Securing the Digital Backbone of Legal Support Services

About the Customer

The customer is a professional services firm specializing in legal process outsourcing (LPO), offering a broad spectrum of services including litigation support, legal research, e-discovery, and document review. Catering to law firms and legal departments across the globe, the organization operates with a highly remote and cloud-based workforce, managing confidential client data, case files, and contracts across secure portals and legal tech platforms.

The Challenge

Operating in a domain where trust and confidentiality are non-negotiable, the firm faced growing cybersecurity and data protection challenges:

Securing legal data repositories including contract archives, case records, and client documentation	**Ensuring compliance with global privacy standards** such as GDPR and client-specific SLAs on data handling.	**Protecting remote legal professionals** and freelancers from phishing, malware, and session hijacking threats.
Monitoring third-party integrations with case management, time tracking, and document automation platforms.	**Maintaining audit readiness** for client security assessments and potential legal proceedings.	**Preventing insider risks and** privilege misuse in shared access environments.

With growing client expectations and increasing regulatory pressure, a continuous and intelligent security approach was essential.

Threat Deception with XDR+

Deception techniques helped identify sophisticated threats:

- Planted fake legal case files and contract folders to monitor unauthorized access attempts.
- Deployed dummy legal email identities to catch phishing and credential stuffing bots.
- Resulted in a 47% improvement in detection speed for anomalies within the document lifecycle.

Security Compliance Enablement with GSOS

GSOS provided the foundation to:

- Map controls to GDPR, client-specific contracts, and vendor security checklists.
- Enable real-time evidence collection for legal audit trails and SLA metrics.
- Empower stakeholders with a dashboard for policy monitoring and control ownership.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Identified 1,900+ assets, including legal SaaS tools, DMS, email accounts, and third-party integrations.
Discovery	Detected 41 critical vulnerabilities, including misconfigured S3 buckets, over-permissive file shares, and unmonitored access tokens.
Prioritization	Flagged 17 high-risk exposures tied to document exfiltration and identity abuse scenarios.
Validation	Emulated attack scenarios like contract scraping and account takeover in isolated test environments.
Mobilization	Resolved 89% of prioritized risks within 18 business days using a hybrid internal and vendor-assisted remediation strategy.

Executive Quote

"Our clients trust us with their most sensitive legal work. Invinsense helped us back that trust with real-time visibility, continuous testing, and a proactive security strategy that aligns with legal industry expectations."

– Director of Legal Operations, Global Legal Support Firm

Solutions Used

To meet these evolving demands, the firm implemented the Invinsense platform:

- Invinsense XDR for centralized visibility across endpoints, SaaS legal tools, cloud storage, and user behavior.
- Invinsense XDR+ to deploy deception assets within document management systems and contract repositories.
- Invinsense OXDR for continuous threat exposure management across public cloud, identity platforms, and case systems.
- Invinsense GSOS for operationalizing and tracking compliance with client SLAs, privacy obligations, and vendor assessments.

Key Results

- 89% closure of identified security gaps within 18 business days.
- 47% faster detection of document-related threats using deception and behavioral analysis.
- Improved audit readiness for global law firm clients and external compliance reviews.
- Strengthened data governance and access control across remote legal teams.
- Elevated client confidence in the firm's ability to safeguard sensitive case data.

Infopercept | INVINSENSE

About Infopercept - Infopercept is one of the fastest growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy