



## DATA SHEET

# Physical Security Assessment

Bridging Physical and Digital—Security Without Gaps

## Overview

### Deliverables

- Physical Security Technical Report with Visual Observations
- Executive Summary for Senior Leadership
- Prioritized Risk and Remediation Matrix
- Optional Covert Red Team Add-On with Behavioral Analysis
- Half-Day Workshop and Debrief Presentation

### Benefits

- Evaluates physical security controls across traditional and modern digital environments.
- Assesses convergence between physical and cybersecurity postures.
- Prioritizes actionable insights for high-risk facilities and emerging threats such as insider attacks and smart-device compromise.
- Supports regulatory compliance, including NIST, ISO/IEC 27001, GDPR CISA guidance etc.
- Integrates with risk management strategies for enterprise-wide protection.

In today's rapidly evolving threat landscape, physical security remains a foundational component of an organization's overall cybersecurity and risk management strategy. Modern physical security assessments must go beyond traditional lock-and-key reviews to evaluate integration with cyber-physical systems, smart surveillance, access analytics, and IoT-based facility controls.

Trellix Guardians' Physical Security Assessment aligns with current security frameworks and threat intelligence to deliver comprehensive, proactive protection of assets, personnel, and sensitive environments.

## Our Methodology

Our Guardians consultants conduct a hybrid physical and technical assessment, beginning with stakeholder interviews and risk scoping. We then perform walkthroughs, vulnerability inspections, and control testing. Modern tools such as smart camera analytics, access logs, and biometric authentication points are reviewed in conjunction with traditional barriers and procedures.

Key areas assessed include:

- Physical Perimeter Controls (barriers, gates, lighting, CCTV)
- Facility Entry Management (biometrics, key cards, visitor controls)
- Data Center Security (environmental sensors, cage access, fire suppression)
- Internal Area Monitoring (motion detection, AI-assisted surveillance)
- Device and Asset Protection (mobile device lockdowns, asset tracking)
- Policy Adherence (physical access logs, tailgating prevention, emergency response)
- Human Factors (security awareness, social engineering resilience)



## Retesting & Continuous Improvement

We offer discounted retesting within 90 days to validate remediations and reinforce accountability. Physical security is not static — our continuous improvement approach helps evolve defenses as new threats emerge.

## The Guardians Difference

All engagements follow our Security Engagement Process (SEP) to ensure transparency, quality assurance, and alignment with business priorities. We leverage our in-house threat intelligence and industry-certified experts to deliver unmatched value.

For more information or to schedule a consultation, please contact us at [Guardians@Trellix.com](mailto:Guardians@Trellix.com)