L1 Cybersecurity Package

> Cybersecurity Essentials for Law Firms
> Tailored to Legal Industry Needs
> Foundational Coverage to Protect Your Law Firm

OVERVIEW: WHO IS STS L1 FOR?

Our Level 1 Cybersecurity Package is designed as an essential foundational cybersecurity suite, tailored to law firms. Consider this package your first step to better cybersecurity standings, with everything you need to provide compliance-focused, basic protections that every law firm needs in place. Designed around world-class cybersecurity frameworks set forth by the Center for Internet Security and National Institute of Standards & Technology, two leading authorities, this package provides law firms and their clients with the essential peace of mind that builds business trust and empowers success.

WHAT'S INCLUDED: THREE LAYERS OF PROTECTION

LAYER 1

PROTECT YOUR PEOPLE

- Security Awareness Training
  - Includes simulated phishing to build safe habits and prevent human error (#1 cause of all cyberattacks)

LAYER 2

SECURE YOUR SYSTEMS

- Web Content Filtering
- Microsoft 365 Security and Email Encryption
- Endpoint & Server Hardening (CIS L1)
- Vulnerability Management

LAYER 3

MONITOR & RAPIDLY RESPOND

- Dark Web Monitoring
- 24/7 Security Monitoring (SIEM & Identity)

WHY LAW FIRM LEADERS CHOOSE STS L1:

Reduce cyber risk
Layered protection across people, endpoints, email & cloud.

Compliance-ready
Aligned to CIS, NIST, HIPAA, PCI-DSS & SOC best practices.

Protect your business
Safeguard client & company information end-to-end to secure what you've built.

Be Insurable
Meet the controls cyber insurers increasingly require.

24/7 Peace of Mind
Round-the-clock SOC monitoring,detection & response.

THE PRACTICAL VALUE:

Understanding the Controls Included in STS L1 Security Package

Your Level 1 Cybersecurity Package includes **seven critical core controls** that cover your law firm from major threat vectors and gaps in your cybersecurity. Below, you'll find their definitions and the practical threats they protect against.

CONTROL	WHAT IT DOES	WITHOUT THIS CONTROL...
01 Security Awareness Training	Interactive training and simulated phishing that build safe habits and stronger threat reporting.	**Employees fall for phishing — exposing credentials and letting ransomware into the network.**
02 Web Content Filtering	Automatically blocks known malicious sites, with category and keywordfiltering for safe browsing.	**One click on a malicious site can trigger a drive-by malware or ransomware infection.**
03 Dark Web Monitoring	Continuously scans stolen-credential databases and gives earlywarning when accounts are exposed.	**Leaked passwords circulate for months, fueling account takeover and business email compromise (BEC) attacks.**
04 04 Microsoft 365 Security & Email Encryption	Hardens Microsoft 365 to the CIS Level 1 baseline and encrypts sensitive email in transit.	**Weak cloud settings and unencrypted email lead to mailbox compromise and leaked sensitive data.**
05 Vulnerability Management	Continuously scans assets for missing patches and prioritizesremediation by risk.	**Attackers exploit known, unpatched weaknesses long after fixes are publicly available.**
62 Security Monitoring	24/7 event and identity-threat monitoring with escalation to a SOC forrapid response.	**Intrusions go undetected for weeks, giving attackers time to steal data and deploy ransomware.**
07 Endpoint & Server Hardening	Applies CIS Level 1 device baselines plus full-disk encryption onlaptops and workstations.	**By default, misconfigured devices give attackers easy footholds to spread across the environment.**

NEXT STEPS: TRY 30 DAYS FREE

Schedule a free consultation and redeem one FREE month of our L1 Security Package when you sign by 11/20/2026. Email sales@stspartner.com to get started!

SOC 2 TYPE II CERTIFIED