Ilminate Platform Overview

Advanced Email Security & Threat Detection Platform

November 2025

Executive Summary

Ilminate is a comprehensive cybersecurity platform that protects organizations from the most sophisticated email threats, including automated phishing attacks, QR code phishing, brand impersonation, and zero day threats. Our multi layered detection architecture achieves 99.5% accuracy with industry leading 0.08% false positive rates—15x better than traditional security solutions.

Platform Overview

Ilminate provides enterprise grade email security through an integrated ecosystem of advanced detection engines, threat intelligence, and automated response capabilities. Our platform combines traditional security tools with advanced machine learning models to detect threats that bypass conventional defenses.

Key Capabilities

• **Automated Phishing Detection** - Industry first capability to detect ChatGPT, Claude, and Gemini generated attacks (94.7% accuracy)

• **QR Code Phishing Detection** - Advanced quishing detection with 99.7% accuracy

• **Logo Impersonation Detection** - Advanced vision analysis identifies fake brand logos (98.3% accuracy)

• **Multi Signal Risk Fusion** - Combines 6 detection layers for comprehensive threat analysis

• **Automated Triage** - Automated analysis and response in under 5 seconds

• **Zero Day Threat Detection** - Behavioral analysis and pattern recognition for unknown threats

APEX Detection Engine

The APEX (Advanced Protection & Exposure Intelligence) Detection Engine is ilminate's core threat detection system, featuring a sophisticated multi layer architecture that combines traditional security tools with advanced machine learning.

Detection Layers

Layer 0: Pre Filtering

APEX Gatekeeper provides whitelist and blacklist management, SPF, DKIM, DMARC authentication checks, and initial threat filtering

Layer 1: Traditional Scanning

APEX Malware Sentinel and APEX Threat Hunter provide malware detection, advanced threat detection, and real time threat intelligence feeds

Layer 2: Pattern Detection

APEX Pattern Shield uses custom pattern matching for malware signatures, automated email threat pattern detection, and automated rule updates

Layer 3: Feature Based Machine Learning

APEX ML Classifier uses gradient boosted decision trees, multi dimensional feature analysis, active learning capabilities, and confidence scoring

Layer 4: Deep Learning Models

APEX Phishing Hunter, APEX Threat Analyzer, APEX AI Forensics, APEX Anomaly Detector, and APEX Vision Scanner provide advanced threat detection, automated content forensics, behavioral anomaly detection, and vision analysis for image threats

Layer 4.5: Advanced Image and QR Code Scanning

APEX QR Shield provides QR code detection using multiple methods, logo impersonation detection, OCR text extraction, screenshot and UI element detection, and hidden link analysis

Detection Capabilities

Automated Phishing Detection

Identifies GPT 4 generated attacks (96.2% accuracy), detects Claude generated content (93.5% accuracy), recognizes Gemini generated threats (92.8% accuracy). Overall automated detection accuracy: 94.7%

QR Code Phishing (Quishing)

Dual method detection using multiple techniques, URL analysis and reputation checking, malicious pattern recognition. 99.7% detection accuracy

Brand Impersonation

Advanced vision model for logo detection, monitors major brands (Microsoft, Google, Apple, PayPal, Amazon, etc.), impersonation threshold detection. 98.3% accuracy

Business Email Compromise (BEC)

APEX BEC Guardian provides multi signal analysis, OSINT integration, behavioral pattern recognition, urgency and social engineering detection

Account Takeover (ATO)

APEX Breach Guardian and APEX Credential Shield provide authentication anomaly detection, login pattern analysis, geographic and temporal analysis, and multi factor authentication monitoring

Threat Intelligence Integration

APEX OSINT Intelligence, APEX Breach Guardian, APEX Domain Intelligence, APEX Dark Web Scanner, and APEX Credential Shield provide comprehensive threat intelligence from multiple sources including breach databases, domain reputation, dark web monitoring, and compromised credential detection.

Performance Metrics

- Overall Accuracy: 99.5%
- False Positive Rate: 0.08% (15x better than competitors)
- Average Scan Time: 80ms
- Threat Detection Rate: 99.5%
- Zero Day Detection: Advanced behavioral analysis

APEX Connect

APEX Connect is ilminate's advanced integration platform that makes APEX detection capabilities available to automated assistants, security tools, and automated systems. This technology enables seamless access to threat intelligence and detection analysis through a standardized Model Context Protocol (MCP) interface.

APEX Connect Capabilities

Email Threat Analysis

BEC and phishing detection with keyword heuristics, multi layer threat scoring, risk assessment and recommendations, automated triage workflows

MITRE ATT&CK; Mapping

Pattern-based technique mapping, attack framework classification, confidence scoring, tactics, techniques, and procedures (TTP) identification

Domain Reputation

Threat intelligence lookup, domain age and history analysis, reputation scoring, first seen/last seen tracking

Campaign Analysis

Active threat campaign tracking, affected domain identification, timeline analysis, technique correlation

Image Scanning

QR code detection and analysis, logo impersonation detection, hidden link extraction, OCR text analysis

Integration Architecture

APEX Connect connects to ilminate's APEX Detection Engine through a Python bridge service, providing standardized API interface, real time threat analysis, multi tenant support, audit logging and compliance, and rate limiting and security controls.

HarborSIM: Phishing Training Template Generator

HarborSIM is a serverless pipeline that transforms real phishing attacks into safe, PII-free training templates for security awareness programs. This enables organizations to use actual attack patterns in training without exposing sensitive data.

Key Features

Secure Sanitization Pipeline

PII redaction, URL and domain removal, dangerous element deweaponization, attachment scanning and flattening

Template Generation

MJML template creation, brand-safe formatting, metadata extraction, curated storage and indexing

Security Guardrails

Originals quarantined in encrypted storage, no live links, forms, or scripts in outputs, KMS encryption at rest, least privilege IAM roles

Pipeline Stages

- **Normalize** - Parse raw EML files and extract HTML content
- **Deweaponize** - Remove dangerous elements (hrefs, URLs, scripts, forms)
- **Attachments** - Scan and flatten attachments
- **PII** - Redact personally identifiable information
- **Template** - Generate final MJML template and persist to storage

MailVault: Enterprise Email Security Platform

MailVault searches and retrieves delivered messages from Microsoft 365 and Google Workspace mailboxes for security operations. The platform provides comprehensive email security capabilities including real time threat detection, automated quarantine, and complete email protection.

Core Capabilities

Message Search and Retrieval

Search and retrieve delivered messages from Microsoft 365 and Google Workspace mailboxes for security operations, incident response, and forensic analysis

Real Time Threat Detection

Multi signal risk fusion (0-100 scoring), heuristic detection, URL reputation checks, IP reputation analysis, spam analysis, malware scanning using APEX detection engines

Automated Response

Automatic quarantine (threshold: 70), risk based decision making, complete audit trail, detection reason logging, dead letter queue handling

Email Infrastructure

Microsoft Graph API integration, Google Workspace API integration, auto renewing subscriptions, multi tenant support, email authentication (SPF, DKIM, DMARC)

Risk Fusion System

MailVault uses a sophisticated multi signal risk scoring system: Heuristic Detection (finance terms +20, URL shorteners +25), URL Reputation checks, IP Reputation analysis, Spam Analysis scoring, and Malware Detection scanning. Each signal contributes a risk delta (0-100). When aggregate risk reaches threshold (default: 70), email is automatically quarantined.

Competitive Advantages

• **Automated Phishing Detection** - Only platform that detects ChatGPT, Claude, and Gemini attacks

• **QR Code Phishing Detection** - Advanced quishing detection (99.7% accuracy)

• **Logo Impersonation Detection** - Advanced vision analysis for brand protection

• **15x Better False Positive Rate** - 0.08% vs. 1-2% industry average

• **6 Detection Layers** - Most comprehensive in the industry

• **80ms Scan Time** - Fastest threat analysis available

Performance Comparison

Metric	Ilminate APEX	Industry Average
Overall Accuracy	99.5%	95-97%
False Positive Rate	0.08%	1-2%
Automated Detection	94.7%	Not Available
QR Code Detection	99.7%	<50%
Logo Detection	98.3%	Not Available
Scan Time	80ms	200-500ms

Conclusion

Ilminate provides the most advanced email security platform available, combining traditional security tools with advanced machine learning to protect against the latest threats. Our industry first capabilities in automated phishing detection, QR code analysis, and brand impersonation protection give organizations a significant advantage in the fight against cybercrime.

With 99.5% accuracy, 0.08% false positive rates, and sub 100ms response times, ilminate delivers enterprise grade protection without compromising performance or user experience.

For more information, visit ilminate.com or contact our security experts.