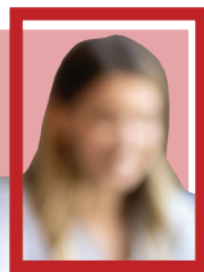


# Enhance Law Firm & Legal Service Provider Security Protocols

Extend physical security controls to your hybrid legal organization. SessionGuardian's isolated identity access controls enable secure document review, source code review, and access to matter-specific Microsoft 365 collaboration.



## Cybersecurity Risk Mitigation

People and data are an organization's primary assets. The need to protect both the individual and data, especially in a hybrid working environment, has never been more critical. Regulated legal documents and IP have an extremely high value, making law firms and third-party legal service providers prime targets for cyberattacks. Reduce the risk of unauthorized access to the data by limiting access to only known personnel on approved devices and approved locations, thus extending physical security controls to the hybrid working environment.

## Why SessionGuardian for Legal Organizations

SessionGuardian ensures that only authorized users on an authorized device from an authorized location can access a VDI or URL via SessionGuardian VDI and SessionGuardian Web. Our use cases include secure matter-specific collaboration with M365 applications, (e.g. Outlook, Teams, file sharing); secure document review, and secure source code review.

## SessionGuardian for Legal Industry Benefits

### Regulatory Compliance

Matter-specific client documents and IP contain sensitive, proprietary information. Knowing the identity of whoever is accessing that data at all times is key. This is especially true in the work-from-anywhere paradigm. Our facial authentication security feature ensures that an authorized user is who they say they are, while also providing geolocation and other security restrictions.

### Insider Threat Avoidance

Insider threats are a significant issue for any organization. This is especially true where sensitive client data or matter-specific data is at risk. By combining person, device, and location as factors of authentication, the probability of malicious (credential sharing, shoulder surfing, mobile phone photos) or accidental (transfer of private data) insider threats is vastly reduced.



### IDENTITY ASSURANCE

- Facial Authentication - Continuous or One-Time
- User Present/Liveness Detection
- Shoulder Surfing Prevention
- 3<sup>rd</sup> Party ID Verification
- SSO Integration

### END-USER DEVICE STATUS



- Verify Device Integrity
- Known Networks (IP/VPN Restrictions)
- GPS-based Geolocation Approve/Deny
- Allowed/Unauthorized Applications
- Time of Day

### DATA PROTECTION

- Screenshot, Screen Capture, Screen Print Prevention
- Mobile Phone Detection for Screen Photo Prevention
- Watermarks



### COMPLIANCE

- No Biometric Data Stored or Transmitted
- Compliant with all major privacy regulations including GDPR
- Granular Audit Trails
- Alerts
- SIEM Integration



## Matter-Specific Collaboration

Our matter-specific infrastructure is the only solution that securely enables cross-organizational projects on Microsoft 365 and safely harnesses the collaborative power of Microsoft Teams. Each member of the matter (including remote and contract attorneys) can host private or group Teams calls, share documents, and collaborate freely with the team. It also flexes to your matter's urgency and litigation teams are able to set up matter-specific workspaces within hours.

## Protect any VDI Environment

Our configurable security controls can be applied to your VDI or sensitive websites, putting security at your fingertips. These controls are defined in a common control plane, managed by your organization, that facilitates VDI service providers (e.g. Azure, Citrix, AWS, Azure) and SessionGuardian Web.

## Configurable Layers of Security

SessionGuardian allows security controls to be configured by an organization. This enables stricter controls as the sensitivity of the data increases.

## Key Use Cases

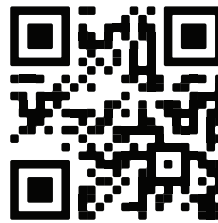
Preventing unauthorized access to client data and IP is essential, and SessionGuardian can help. We enable you to limit access to your data by extending physical security controls to the hybrid working environment and allowing only authorized personnel from authorized devices in authorized locations. With SessionGuardian's technology, you can secure:

- Matter-specific collaboration
- Third-Party / BPO access to data
- Document review
- Source code review
- eDiscovery

## About SessionGuardian

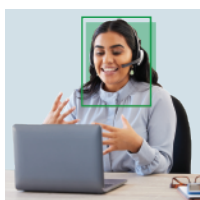
SessionGuardian is the leader in identity access control and authentication for hybrid teams. Our cybersecurity solutions protect highly sensitive assets from data theft by ensuring only authorized users access the data.

For more information about SessionGuardian and to schedule a demo, contact [info@SessionGuardian.com](mailto:info@SessionGuardian.com).

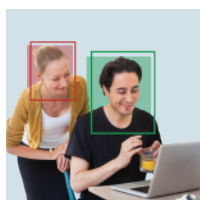


# Can you prove who is looking at your sensitive data?

SessionGuardian reduces the risk of sensitive data disclosures in hybrid and remote access environments.



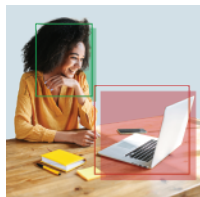
Ensure the authorized user is physically present.



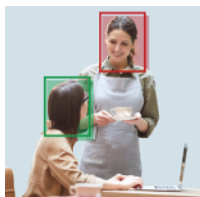
Prevent unauthorized shoulder surfing.



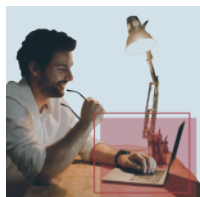
Prevent screen sharing and screenshots.



Ensure the device is safe to access secure information.



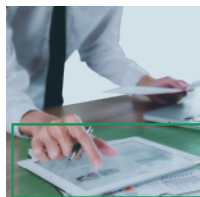
Ensure users logon from a permitted location and network.



Ensure users logon at the desired time of day.



Maintain detailed audit trails for compliance.



Generate automated time tracking reports.