long they will receive software updates**: This means that software updates are created and released to maintain the security of the device throughout its declared lifespan

* More detail: https://www.optomaeurope.com/company/statements/product-security-psti

ISO/IEC 27001: Optoma software solution undergo regular independent third-party audits for ISO/IEC 27001 compliance, which provides built-in initiative definitions to view a list of controls and compliance domains based on responsibility – customer, Optoma, or shared.

Compliance with ISO/IEC 27001, certified by an accredited auditor, demonstrates that Optoma uses internationally recognized processes and best practices to manage the infrastructure and organization that support and deliver its services. The certificate validates that Optoma has implemented the guidelines and general principles for initiating, implementing, maintaining, and improving the management of information security.

A Comprehensive Security Assurance

In conclusion, Optoma ensures comprehensive security by integrating robust measures across our product suite. We focus on:

- **Application Security:** Implement strong authentication and access controls, complemented by regular security assessments to safeguard applications.
- **Device Security:** Deployment of encryption, strict access controls, and data protection features to secure devices against unauthorised access.

- **Network Security:** Utilization of WPA2 and WPA3 encryption, secure transmission protocols, and VPN support to protect data during transmission.
- **Cloud Security:** Leveraging cloud security features like encryption, multi-factor authentication, and compliance with industry standards to secure data storage and processing.
- **Verification and Compliance:** Continuous security evaluations, including third-party audits and adherence to data protection regulations, ensure our commitment to maintaining high-security standards.

Our commitment to security is not just protocol; it reflects our deeply held core values of customer focus, innovation, and integrity. These guiding principles ensure that Optoma's security framework meets our partners' expectations, embedding trust and reliability at the core of your experience with us.

Copyright © Optoma 2024, Optoma and its logo is a registered trademark of Optoma Corporation and its affiliates ("Optoma"). All other product names and company names used herein are for identification purposes only and may be trademarks or registered trademarks of their respective owners other than Optoma, and Optoma disclaims any and all rights in these marks. The information contained herein is subject to change without notice.