

PRIVACY PROS: **YOUR SECURITY** **TEAM NEEDS YOU!**

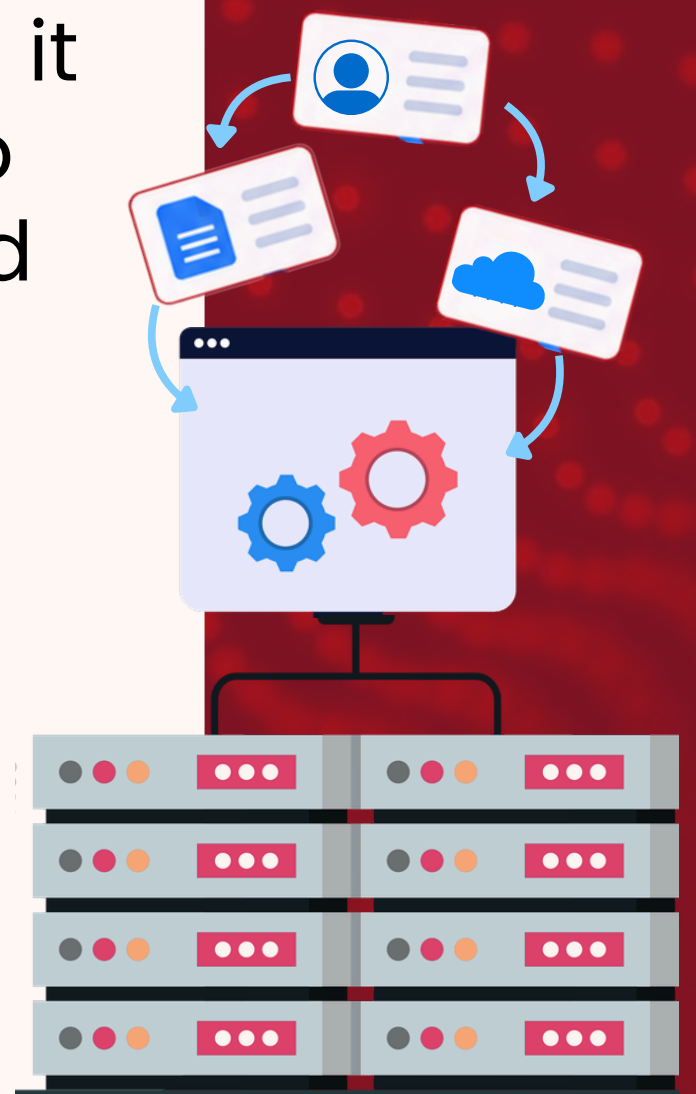
**6 ways privacy strengthens
cybersecurity resilience**



Mapping the Data Landscape

Security teams cannot protect what they cannot see.

Privacy teams often maintain the data maps and inventories that track where personal information lives and how it moves. This helps reduce blind spots, making it easier for security teams to apply the right controls and spot anomalies early.



01

Reducing the Attack Surface Through Data Minimization

The more data a company holds, the more attractive it becomes to attackers.

Privacy teams establish data minimization policies and systems that limit collection, storage, and processing to what's necessary for business purposes.

Enforcing retention schedules and coordinating secure disposal with security teams keeps dormant data from becoming an unmonitored risk.

02



Putting Risk Awareness in Motion

03

Privacy Impact Assessments (PIAs) can strengthen security posture.

When privacy teams conduct PIAs, they might uncover risks security teams need to address immediately, like weak access controls or insecure transfer methods.

Tracking remediation tasks on a shared dashboard with other security work supports visibility, accountability, and follow-through.



Championing Vendor & Third-Party Risk Alignment

04

Third-party breaches remain one of the most common and damaging attack vectors.

Privacy teams already assess vendors for data handling practices, which can reveal security weaknesses before contracts are signed.

Aligning those assessments with security's due diligence processes lets both teams evaluate a vendor's privacy and security requirements in a single pass.



Enriching Threat Intelligence with Privacy Risk Signals

Security threat models often focus on technical vulnerabilities.

Privacy teams are attuned to risks such as re-identification, metadata, and unstructured data that traditional security tools may not catch.

Feeding privacy-specific risk indicators into threat intelligence pipelines allows security teams to detect and prioritize threats more effectively.

05



Spotting Data Misuse from the Inside

06

Not all threats involve external attackers. Privacy teams are well positioned to spot patterns, like over-collection, unauthorized access, or scope creep, that may not trigger traditional security alerts.

By setting up anomaly detection for unusual access to sensitive datasets, privacy teams give security teams a head start on insider risks.



When privacy and security work as one integrated system instead of on parallel tracks, organizations can anticipate threats rather than react to them.

Need help turning privacy into your security team's strongest partner?

**Get in touch at:
www.redcloveradvisors.com**