2/14/2025

# Pennsylvania State University
# College of Information Sciences and Technology

IST 554 Graduate Network Security

## Project Deliverable 1

Group - 3 : *Aniket Nimbalkar , Gokul Gopakumar, Siddharth Mishra, Sohan Ramalingaiah*

Organization Name : OpenGuardian Solutions
( This is all a hypothetical organization and their current status of where they are as a Startup booming in the IT World )

## Organization Abstract

OpenGuardian Solutions has its headquarters in Santa Barbara, California, and presently operates out of one building. It started in 2020 and today employs 62 people, which includes 45 technical staff, 10 sales and marketing specialists, and 7 executives. The vision for OpenGuardian is to empower organizations to secure and automate their digital futures. OpenGuardian's clients include mid-size healthcare providers, fintech start-ups, and e-commerce websites.

Founded by Emilia Perez and Rachel Zegler, OpenGuardian fosters a more in-person work culture, with 30% of its staff having the option to operate in a hybrid model. The company prioritizes continuous learning, heavily investing in industry-recognized certifications such as CISSP and AWS/Azure cloud training to ensure its technical teams maintain top-tier expertise.

Currently, the organization is looking to expand its footprints to Boston, Texas & Canada as their product has been gaining traction over the past 2 years with multiple clients such as Robinhood and Nvidia adopting the products used.

Briefly, the products that OpenGuardian offers:

- SentinelMDR: AI-facilitated threat detection and incident response solution for hybrid clouds.
- CloudFlow Orchestrator: Low-code DevOps automation platform for AWS, Azure, and GCP.
- ComplianceGuard: SaaS compliance monitoring platform (GDPR, HIPAA, PCI-DSS) in real-time.

Since this is a startup, there have been issues that the Security Team has been trying to solve as no organization starts from the most secure system which are discussed in the security structure section.

## Organization Products

OpenGuardian offers a range of next-generation security and automation solutions that are tailored to suit the requirements of businesses across different sectors. SentinelMDR, one of its flagship products, offers managed detection and response 24/7 with 24/7 continuous network monitoring aimed at detecting and removing threats such as ransomware. For example, a Santa Barbara-based hospital leverages SentinelMDR to detect unusual access patterns in its patient database, automatically isolating compromised devices to prevent data breaches.

The second core product is CloudFlow Orchestrator, which automates deployment of container-based applications into multi-cloud environments with Kubernetes and Docker. Its automation realizes enormous reductions in complexity and deployment time. Example : A Denver logistics startup, for instance, reported a 70% decrease in deployment time after implementing CloudFlow's pre-built templates for AWS ECS, enhancing their scalability and efficiency

To address regulatory compliance challenges, OpenGuardian developed the product ComplianceGuard, a strong solution that searches cloud storage sites like AWS S3 and Azure Blob Storage for unencrypted personally identifiable information (PII). ComplianceGuard provides real-time audit reports to help companies maintain security and compliance levels intact. Example : A Boston-based e-commerce company successfully achieved PCI-DSS compliance within three weeks using ComplianceGuard's intuitive dashboards, streamlining their security and regulatory processes.

## Organization Components

Single Office in Santa Barbara, California : One building with open-floor workspaces, a server room, and conference areas.

Devices:

- Endpoints: 62 PCs (45 technical, 10 sales, 7 executives).
- Servers: 3 on-premises servers (DNS/DHCP, file storage, backups)
- Internet: Single ISP connection (no redundancy).
- Cloud Integration: Minimal; ComplianceGuard and SentinelMDR products interact with client cloud environments (AWS/Azure), but internal operations are on-premises.

| | | |
|---|---|---|
| Technical (Engineering, DevOps, Security) | 45 | 45 PCs |
| Sales & Marketing | 10 | 10 PCs |
| Executives & Admin | 7 | 7 PCs |
| Server Room (Internal) | - | 3 Servers |

## Security Structure of Organization

Currently, this is the recent risk assessment done for the year 2024 :

Risk Assessment

| Risk | Likelihood | Impact | Mitigation Priority |
|---|---|---|---|
| Ransomware Infection | High | Critical | Urgent |
| Unauthorized Wi-Fi Access | High | High | High |
| Server Downtime | Low | High | Medium |
| Insider Threat | Low | High | Medium |

These are the additional policies that the organization is currently working on to meet this year 2025:

- Alignment with Industry Standards HIPAA/GDPR/PCI-DSS: ComplianceGuard helps clients meet these standards, but OpenGuardian's internal network does not fully comply.
- Gaps:
  Unencrypted Wi-Fi violates GDPR and HIPAA data-in-transit requirements.
  No audit trails for internal user activity.
- Setup multiple backups as if ransomware encrypts the backup servers (located on the same network), all backups are lost.
- Needs to improve traffic and collision control as well as servers and departments coexist in one network.
- Needs to upgrade the systems of the Sales department due to no longer free support for Windows 10.

## Network Topology

Single-Site Flat Network: All devices (62 employees, servers, and hybrid workers) operate on a single subnet (192.168.1.0/24) with no VLAN segmentation.

Subnets:

- Office Subnet: 192.168.1.0/24 (62 PCs, servers, and wireless devices).
- Production Subnet: Not applicable; all internal operations share the same broadcast domain.

No Segmentation: Departments (Technical, Sales, Executives) and servers coexist on the same network, increasing broadcast traffic and collision risks.

Endpoint Devices

Workstations:

- 45x Technical PCs (Windows 11, CISSP-trained staff).
- 10x Sales/Marketing PCs (Windows 10, CRM tools).
- 7x Executive PCs (Mac OS 15.3.1, financial/strategic tools).
- Hybrid Devices:  BYOD Laptops/tablets connected via OpenVPN to the network. (Still looking into ways to improve the security and IAM control)

On-Premises Servers:

DNS/DHCP Server: Static IP assignments for servers; dynamic for endpoints.

File Server: Hosts internal documents and ComplianceGuard audit templates.

Backup Server: Local backups only; no off-site or cloud redundancy.

Cloud Integration:

SentinelMDR and ComplianceGuard interact with client AWS/Azure environments with backups.

In both backup cases (including on premises, need to start using the 3-2-1 strategy for backups, currently in testing phases and should be done in production)

Current Backup Strategy:

- On-Prem Only: All backups stored on 192.168.1.4 (same subnet as production).
- No Immutable Backups: Backup server is vulnerable to ransomware encryption.

Firewall & Traffic Filtering:

Firewall setup between router and core switch; all traffic flows restricted but is not maintained well to follow recent security trends.

Gaps: Firewall isn't maintained, hence is susceptible to Ransomware attacks through allowed ports.

Endpoint Protection:

Antivirus: Basic tools with outdated definitions.

Patching: Irregular updates for workstations; servers lack critical security patches.

Authentication & Access:

Passwords: Minimum 8 characters, reused across accounts.

Shared Credentials: Technical team uses shared admin accounts for server access.

Other than the stated expansion plans, the organization is planning to solve these issues within end of Q1

Immediate Upgrades:

- Encrypt Wi-Fi: Deploy WPA3-Enterprise with RADIUS authentication for hybrid workers.
- Segment Network: Implement VLANs for departments, servers, and wireless traffic.
- Backup Strategy: Adopt 3-2-1 rule (AWS S3 for off-site, immutable backups).
- MFA Enforcement: Require Duo Security or Microsoft Authenticator for all logins.

## Compliance

Currently the organization is PCI-DSS Compliant, CCPA compliant and GDPR compliant (In the hopes to potentially open remote locations in the EU in Q4) but not HIPAA yet.

PCI-DSS: The system encrypts and protects credit card data in transit and at rest, uses strong access controls, and meets PCI requirements for handling payments. This is required for cloud providers processing credit card transactions especially for OpenGuardian as they provide security and compliance solutions, their services must align with PCI-DSS to support these clients.

GDPR: It allows users to control their personal data, ensures lawful processing, and provides mechanisms for data deletion.

CCPA: OpenGuardian is headquartered in Santa Barbara, CA, meaning it falls under CCPA's jurisdiction. Any California resident whose personal data is processed by OpenGuardian or its clients is protected under CCPA.

HIPAA (Not Compliant): HIPAA requires cloud service providers (CSPs) working with healthcare clients to sign Business Associate Agreements (BAAs) with each covered entity (hospitals, clinics, etc.) to ensure proper PHI protection. Since OpenGuardian hasn't signed BAAs with these clients, they are not HIPAA compliant. OpenGuardian additionally invests in CISSP & AWS/Azure/Google cloud training, but HIPAA requires specific workforce training on handling PHI, which is not be part of their program.