# Case Study

**Customer Profile:** A large-sized Law Organization operating across four physical locations, including a main site with approximately 300 employees

**Customer Challenge:** The organization required advanced network security and real-time threat visibility that traditional hygiene, and endpoint protection software tools were not able to detect.

**Their specific concerns included:**

- ICMP Scans: Identifying unauthorized network reconnaissance attempts.
- TCP Port Scans: Detecting attackers probing for open vulnerabilities.
- Lateral Movement: Tracking unauthorized traversal between endpoints.
- Large File Transfers: Monitoring unusual data uploads, downloads, or deletions.
- Command and Control (C2) Beaconing: Detecting malicious external communications.
- Real time identification in the **ABBI** (After Breach Before Impact) phase of the attack
- Decrease the MTTI (Mean TIME to IDENTIFY) time from 271 days to days, weeks
- Internal Threats

They also sought a security solution that integrates network detection and response (NDR) capabilities with endpoint protection software, enabling automated incident response workflows.


Mirai Systems

# Case Study

**GuardTower Solution Implementation:** GuardTower will be able to provide real-time network visibility, proactive threat detection, and automated incident alerts across all locations.

1. **Deploying GuardTower Digital Twin / AI Decoys:**
   - Placed at the perimeter and internal network points of all four locations.
   - Monitor traffic in real time to detect anomalous behavior.
2. **Threat Intelligence & AI-Driven Analysis:**
   - GuardTower's AI-powered engine will analyze network traffic for reconnaissance activities like ICMP and TCP scans.
   - Behavioral analytics track lateral movement and unauthorized data transfers.
   - Deep learning algorithms will identify C2 beaconing, preventing malware from establishing persistence.
3. **Seamless Integration with Endpoint Protection Software & SIEM Tool:**
   - GuardTower's intelligent alerting system will trigger real time notifications upon detecting suspicious activity, uncovering threats that have already bypassed the existing hygiene and endpoint security system. This crucial capability provides visibility into previously undetected breaches in the **ABBI** Phase of the attack, ensuring a proactive response before full network compromise.
   - Automated workflows will isolate compromised endpoints, preventing further spread.
   - GuardTower communicates with the organization's existing SIEM tool to augment, alert, and kick off their cybersecurity plan, ensuring rapid remediation before a full network impact occurred.
4. **Advanced Network Layer Visibility:**
   - Provides continuous monitoring without interfering with existing endpoint security tools.
   - Offers real-time, historical forensics for security analysts.


Mirai Systems

# Case Study

**Conclusion:** By deploying GuardTower, the organization will enhance its security posture, detecting and alerting to network threats that traditional hygiene and endpoint protection solutions fail to identify.  GuardTower's ability to share signals with existing hygiene tools, endpoint protection software, and SIEM ensures an orchestrated offensive mechanism, integrating Defense-in-Depth (DID) strategies to drastically reduce the attack surface, lower Mean Time to Identify (MTTI), enable real-time threat detection during the ABBI attack phase, and significantly strengthen operational security

| | | Outcomes |
|---|---|---|
| **Proactive Threat Detection** | ✓ | The organization gained real-time insights into malicious activities, reducing dwell time from months, weeks to minutes. |
| **Enhanced Incident Response** | ✓ | Automated signals between GuardTower, SIEM, and endpoint security improved containment strategies. |
| **Increased Network Layer Visibility** | ✓ | GuardTower provided detection capabilities beyond traditional endpoint solutions. |
| **Minimized Security Risks** | ✓ | Improved response times helped prevent data exfiltration and system compromise. |
| **Scalability & Flexibility** | ✓ | GuardTower's solution adapted to all four locations, including variable hoteling sites. |


Mirai Systems