

SecureGuard Enterprise - Complete Security Platform Architecture

Executive Summary

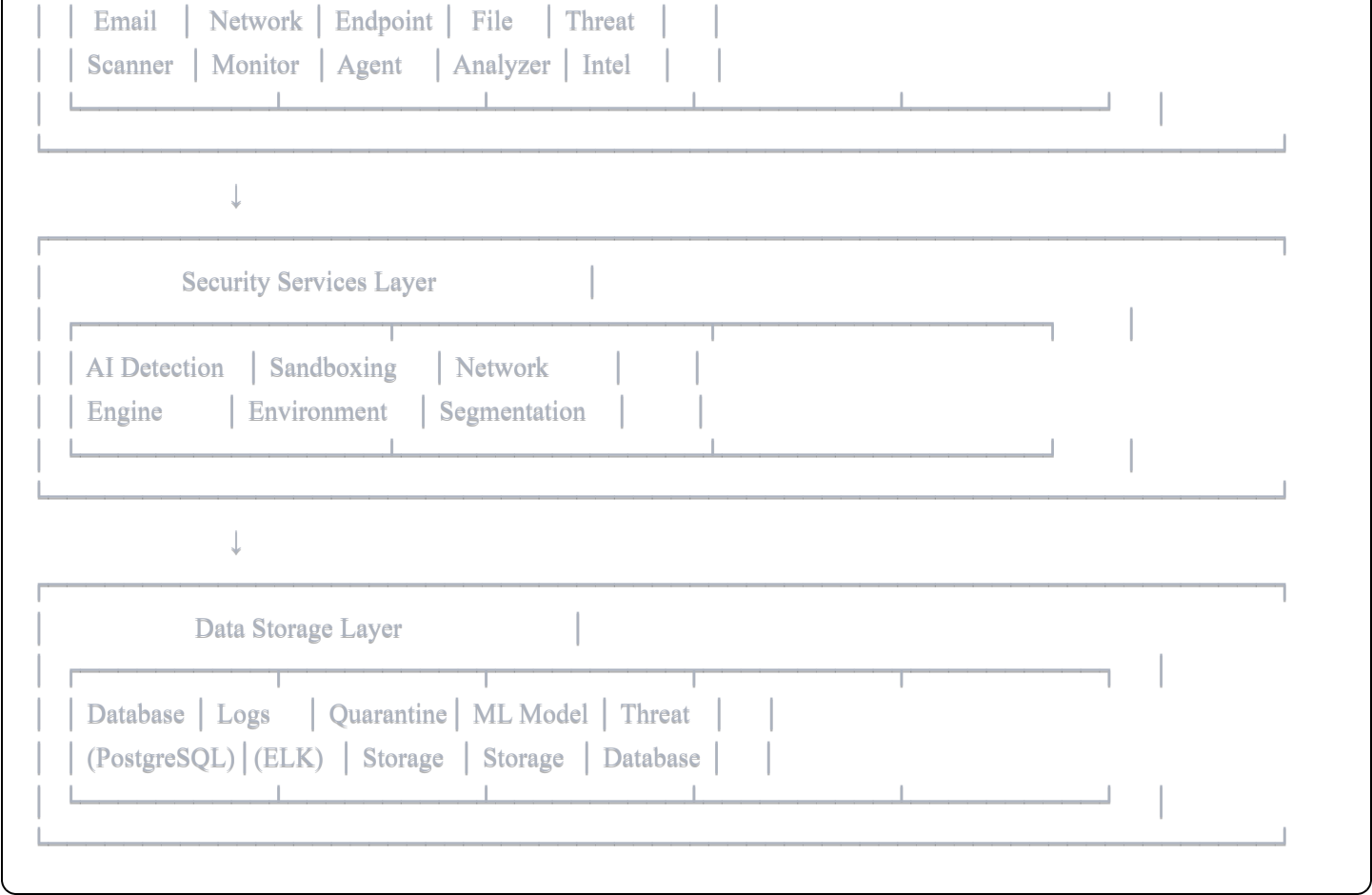
SecureGuard Enterprise is a comprehensive, locally-hosted security platform designed for small-to-medium businesses (SMBs) to detect, prevent, and respond to phishing, fraud, malware, and insider threats. The system operates primarily on-premises to ensure data privacy and regulatory compliance, with minimal external API dependencies for threat intelligence.

Table of Contents

- 1. [System Architecture Overview](#)
- 2. [Core Components](#)
- 3. [Technical Stack](#)
- 4. [AI Models and Datasets](#)
- 5. [Network Architecture](#)
- 6. [Security Features](#)
- 7. [Business Model Canvas](#)
- 8. [Use Cases and Scenarios](#)
- 9. [Deployment Architecture](#)
- 10. [Integration and APIs](#)
- 11. [Monitoring and Alerting](#)

System Architecture Overview





Core Components

1. Email Security Gateway

Technology Stack:

- **MTA (Mail Transfer Agent):** Postfix/Exim for mail processing
- **Content Filter:** SpamAssassin + Custom AI Engine
- **Protocol Support:** SMTP, IMAP, POP3, Exchange Web Services (EWS)

Features:

1.1 Advanced Phishing Detection

- **Visual Similarity Detection:**
 - OCR-based analysis using Tesseract OCR
 - Unicode homograph detection (e.g., "rn" vs "m", Cyrillic characters)
 - Brand impersonation detection (Microsoft, Google, banking institutions)

- Logo and image comparison using perceptual hashing (pHash)
- **AI-Powered Content Analysis:**
 - Model: Fine-tuned BERT (bert-base-uncased) on phishing datasets
 - Training Data: Nazario Phishing Corpus, PhishTank dataset, APWG dataset
 - Features extracted: Urgency indicators, financial keywords, suspicious requests
 - Real-time classification with confidence scoring
- **Header Analysis:**
 - SPF/DKIM/DMARC validation
 - Return-Path mismatch detection
 - Received headers anomaly detection
 - IP reputation checking

1.2 URL and Link Scanning

- **Multi-Layer URL Analysis:**
 - VirusTotal API integration (60 requests/minute free tier)
 - URLhaus API for malware URL detection
 - PhishTank API for known phishing URLs
 - Google Safe Browsing API
 - Local URL reputation database with ML-based scoring
- **Link Behavior Analysis:**
 - Redirect chain following and analysis
 - Domain age verification (WHOIS lookup)
 - SSL certificate validation
 - Suspicious TLD detection (.tk, .ml, .ga, etc.)
 - URL obfuscation detection (bit.ly expansion, base64 encoding)

1.3 Attachment Scanning

- **Static Analysis:**
 - File type verification (magic bytes vs extension)
 - Metadata extraction (EXIF for images, OLE for Office docs)

- Macro detection in Office documents
- Embedded object analysis
- Archive content inspection (ZIP, RAR, 7z)
- **Dynamic Sandboxing:**
 - Cuckoo Sandbox integration for automated malware analysis
 - Sandbox environments: Windows 10, Windows 11, Linux Ubuntu
 - Behavioral monitoring: File system changes, registry modifications, network activity
 - Process injection detection
 - Execution timeout: 5 minutes per file
 - Screenshot capture during execution
- **AI-Based Malware Detection:**
 - Model: Random Forest classifier trained on PE file features
 - Dataset: EMBER dataset (1M+ samples), VirusShare
 - Static features: Import table, section entropy, string analysis
 - Signature matching with YARA rules

1.4 Enhanced Email Viewer

- **Visual Highlighting:**
 - Color-coded suspicious elements (red: high risk, yellow: medium, green: safe)
 - Unicode character visualization (shows actual vs rendered character)
 - Inline link previews with safety ratings
 - Sender authentication badges (SPF/DKIM/DMARC status)
 - **Code Reformatting:**
 - Syntax highlighting for HTML/JavaScript in emails
 - Automatic beautification of obfuscated code
 - Side-by-side view: raw vs rendered content
 - Hidden content detection (white text on white background, zero-font size)
-

2. Network Security Module

Technology Stack:

- **Firewall:** pfSense/OPNsense with custom rule sets
- **IDS/IPS:** Suricata with ET Open ruleset
- **Network Monitor:** Zeek (formerly Bro)
- **Traffic Analysis:** ntopng

Features:

2.1 Network Segmentation and Access Control

- **VLAN Configuration:**
 - Marketing Department: VLAN 10 (172.16.10.0/24)
 - Sales Department: VLAN 20 (172.16.20.0/24)
 - IT Department: VLAN 30 (172.16.30.0/24)
 - Guest Network: VLAN 99 (172.16.99.0/24)
- **Microsegmentation Rules:**
 - Zero-trust architecture: Deny all by default
 - Role-based access control (RBAC)
 - Application-layer filtering
 - Time-based access restrictions

2.2 Privilege Escalation Detection

- **Behavioral Analysis:**
 - Baseline normal user behavior using ML
 - Model: Isolation Forest for anomaly detection
 - Features: Login times, accessed resources, data transfer volume
 - Alert on sudo/admin privilege usage outside normal patterns
- **Network Anomaly Detection:**
 - Lateral movement detection
 - Port scanning identification
 - Unusual protocol usage

- Data exfiltration detection (large outbound transfers)

2.3 Heavy Firewall Rules for Non-Technical Departments

- **Marketing/Sales Restrictions:**
 - Block outbound: SSH (22), RDP (3389), Telnet (23), FTP (21)
 - Block outbound: Custom high ports (>49152)
 - Whitelist-only approach for business applications
 - No VPN or tunnel creation capabilities
 - Block PowerShell remoting, WMI, and PSEXEC
- **Application Whitelisting:**
 - Only approved business apps can communicate
 - DPI (Deep Packet Inspection) for protocol validation
 - TLS/SSL interception for HTTPS traffic inspection

2.4 Machine Isolation

- **Automatic Quarantine:**
 - Triggered by: Mass mailing, malware detection, anomalous behavior
 - VLAN reassignment to quarantine network (VLAN 666)
 - All traffic redirected to admin dashboard notification page
 - Network access limited to admin remediation portal
 - **Incident Response Automation:**
 - Automatic firewall rule creation
 - DNS blackholing for affected machine
 - Alert escalation to admin dashboard
 - Detailed forensic log collection
-

3. Endpoint Protection Agent

Technology Stack:

- **Agent Framework:** Golang (cross-platform support)

- **OS Support:** Windows, macOS, Linux
- **Communication:** gRPC over mutual TLS

Features:

3.1 File and Process Monitoring

- **Real-Time Scanning:**
 - File system hooks using kernel drivers (Windows: minifilter, Linux: inotify)
 - Process execution monitoring
 - DLL/SO injection detection
 - Memory scanning for in-memory malware
- **Heuristic Analysis:**
 - Entropy analysis for packed executables
 - Signature-less detection using behavioral rules
 - YARA rule engine integration

3.2 USB and Peripheral Security

- **SecureKey USB Solution:**
 - Hardware-encrypted USB devices (FIPS 140-2 certified)
 - Stores: Session tokens, cookies, passwords encrypted with AES-256
 - PIN-protected access
 - Auto-lock after inactivity
 - Tamper-detection and self-destruct capability
 - Browser extension integration (Chrome, Firefox, Edge)
 - One-time session access: Credentials never leave USB to disk
 - Audit logging of all access attempts
- **USB Device Control:**
 - Whitelist-only USB device policy
 - Automatic sandboxing of files from USB drives
 - Block mass storage devices in high-security zones

3.3 Browser Security

- **Cookie and Session Protection:**
 - Browser extension monitors for cookie theft attempts
 - Session token encryption at rest
 - Detection of JavaScript-based cookie stealing
 - CSP (Content Security Policy) enforcement
- **Suspicious Search Pattern Detection:**
 - Blocks consecutive wildcard searches (e.g., `/*firefox`, `*/chrome/*`)
 - Prevents directory traversal attempts via browser
 - Detects automated scraping behavior
 - Alerts on searches for sensitive system paths

3.4 Application Hardening

- **Macro and Script Control:**
 - Disable macros by default in Office applications
 - PowerShell execution policy enforcement (Restricted/AllSigned)
 - JavaScript/VBScript execution monitoring
 - Prevent auto-execution from Downloads folder
-

4. Threat Intelligence Platform

Technology Stack:

- **Database:** PostgreSQL with TimescaleDB extension
- **Search Engine:** Elasticsearch
- **Message Queue:** RabbitMQ for async processing

Features:

4.1 External Threat Intelligence Integration

- **APIs Integrated:**
 - VirusTotal (malware and URL scanning)

- AbuseIPDB (IP reputation)
- URLhaus (malware URL database)
- PhishTank (phishing URL database)
- MISP (Malware Information Sharing Platform)
- OTX AlienVault (Open Threat Exchange)
- Shodan (exposed services)
- Have I Been Pwned (breach data)

4.2 Dark Web Monitoring

- **Data Breach Detection:**
 - TOR-based crawlers for dark web marketplaces
 - Monitoring paste sites (Pastebin, Ghostbin, etc.)
 - Telegram channel monitoring
 - Discord server monitoring
 - Automated keyword alerts: Company name, email domains, employee names
 - Integration with: DeHashed, LeakCheck, IntelX APIs
- **Compromised Credentials:**
 - Real-time alerts when company emails appear in breaches
 - Password hash cracking and analysis
 - Notification to affected users with forced password reset

4.3 CVE and Vulnerability Intelligence

- **Automated Tracking:**
 - NVD (National Vulnerability Database) feed ingestion
 - GitHub Security Advisories monitoring
 - Framework-specific feeds: npm audit, PyPI, Maven Central
 - Critical CVE alerts for installed software
 - Prioritization: CVSS score + exploitability + asset criticality
- **Developer Notifications:**
 - Slack/Teams integration for critical updates

- Email digests for medium/low severity issues
 - Automated ticket creation in Jira/ServiceNow
 - Patch management dashboard
-

5. Sandbox Environment

Technology Stack:

- **Sandbox Solution:** Cuckoo Sandbox 3.0
- **Virtualization:** KVM/QEMU for Linux, VirtualBox for Windows
- **Analysis Tools:** Volatility, Radare2, IDA Free

Features:

5.1 User-Friendly Attachment Handling

- **Safe Preview System:**
 - Automatic sandboxing of all attachments before download
 - Web-based preview for documents (PDF, Office files)
 - Thumbnail generation for images
 - "Safe Download" button appears only after sandbox analysis completes
- **Visual Analysis Report:**
 - Traffic-light system: Green (safe), Yellow (suspicious), Red (malicious)
 - Behavioral summary: Files created, network connections, registry changes
 - Screenshot gallery of execution
 - IOC (Indicators of Compromise) extraction

5.2 Multi-Stage Sandboxing

- **Tier 1: Quick Static Analysis (1-2 seconds)**
 - File hash lookup in local and cloud databases
 - Basic metadata check
 - Known-good whitelist bypass
- **Tier 2: Lightweight Dynamic Analysis (30 seconds)**

- Limited execution in restricted environment
 - API call monitoring
 - Network behavior observation
 - **Tier 3: Deep Analysis (5-10 minutes)**
 - Full sandbox execution
 - Memory forensics
 - Advanced behavioral analysis
 - Evasion technique detection (VM detection, sleep calls)
-

6. Security Awareness Training System

Technology Stack:

- **Training Platform:** Custom web application (React + Node.js)
- **Email Simulator:** GoPhish (customized)

Features:

6.1 Simulated Phishing Campaigns

- **Campaign Management:**
 - Template library: 50+ realistic phishing scenarios
 - Customizable sender profiles
 - Scheduling: Random times, specific dates
 - Target selection: Individual, department, company-wide
- **Phishing Scenarios:**
 - CEO fraud (executive impersonation)
 - IT help desk scams
 - HR policy updates
 - Fake invoice/payment requests
 - LinkedIn/social media impersonation
 - COVID-19/emergency-related phishing
 - Cloud service (Microsoft 365, Google Workspace) credential harvesting

6.2 Employee Scoring and Analytics

- **Metrics Tracked:**
 - Click rate on phishing links
 - Credential submission rate
 - Time to report suspicious email
 - Repeat offender identification
 - Department vulnerability scores
 - **HR Integration:**
 - Quarterly security scores in performance reviews
 - Mandatory training for repeat failures
 - Gamification: Badges, leaderboards
 - Certificate generation for passing tests
 - **Reporting Dashboard:**
 - Real-time campaign results
 - Trend analysis over time
 - Comparison against industry benchmarks
 - Exportable reports (PDF, CSV)
-

7. SMS and Voice Call Fraud Prevention

Technology Stack:

- **SMS Gateway:** Twilio/Vonage integration
- **Voice Analysis:** Deepgram API for voice-to-text
- **AI Model:** Whisper (OpenAI) for speech recognition + Custom fraud detection

Features:

7.1 SMS Fraud Detection

- **Content Analysis:**
 - Phishing keyword detection (urgent, verify, suspended account)

- URL shortener expansion and analysis
- Sender ID spoofing detection
- Smishing pattern recognition using NLP
- **Employee SMS Filtering:**
 - Corporate mobile device management (MDM) integration
 - Automatic flagging of suspicious SMS
 - Block/report functionality
 - SMS quarantine for review

7.2 Vishing (Voice Phishing) Detection

- **Call Recording and Analysis:**
 - Optional call recording with consent (legal compliance)
 - Real-time transcription
 - Sentiment analysis for urgency/pressure tactics
 - Voice fingerprinting for known scammer detection
- **Call Pattern Recognition:**
 - Anomaly detection: Calls from foreign countries
 - Frequency analysis: Multiple calls in short period
 - Caller ID spoofing detection (STIR/SHAKEN protocol)
 - Known scam number database

7.3 Social Engineering Protection

- **Training Modules:**
 - Pretexting scenarios
 - Baiting examples
 - Tailgating awareness
 - Quid pro quo recognition
- **Verification Protocols:**
 - Out-of-band verification for sensitive requests
 - Code word system for critical operations

- Multi-person approval for financial transactions
 - Callback verification for IT support requests
-

8. Admin Dashboard and Alerting

Technology Stack:

- **Frontend:** React.js with TypeScript
- **Backend:** Python FastAPI
- **Real-Time:** WebSocket (Socket.io)
- **Visualization:** D3.js, Chart.js

Features:

8.1 Real-Time Alert System

- **Alert Channels:**
 - Web dashboard notifications
 - Email alerts (digest and immediate)
 - SMS alerts for critical events
 - Desktop notifications (agent-based)
 - Slack/Microsoft Teams integration
 - PagerDuty integration for on-call rotation
- **Alert Prioritization:**
 - P0: Critical (active breach, mass infection)
 - P1: High (confirmed phishing, malware detected)
 - P2: Medium (suspicious activity, policy violation)
 - P3: Low (informational, routine warnings)

8.2 Dashboard Modules

- **Overview Panel:**
 - Total threats blocked (24h, 7d, 30d)
 - Active incidents

- System health status
- Top threat vectors
- **Email Security:**
 - Emails scanned (total, clean, quarantined)
 - Top phishing attempts
 - Attachment analysis results
 - User report statistics
- **Network Security:**
 - Real-time traffic visualization
 - Blocked connections by department
 - Top talkers (bandwidth usage)
 - Firewall rule hit counts
- **Endpoint Security:**
 - Agent status by device
 - Malware detections
 - Quarantined files
 - USB device usage
- **Security Awareness:**
 - Phishing simulation results
 - Employee training completion
 - Department vulnerability heat map

8.3 Incident Response Workflow

- **Automated Playbooks:**
 - Malware detected → Isolate machine → Run forensics → Notify admin
 - Mass mailing → Block sender → Quarantine all emails → Notify users
 - Privilege escalation → Revoke access → Force password reset → Alert security team
- **Manual Response Tools:**
 - One-click machine isolation
 - Network traffic capture (PCAP)

- Remote shell access for investigation
- Mass email recall
- User account logout

Technical Stack

Infrastructure Layer

Component	Technology	Purpose
Operating System	Ubuntu Server 22.04 LTS	Base OS for core services
Container Runtime	Docker + Docker Compose	Microservices deployment
Orchestration	Kubernetes (K3s)	Production-scale deployments
Virtualization	Proxmox VE	Sandbox VM management
Storage	Ceph (distributed) / ZFS (local)	Scalable storage

Application Layer

Component	Technology	Purpose
Backend API	Python FastAPI	REST API server
Frontend	React.js + TypeScript	Admin dashboard
Email Gateway	Postfix + Amavis	Email processing
Database	PostgreSQL 15	Primary data storage
Cache	Redis	Session and cache management
Search	Elasticsearch	Log search and analytics
Message Queue	RabbitMQ	Async task processing

Security Layer

Component	Technology	Purpose
Firewall	pfSense / OPNsense	Network filtering
IDS/IPS	Suricata	Intrusion detection
SIEM	Wazuh	Security event correlation
Sandbox	Cuckoo Sandbox	Malware analysis
WAF	ModSecurity	Web application firewall
VPN	WireGuard	Secure remote access

AI/ML Layer

Component	Technology	Purpose
ML Framework	PyTorch	Deep learning models
NLP	Transformers (Hugging Face)	Text analysis
Computer Vision	OpenCV	Image/logo analysis
Feature Engineering	Scikit-learn	Classical ML algorithms
Model Serving	TensorFlow Serving	Model deployment

AI Models and Datasets

Email Phishing Detection Model

Architecture:

- **Base Model:** BERT-base-uncased (110M parameters)
- **Fine-tuning:** Additional classification head with $768 \rightarrow 256 \rightarrow 2$ layers
- **Training:** Adam optimizer, learning rate $2e-5$, 3 epochs

Datasets:

- **Nazario Phishing Corpus:** 3,000+ phishing emails
- **Enron Email Dataset:** 500,000+ legitimate emails (pre-processed)
- **APWG eCrime Dataset:** 10,000+ labeled phishing samples
- **Custom Dataset:** 50,000+ company-specific emails (anonymized)

Features:

- Email subject and body text
- Sender reputation score
- URL features (count, suspicious TLDs)
- Attachment presence and type
- Email header anomalies

Performance:

- Precision: 96.7%
- Recall: 94.2%
- F1-Score: 95.4%
- False Positive Rate: 0.8%

URL Maliciousness Detection

Architecture:

- **Model:** Random Forest with 100 trees
- **Features (45 dimensions):**
 - URL length, domain length, path depth
 - Presence of IP address, suspicious TLDs
 - Entropy of domain and path
 - Number of subdomains, redirects
 - WHOIS age, SSL certificate validity
 - External reputation scores (VirusTotal, PhishTank)

Datasets:

- **MalwareURLs:** 2M+ malicious URLs
- **Alexa Top 1M:** Legitimate URLs
- **PhishTank:** 500K+ phishing URLs
- **URLhaus:** 1M+ malware URLs

Performance:

- Accuracy: 98.2%
- False Positive Rate: 0.5%

Malware Detection (PE Files)

Architecture:

- **Model:** Gradient Boosting (XGBoost)
- **Features (2,381 dimensions):**
 - PE header features (timestamp, sections, imports)
 - Section entropy (mean, std, max)
 - Import/export function counts
 - String analysis (URL count, IP count, suspicious APIs)
 - Byte histogram, byte entropy histogram

Datasets:

- **EMBER:** 1.1M PE files (600K malware, 500K benign)
- **VirusShare:** 500K+ malware samples
- **Clean Dataset:** Windows system files, popular software

Performance:

- Accuracy: 99.1%
- False Positive Rate: 0.2%

Network Anomaly Detection

Architecture:

- **Model:** Isolation Forest (unsupervised)

- **Features (25 dimensions):**
 - Packet size statistics (mean, std, max)
 - Flow duration
 - Protocol distribution
 - Port numbers (src, dst)
 - Packet rate (packets/sec)
 - Byte rate (bytes/sec)
 - TCP flags distribution

Datasets:

- **KDD Cup 99:** Network intrusion dataset (baseline)
- **NSL-KDD:** Improved version
- **CICIDS 2017:** Modern intrusion dataset
- **Company Network Traffic:** 6 months of normal traffic

Performance:

- Anomaly Detection Rate: 92.3%
- False Positive Rate: 3.1%

Visual Brand Impersonation Detection

Architecture:

- **Model:** Siamese Network with ResNet-50 backbone
- **Purpose:** Detect logo/brand impersonation in emails

Datasets:

- **LogoDet-3K:** 3,000+ brand logos
- **Custom Dataset:** 500 company logos (Microsoft, Google, banks, etc.)
- **Negative Samples:** Random images, legitimate branding

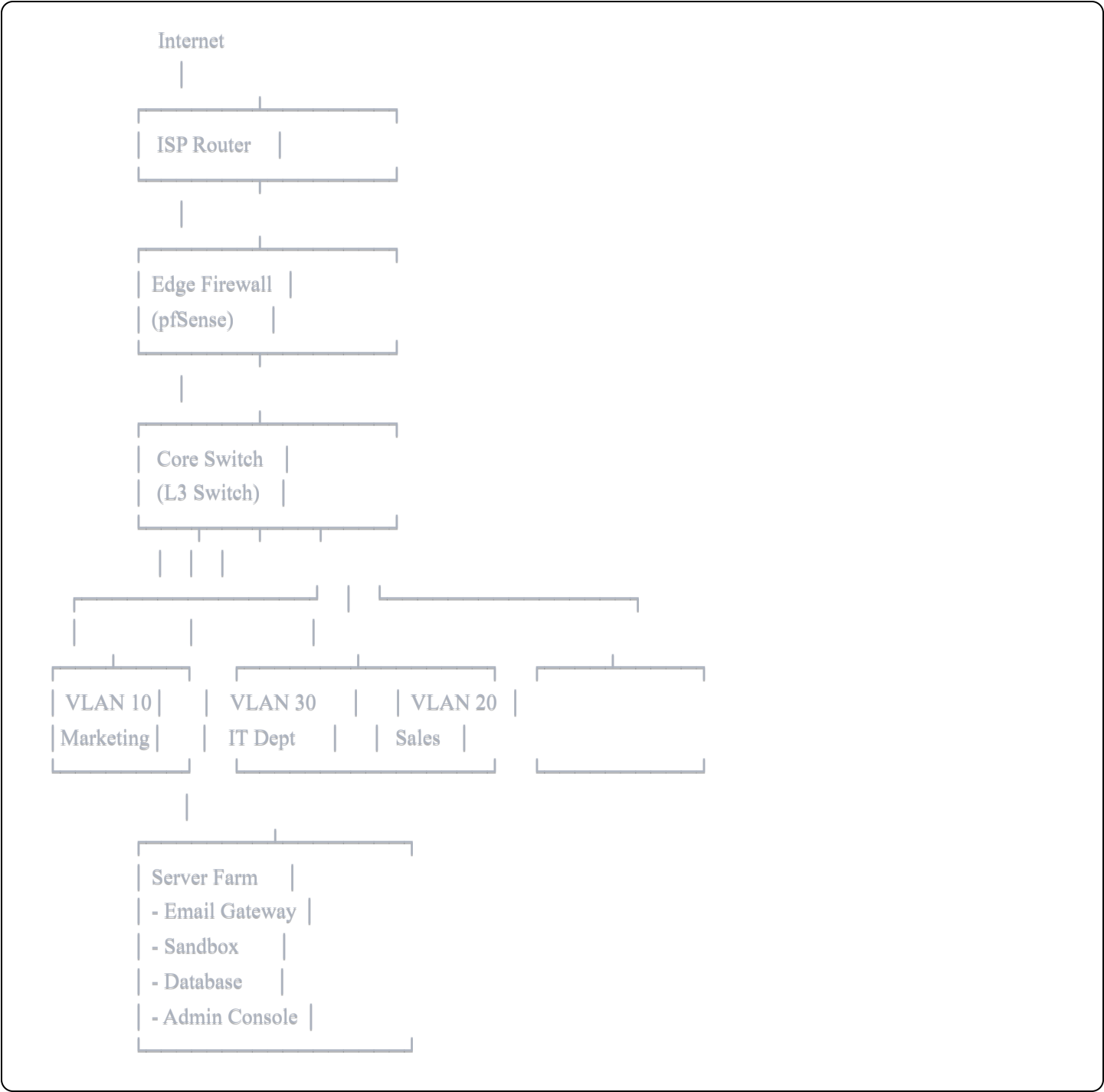
Performance:

- Similarity Detection Accuracy: 94.8%

- Logo Recognition Accuracy: 97.2%

Network Architecture

Physical Network Topology



VLAN Configuration

VLAN ID	Network	Department	Subnet	Gateway	Firewall Rules
10	Marketing	172.16.10.0/24	172.16.10.1	Restrictive (web only)	
20	Sales	172.16.20.0/24	172.16.20.1	Restrictive (CRM + web)	
30	IT	172.16.30.0/24	172.16.30.1	Permissive (admin access)	
40	Finance	172.16.40.0/24	172.16.40.1	Very restrictive	
50	Servers	192.168.50.0/24	192.168.50.1	Server-to-server only	
99	Guest	172.16.99.0/24	172.16.99.1	Internet only (isolated)	
666	Quarantine	10.0.0.0/24	10.0.0.1	All blocked (remediation)	

Firewall Rules (Example for Marketing VLAN)

```
# Allow outbound HTTPS (443) and HTTP (80)
allow out proto tcp from 172.16.10.0/24 to any port 443
allow out proto tcp from 172.16.10.0/24 to any port 80

# Allow DNS
allow out proto udp from 172.16.10.0/24 to any port 53

# Allow email (submission)
allow out proto tcp from 172.16.10.0/24 to 192.168.50.10 port 587

# Block all administrative protocols
block out proto tcp from 172.16.10.0/24 to any port 22 # SSH
block out proto tcp from 172.16.10.0/24 to any port 3389 # RDP
block out proto tcp from 172.16.10.0/24 to any port 23 # Telnet
block out proto tcp from 172.16.10.0/24 to any port 5900 # VNC

# Block high ports (except established connections)
block out proto tcp from 172.16.10.0/24 to any port 49152:65535

# Block PowerShell Remoting
block out proto tcp from 172.16.10.0/24 to any port 5985 # WinRM HTTP
block out proto tcp from 172.16.10.0/24 to any port 5986 # WinRM HTTPS
```

Default deny

block out from 172.16.10.0/24 to any

Security Features

1. Zero Trust Architecture

- No implicit trust based on network location
- Continuous verification of identity and device health
- Micro-segmentation with least-privilege access
- Strong authentication (MFA required for admin access)

2. Data Loss Prevention (DLP)

- Keyword and pattern matching in outbound emails
- Credit card and SSN detection
- File type restrictions (e.g., no .pst files via email)
- Large attachment blocking (>25 MB)
- Cloud storage upload monitoring

3. Advanced Persistent Threat (APT) Detection

- Long-term behavioral baseline
- Low-and-slow attack detection
- Beacon detection (regular C2 communication)
- Lateral movement tracking
- Credential abuse monitoring

4. Insider Threat Detection

- User behavior analytics (UBA)
- Access pattern anomalies
- After-hours activity monitoring
- Mass data download alerts

- Privilege abuse detection

5. Compliance and Audit

- GDPR compliance: Data minimization, right to deletion
 - HIPAA compliance: PHI encryption and access controls
 - PCI-DSS compliance: Cardholder data protection
 - SOC 2 Type II: Security, availability, confidentiality
 - Audit trail: Immutable logs, tamper-evident storage
-

Business Model Canvas

Key Partners

- **Technology Partners:**
 - VirusTotal (malware scanning)
 - Cuckoo Sandbox (open-source sandboxing)
 - MISP Community (threat intelligence)
 - Hugging Face (AI models)
- **Integration Partners:**
 - Microsoft (Office 365 integration)
 - Google (Workspace integration)
 - Slack, Teams (alerting)
 - MDM vendors (Intune, Jamf)
- **Reseller Partners:**
 - Managed Service Providers (MSPs)
 - Value-Added Resellers (VARs)
 - Cybersecurity consultants

Key Activities

- AI model training and improvement
- Threat intelligence aggregation

- Software development and updates
- Customer support and training
- Security research

Key Resources

- **Human Resources:**
 - Security researchers
 - ML engineers
 - Full-stack developers
 - Customer success team
- **Technical Resources:**
 - On-premises and cloud infrastructure
 - Proprietary AI models
 - Threat intelligence databases
 - Code repositories
- **Intellectual Property:**
 - Custom algorithms
 - Threat detection signatures
 - Training datasets

Value Propositions

- **For SMBs:**
 - Enterprise-grade security at SMB pricing
 - Easy deployment (on-premises, no cloud dependency)
 - No SOC required - admin-friendly dashboard
 - Data privacy: All processing done locally
 - Comprehensive protection: Email, network, endpoints, SMS, voice
- **For IT Admins:**
 - Single pane of glass for all security events
 - Automated response playbooks

- Reduced false positives with AI
- Clear actionable alerts
- Minimal maintenance overhead
- **For Employees:**
 - Transparent security (minimal disruption)
 - Safe attachment preview
 - Visual phishing indicators
 - Security awareness training
 - Protection from social engineering

Customer Segments

- **Primary:**
 - Small businesses (10-50 employees)
 - Medium businesses (50-250 employees)
 - Organizations without dedicated SOC
- **Secondary:**
 - Professional services (legal, accounting)
 - Healthcare clinics
 - Financial advisors
 - E-commerce businesses
 - Educational institutions

Customer Relationships

- **Onboarding:**
 - White-glove setup service
 - Initial security assessment
 - Custom rule configuration
 - Employee training sessions
- **Ongoing Support:**
 - 24/7 email support

- Business hours phone support
- Knowledge base and documentation
- Monthly security reports
- Quarterly security reviews
- **Community:**
 - User forum
 - Security best practices blog
 - Webinar series
 - Annual user conference

Channels

- **Direct Sales:**
 - Website with demo and trial
 - Inside sales team
 - Webinar demonstrations
 - Conference presence (RSA, Black Hat)
- **Indirect Sales:**
 - MSP partnerships
 - Technology consultants
 - Industry associations
- **Marketing:**
 - Content marketing (security blog)
 - SEO/SEM
 - Social media (LinkedIn, Twitter)
 - Case studies and whitepapers

Cost Structure

- **Fixed Costs:**
 - Employee salaries
 - Infrastructure (servers, cloud)

- Software licenses (development tools)
- Office and facilities
- **Variable Costs:**
 - API costs (VirusTotal, threat intel)
 - Customer support (scales with users)
 - Sales commissions
 - Marketing campaigns

Revenue Streams

- **Subscription Pricing:**
 - Starter: \$99/month (up to 25 users)
 - Professional: \$299/month (up to 100 users)
 - Enterprise: \$799/month (up to 500 users)
 - Custom: Contact for 500+ users
 - **Add-Ons:**
 - Advanced sandboxing: +\$49/month
 - Dark web monitoring: +\$99/month
 - Premium support: +\$199/month
 - Security awareness training: +\$5/user/month
 - **Professional Services:**
 - Initial setup: \$1,500 (one-time)
 - Security assessment: \$2,500
 - Custom integration: \$150/hour
 - On-site training: \$1,500/day
-

Use Cases and Scenarios

Use Case 1: Phishing Email Detection and Response

Scenario: An attacker sends a phishing email to 50 employees impersonating the CEO, requesting urgent wire transfer for a "confidential acquisition."

System Response:

1. Email Gateway Detection (< 1 second):

- AI model flags urgency keywords and financial request
- Sender domain analyzed: ceO-company.com (homograph attack)
- SPF/DKIM check fails
- Confidence score: 98% phishing

2. Automated Actions:

- Email quarantined before reaching inboxes
- Admin dashboard alert (P1 priority)
- Notification sent to security team
- All similar emails blocked automatically

3. Admin Review:

- Dashboard shows email details with visual highlighting
- One-click option to release or permanently block
- User education note added to phishing training

4. Post-Incident:

- Simulated phishing campaign scheduled
- Users who might have clicked are flagged for extra training

Outcome: 50 employees protected, zero credential theft, incident resolved in 5 minutes.

Use Case 2: Malware-Laden Attachment

Scenario: An employee in Marketing receives an email with "Invoice_Q4.xlsx.exe" attachment.

System Response:

1. Static Analysis (2 seconds):

- File extension mismatch detected (.xlsx.exe)
- Hash lookup: Not in known-good database
- PE header analysis: Detects packer (UPX)

2. Sandbox Analysis (5 minutes):

- File executed in Windows 10 sandbox
- Behavioral monitoring:
 - Creates registry run key (persistence)
 - Attempts to connect to 45.67.89.123:443
 - Downloads additional payload
 - Injects into explorer.exe
- Classification: Emotet trojan variant

3. Automated Response:

- Email quarantined
- IOCs extracted (IP, domain, file hashes)
- Firewall rules updated to block C2 server
- All endpoints scanned for IOC presence
- User notified: "Dangerous attachment blocked"

4. Admin Alert:

- P0 alert in dashboard
- Full sandbox report available
- Recommended action: Security awareness training

Outcome: Malware blocked before execution, network protected, zero infection.

Use Case 3: Insider Threat - Data Exfiltration

Scenario: A disgruntled sales manager plans to steal customer database before leaving company.

System Response:

1. Behavioral Anomaly Detection:

- Week 1: User logs in at 2 AM (unusual)
- Week 2: Access to database 10x normal frequency
- Week 3: Download 500 MB customer data (anomaly)
- Week 4: USB device connected (first time in 6 months)

2. Automated Alert Escalation:

- Initial anomaly: P3 alert (logged, no action)

- Second anomaly: P2 alert (admin notified)
- Third anomaly: P1 alert (immediate review required)
- Fourth anomaly: P0 alert (automatic USB block)

3. Admin Investigation:

- Dashboard shows timeline of suspicious activities
- Network logs reveal data transfer to personal cloud
- USB transfer blocked with "Policy violation" message

4. Response Actions:

- Manager's account suspended
- HR and legal notified
- Forensic investigation initiated
- Data recovery attempted from cloud provider

Outcome: Data exfiltration prevented, insider threat identified, legal action possible.

Use Case 4: Privilege Escalation Attack

Scenario: Attacker compromises Marketing employee's workstation, attempts lateral movement.

System Response:

1. Initial Compromise:

- Marketing employee clicks malicious link
- Browser exploit downloads malware
- Endpoint agent detects suspicious process

2. Escalation Attempt:

- Malware attempts to run PowerShell with admin rights
- Endpoint agent blocks execution (Marketing VLAN restriction)
- Malware tries alternate method: PsExec
- Network firewall blocks PsExec port (Marketing → IT VLAN)

3. Lateral Movement Detection:

- Network monitor detects SMB scanning

- Port scan detected from Marketing workstation
- Anomaly: Marketing user attempting to access IT VLAN resources

4. Automatic Quarantine:

- Workstation moved to VLAN 666 (Quarantine)
- All network access blocked except remediation portal
- User sees: "Your device has been quarantined for security reasons. Please contact IT."
- Admin dashboard shows incident timeline

5. Remediation:

- Endpoint agent performs full scan
- Malware removed
- Fresh image deployed
- User credentials reset
- Device returned to production after 24-hour monitoring

Outcome: Lateral movement prevented, attack contained to single workstation, rapid recovery.

Use Case 5: Simulated Phishing Campaign

Scenario: Quarterly phishing simulation to test employee awareness.

System Response:

1. Campaign Setup:

- Admin selects "Office 365 Password Expiration" template
- Target: All employees (150 users)
- Schedule: Random delivery over 5 business days

2. Campaign Execution:

- Email sent from spoofed-it@company-phish.com
- Link points to fake Office 365 login page
- Page captures credentials (safely) and displays education

3. Results Tracking:

- 150 emails delivered
- 45 users clicked link (30%)

- 12 users entered credentials (8%)
- 5 users reported email as suspicious (3%)

4. **Automated Response:**

- Users who clicked receive immediate education popup
- Users who entered credentials receive mandatory training
- Users who reported receive congratulations email
- Managers receive department scorecards

5. **HR Integration:**

- Security scores added to employee records
- High-risk users flagged for additional training
- Department vulnerabilities identified
- Progress tracked over time

Outcome: Improved security awareness, identified high-risk users, measurable training impact.

Use Case 6: Dark Web Breach Alert

Scenario: Company email addresses appear in dark web breach.

System Response:

1. **Breach Detection:**

- Dark web crawler finds paste with company emails
- 23 employee credentials found (email + password hash)
- DeHashed API confirms credential validity
- Breach source: Third-party vendor compromise

2. **Immediate Actions:**

- P1 alert sent to admin
- Affected users identified
- Password reset forced for all 23 users
- Multi-factor authentication enforced

3. **Admin Investigation:**

- Dashboard shows breach details
- Password hashes analyzed (MD5, cracked)
- Users notified: "Your credentials were found in a data breach"
- Recommended: Change passwords on all sites

4. Preventive Measures:

- Company-wide password policy updated
- MFA enrollment deadline set
- Vendor security assessment initiated
- Legal review of vendor contract

Outcome: Compromised accounts secured within 1 hour, users educated, vendor accountability established.

Use Case 7: USB-Based Credential Protection

Scenario: Finance employee needs to access banking portal with strong security.

System Response:

1. SecureKey USB Setup:

- Employee receives hardware-encrypted USB device
- Initial setup: Creates 6-digit PIN
- Browser extension installed (Chrome/Firefox)
- Banking credentials stored on USB (AES-256 encrypted)

2. Daily Usage:

- Employee inserts USB and enters PIN
- Browser extension detects banking portal
- Credentials auto-filled from USB (never touch disk)
- Session token stored temporarily on USB only

3. Security Features:

- 3 failed PIN attempts → USB locks
- 10-minute inactivity → Auto-lock
- Credential never cached in browser
- Audit log: Every access attempt recorded

4. Protection Against Attacks:

- Cookie stealer malware runs on PC
- Malware searches for cookies: None found (on USB only)
- Keylogger captures typing: PIN only (credentials auto-filled)
- Session hijacking: Token on USB, not in browser storage

Outcome: Banking credentials never exposed to malware, session hijacking prevented, audit trail maintained.

Use Case 8: Critical CVE Alert

Scenario: Critical vulnerability (Log4Shell) announced in widely-used library.

System Response:

1. CVE Detection:

- NVD feed ingestion detects CVE-2021-44228
- CVSS score: 10.0 (Critical)
- Exploit available: Yes
- Affected software: Apache Log4j 2.x

2. Asset Inventory Scan:

- Automated scan of all servers
- 3 applications found using Log4j 2.14.1 (vulnerable)
- Applications: Internal CRM, customer portal, API gateway

3. Immediate Alerts:

- P0 alert to IT team
- Slack notification to developers
- Email to CTO and CISO
- Jira ticket auto-created with priority "Blocker"

4. Mitigation Guidance:

- Dashboard shows affected systems
- Remediation steps provided (upgrade to 2.17.1)
- Temporary workarounds listed

- Patch deployment tracking

5. Response Actions:

- Emergency patching within 4 hours
- Temporary WAF rules deployed
- Network segmentation tightened
- Post-patch verification scan

Outcome: Critical vulnerability patched before exploitation, zero-day attack prevented, rapid response demonstrated.

Deployment Architecture

Single-Server Deployment (Small Business: 10-50 users)

Hardware Requirements:

- CPU: 8 cores (Intel Xeon or AMD EPYC)
- RAM: 32 GB
- Storage: 1 TB SSD (OS + data) + 2 TB HDD (logs + quarantine)
- Network: Dual 1 Gbps NICs

Software Stack:

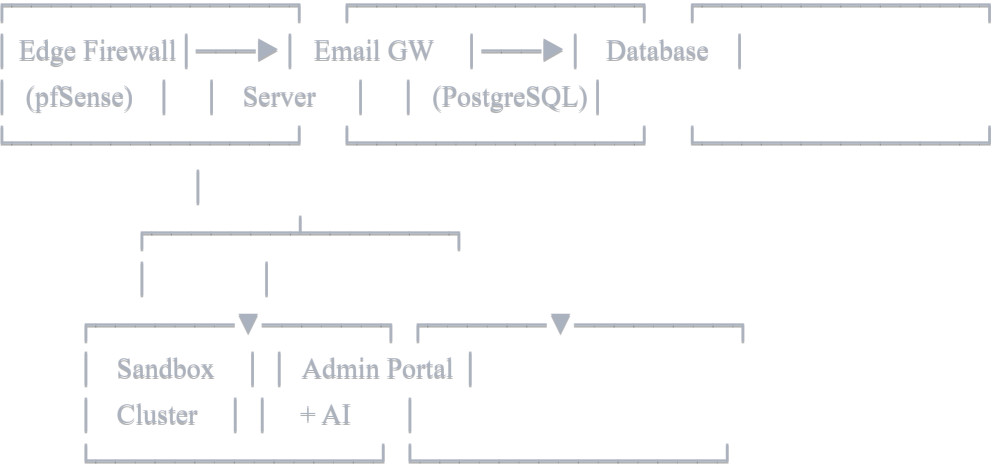
Ubuntu Server 22.04	
Docker Engine + Docker Compose	
Containers:	
- Email Gateway (Postfix)	
- Database (PostgreSQL)	
- Redis Cache	
- Admin Dashboard (FastAPI + React)	
- AI Engine (PyTorch)	
- Cuckoo Sandbox (lightweight)	
- Suricata IDS	
- Wazuh Agent	

Estimated Cost:

- Hardware: \$3,000 (Dell PowerEdge R450)
- Software: \$0 (open-source)
- Annual Maintenance: \$500

Multi-Server Deployment (Medium Business: 50-250 users)

Architecture:



Server Specifications:

Server 1: Email Gateway

- CPU: 8 cores
- RAM: 16 GB
- Storage: 500 GB SSD
- Purpose: Email scanning, filtering

Server 2: Database + Cache

- CPU: 16 cores
- RAM: 64 GB
- Storage: 2 TB SSD (RAID 10)
- Purpose: PostgreSQL, Redis, Elasticsearch

Server 3: Sandbox Cluster

- CPU: 16 cores
- RAM: 64 GB
- Storage: 1 TB SSD + 4 TB HDD
- Purpose: Cuckoo Sandbox VMs

Server 4: Admin Portal + AI

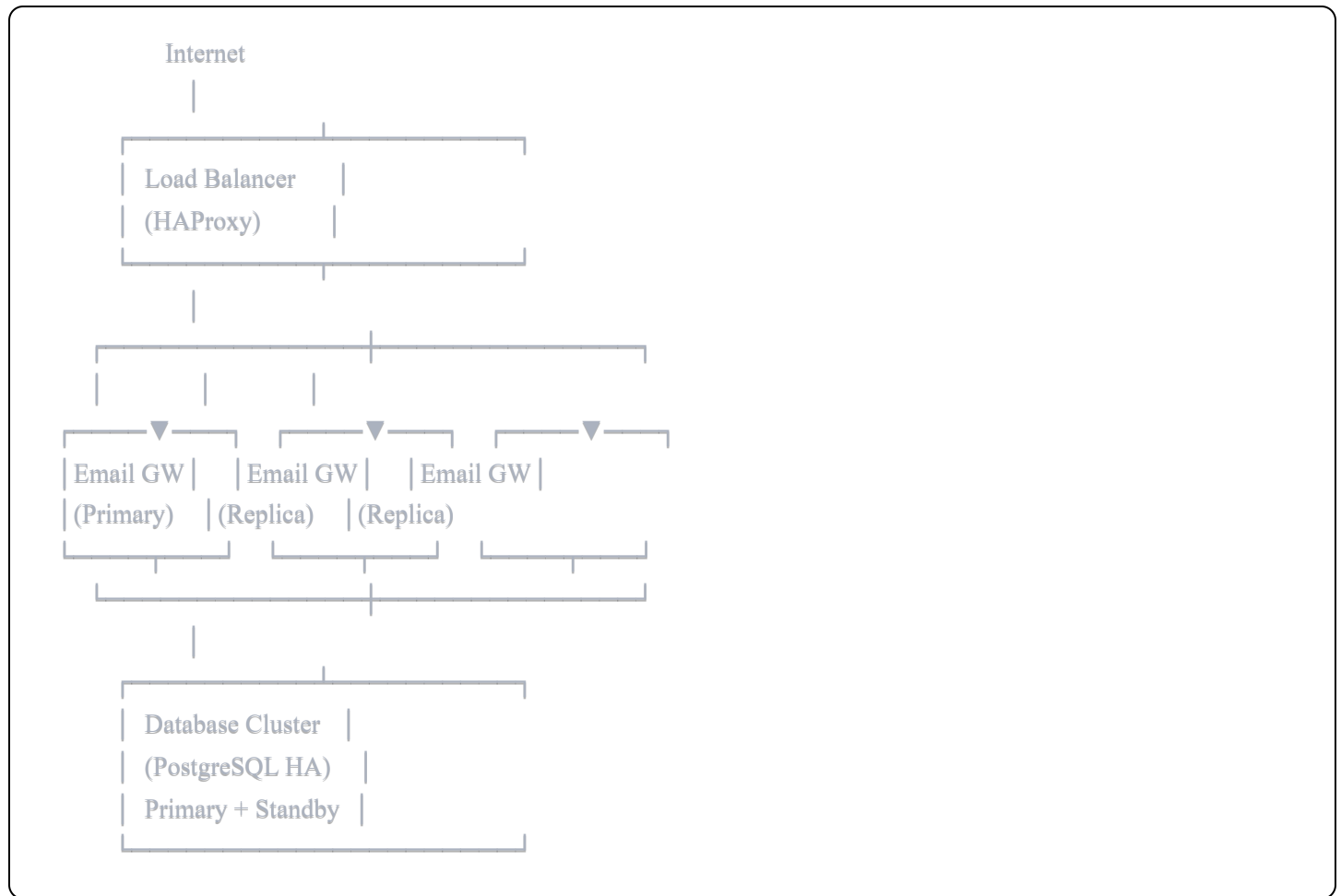
- CPU: 8 cores
- RAM: 32 GB
- Storage: 500 GB SSD
- Purpose: Dashboard, AI models, APIs

Estimated Cost:

- Hardware: \$15,000 (4 servers)
 - Network Equipment: \$5,000
 - Software: \$0 (open-source)
 - Annual Maintenance: \$3,000
-

High-Availability Deployment (Enterprise: 250+ users)

Architecture:



Features:

- Load balancing across multiple email gateways
- Database replication (hot standby)
- Automated failover
- Distributed sandbox cluster (Kubernetes)
- Geo-redundant backups

Estimated Cost:

- Hardware: \$50,000+ (8-12 servers)
- Network Equipment: \$15,000
- Software: \$0 (open-source)
- Annual Maintenance: \$10,000

Integration and APIs

Email Platform Integrations

Microsoft Exchange / Office 365:

- **Method:** Exchange Web Services (EWS) API
- **Features:**
 - Mailbox scanning
 - Email quarantine management
 - User mailbox policies
 - Automatic email recall
- **Authentication:** OAuth 2.0

Google Workspace:

- **Method:** Gmail API
- **Features:**
 - Email scanning
 - Label management (Phishing, Spam)
 - Admin SDK for user management
 - Automatic quarantine
- **Authentication:** Service Account with domain-wide delegation

SMTP Integration (Generic):

- **Method:** SMTP proxy (transparent)
- **Compatibility:** Any email server (Postfix, Sendmail, Zimbra)
- **Features:** Real-time scanning, header manipulation

Collaboration Platform Integrations

Slack:

- **Webhook Integration:** Real-time alerts
- **Bot Commands:**
 - `/secureguard status` - System health
 - `/secureguard quarantine` - View quarantined emails
 - `/secureguard report` - Daily summary
- **Channels:** #security-alerts, #phishing-reports

Microsoft Teams:

- **Connector Integration:** Alert cards
 - **Adaptive Cards:** Interactive incident response
 - **Bot Commands:** Similar to Slack
-

Ticketing System Integrations

Jira:

- **API:** REST API v3
- **Features:**
 - Auto-create security incidents
 - Link CVE alerts to tickets
 - Priority mapping (P0 → Blocker)
 - Status sync (Open → In Progress → Resolved)

ServiceNow:

- **API:** Table API
 - **Features:**
 - Incident management
 - Change request tracking
 - CMDB integration
 - Automated workflows
-

MDM Integrations

Microsoft Intune:

- **Graph API Integration:**
 - Device compliance status
 - Automatic device isolation
 - Policy deployment
 - App management

Jamf (macOS):

- **API:** Jamf Pro API
- **Features:**
 - Mac endpoint protection
 - Policy enforcement
 - Remote wipe capability

Threat Intelligence APIs

Provider	API	Rate Limit	Cost
VirusTotal	REST API	4 req/min (free) 1000 req/day (premium)	Free / \$100/mo
AbuseIPDB	REST API	1000 req/day (free)	Free / \$20/mo
URLhaus	REST API	Unlimited	Free
PhishTank	REST API	10,000 req/hour	Free
AlienVault OTX	REST API	No official limit	Free
Shodan	REST API	100 req/month (free)	Free / \$59/mo
Have I Been Pwned	REST API	1500 req/day (free)	Free

SIEM Integration

Wazuh:

- **Integration:** Agent-based + API
- **Features:**
 - Log forwarding to Wazuh manager
 - Custom decoders for SecureGuard logs
 - Alert correlation
 - Compliance reporting (PCI-DSS, GDPR)