Security Model Justification

1. Introduction

The client operates as a Mid-size law firm specializing in corporate and intellectual property law, handling highly confidential client data and sensitive legal documents. Due to the high-value nature of its cases and clientele, the organization is an attractive target for ransomware groups, advanced persistent threats (APTs), and insider risk.

Given these threat conditions, the recommended security architecture is based on the Zero Trust model, supplemented by Defense-in-Depth principles to provide layered safeguards.

2. Zero Trust Security Model Overview

Zero Trust operates under the principle of “Never trust, always verify.” Access to resources is granted only after continuous authentication, authorization, and validation of user/device context, regardless of network location.

Key Zero Trust Principles for the Client:

- Strict Identity Verification: Multi-factor authentication (MFA) for all user logins, including partners and remote staff.
- Least Privilege Access: Role-based access control (RBAC) to ensure staff only access data required for their duties.
- Micro-Segmentation: Dividing the network into smaller, secure segments to limit lateral movement in case of compromise.
- Continuous Monitoring: Real-time inspection of all user activity and network traffic.
- Device Compliance Enforcement: Only compliant, monitored devices are permitted to access classified case systems.

3. Defense-in-Depth Considerations

While Zero Trust provides strong identity and access controls, Defense-in-Depth ensures the client's environment has multiple, redundant security layers to address evolving attack vectors.

This layered approach ensures that if one defense mechanism fails, additional controls remain in place to prevent or mitigate the breach.

Defense-in-Depth Layers for the Client:

- Endpoint Protection: OpenEDR with behavioral detection and automated containment.
- Network Monitoring: Wazuh SIEM for centralized log correlation, mapped to MITRE ATT&CK.
- Email Security: Advanced phishing detection and attachment sandboxing.
- Data Protection: Encrypted storage for case files and secure document sharing platforms.
- Tailscale VPN enforces authenticated and encrypted access across all sites.
- Suricata IDS deployed on a dedicated Ubuntu server monitoring Tailscale traffic.

4. Justification for Hybrid Approach

The Zero Trust model directly addresses the client's most critical security concerns: insider threats, credential theft, and unauthorized access to high-value legal data. By enforcing continuous verification and least privilege, it significantly reduces the likelihood of data breaches.

However, legal sector threats often include multi-stage attacks such as phishing → credential theft → ransomware deployment. In such cases, Defense-in-Depth ensures that even if an attacker breach one-layer, multiple other security controls remain to block their progress or limit damage.

By combining both models:

- Zero Trust ensures no implicit trust is granted to any user or device.

- Defense-in-Depth ensures resilience through redundant protective layers.

5. Conclusion

Given the client’s operational sensitivity, legal compliance obligations, and history of targeted attacks (including a ransomware incident), a hybrid security strategy combining Zero Trust and Defense-in-Depth is essential.