SERKET-TECH SECURITY

Cybersecurity for Modern Law Firms

Cybersecurity, compliance, and resilience services for law firms, legal service providers, eDiscovery teams, and adjacent organizations.

Protect privileged data, reduce client diligence friction, and secure modern legal operations.

Legal organizations manage privileged communications, litigation records, financial data, and highly sensitive personal information across email, cloud platforms, document systems, and third-party providers. Clients, insurers, and internal leadership now expect stronger security evidence, faster readiness for responses, and better control of vendor risk.

Serket-Tech Security helps legal teams build practical security programs that align with how matters move through the business.

Our work spans governance, assurance, testing, response, managed protection, and executive guidance without losing sight of client service, billable work, or operational continuity.

Reduce Client and Insurer Friction

Prepare for security questionnaires, outside counsel requirements, cyber insurance reviews, and customer diligence with clearer evidence and a more robust program structure.

Prepare for Disruption and Maintain Continuity

Improve incident response, business continuity, executive decision-making, and recovery planning before a breach or outage disrupts active matters.

Strengthen Cloud and Vendor Oversight

Evaluate document management, eDiscovery, practice management, and other third-party platforms that handle sensitive legal and client information.

Protect Privilege and Confidentiality

Secure documents, email, collaboration, mobile work, and matter data with controls that fit legal workflows and confidentiality expectations.

Best fit for law firms, corporate legal departments, alternative legal service providers, eDiscovery and litigation support teams, title and settlement groups, expert witness organizations, and other businesses that handle sensitive legal data.

SERKET-TECH SECURITY

Comprehensive Service Portfolio

A single partner that can support program development, technical validation, response readiness, and ongoing operations across the legal security lifecycle.

Governance, Risk, and Compliance

- Policy development and control design
- Security program support and risk assessments
- Regulatory, contractual, and client requirement mapping

Third-Party and Vendor Risk

- eDiscovery, SaaS, and service provider reviews
- Security due diligence for vendors and subcontractors
- Stronger oversight workflows and reporting

Assurance and Trust Support

- SOC 2 readiness and attestation support for legal tech and service providers
- HITRUST readiness and certification path support where regulated data drives the requirement
- Evidence planning, remediation, and control ownership

Incident Response, Resilience, and Managed Services

- Tabletop exercises, breach support, and forensic coordination
- Monitoring, detection, and response support
- Ongoing control monitoring and issue tracking

Executive Leadership and Program Development

- Fractional CISO support
- Cybersecurity strategy and roadmap reviews
- Executive briefings, board reporting, and program governance

Data Protection and Workflow Security

- Email, collaboration, endpoint, and identity hardening
- Encryption, access control, and least privilege design
- Metadata protection and secure file sharing

Security Assessments and Testing

- Security posture and maturity assessments
- Architecture and control reviews
- Vulnerability assessments and remediation planning

Penetration Testing and Validation

- External and internal network testing
- Web application and cloud testing
- Prioritized findings and retest support

Programs can be tailored to client outside counsel guidelines, security questionnaires, cyber insurance reviews, state breach obligations, and matter-specific requirements, such as the FTC Safeguards Rule, HIPAA, CJIS, NIST, or CMMC, when the practice and data involved warrant it.

SERKET-TECH SECURITY

Built for Legal Sector Realities

Serket-Tech Security focuses on the issues that legal buyers and adjacent providers are under pressure to solve now, while keeping the full-service set broad enough to support one-time projects or ongoing programs.

- **Client Confidentiality and Privileged Data**
  Protect email, document repositories, shared workspaces, mobile devices, and matter files that contain privileged, confidential, or court-sensitive information.
- **AI Governance for Legal Workflows**
  Set guardrails for drafting, research, review, and discovery use cases to ensure confidentiality, human review, accuracy, and tool oversight remain in focus.
- **Wire Fraud, Account Compromise, and Payment Risk**
  Reduce exposure to phishing, business email compromise, fraudulent payment instructions, and high-consequence approval failures in finance and settlement workflows.
- **Client Diligence and Outside Counsel Expectations**
  Respond to security questionnaires, client audits, and outside counsel requirements with clearer controls, better evidence, and stronger operational follow-through.

How Clients Engage Serket-Tech Security

Engagements can start with a readiness review, targeted assessment, tabletop exercise, penetration test, assurance initiative, or recurring advisory and managed support program.

1. Assess
Review current posture, obligations, gaps, and business priorities.

2. Prioritize
Define the roadmap, sequence remediation, and assign owners.

3. Implement
Deploy controls, perform testing, support reviews, and close gaps.

4. Operate
Monitor, report, respond, and keep the program current.

Representative clients include litigation and trial firms, corporate and M&A practices, real estate and trust teams, legal departments, alternative legal service providers, eDiscovery vendors, expert witness organizations, investigations teams, and legal tech businesses serving regulated clients.

Build a legal security program that is client-ready, incident-ready, and aligned with how legal work actually moves.