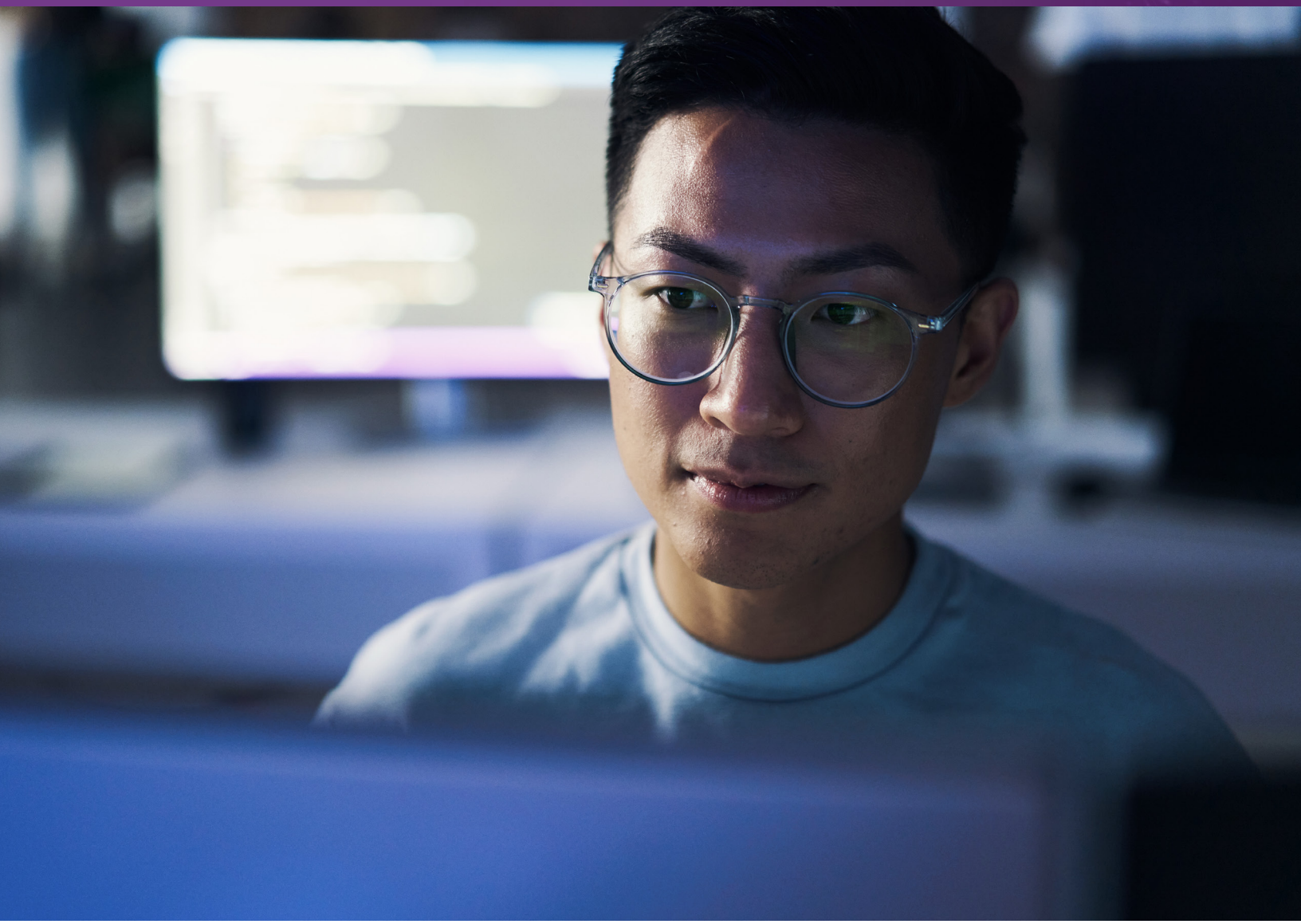
SOLUTION BROCHURE

Protect Privileged Legal Data When Access Is Compromised

Data-centric protection and resilience for large law firms facing ransomware and data exfiltration risk



ENTRUST

SECURING A WORLD IN MOTION

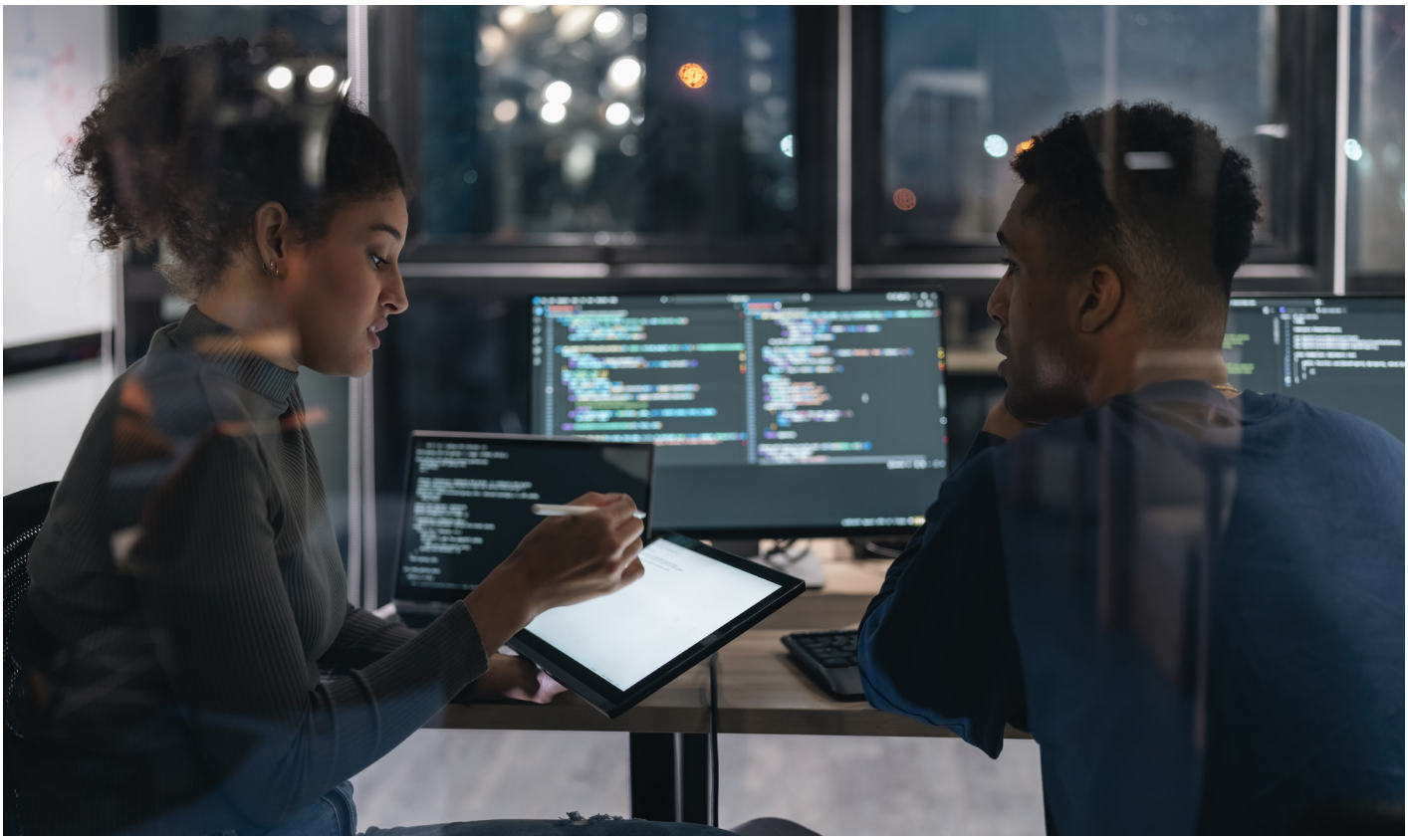
Law firms cannot rely on prevention alone. As ransomware shifts toward data theft and extortion, firms need to protect sensitive legal data directly – so even if attackers gain access, privileged information remains controlled, encrypted, and unusable.

Overview

Today's ransomware attacks are no longer just about encrypting systems or disrupting operations. Recent attacks have reinforced that law firms are priority targets for ransomware and data extortion. Attackers are increasingly focused on gaining access to sensitive data, extracting it quickly, and using that exposure as leverage.

For law firms, this creates immediate business risk. Firms hold privileged client communications, merger and acquisitions (M&A) activity, litigation strategy, intellectual property, and other highly sensitive information that can directly impact clients, active matters, and firm reputation if exposed.

As this threat evolves, law firms need more than perimeter defense and recovery planning. They need to protect the data itself – so even if access is compromised, sensitive information remains controlled, encrypted, and unusable.



The Challenge: A New Class of Legal Data Exposure Risk

Large law firms operate in complex, distributed data environments. Sensitive legal information lives across documents, file shares, cloud storage, collaboration platforms, backups, archive data, and client workflows. Attorneys, partners, clients, and third parties all require access, increasing the number of paths through which data can be exposed. Law firm mergers can compound this complexity, introducing new client data, systems, repositories, and security practices that must be brought under consistent protection and control.

At the same time, attackers are shifting tactics. Rather than relying only on system encryption, many attacks now prioritize data exfiltration and extortion – creating risk even when operations remain online.

Understand the Risks:

- **High-value sensitive data**

  Law firms manage privileged communications, M&A activity, litigation strategy, intellectual property, and client-confidential material.

- **Distributed access and users**

  Attorneys, partners, clients, and third parties require access across locations, devices, and workflows.

- **Control gaps after access**

  Traditional controls often focus on prevention but may not protect sensitive data once an attacker gains legitimate access.

- **Fragmented ownership and governance**

  Security, IT, and practice groups may operate independently, creating inconsistent policies and limited visibility into how sensitive data is accessed and used.

Why It Matters

Once sensitive client information is copied or used for extortion, the impact extends beyond IT. Data exposure can erode client trust, create legal, privacy, and regulatory exposure, disrupt active matters, and damage the firm's reputation.

For many firms, this is becoming an executive-level issue – not simply a security operations concern – because data exposure can affect client trust, active operations, regulatory posture, and firm reputation.

> For law firm leaders, the question is no longer only, "Can we stop every attack?" It is also, "If someone gets in, can they use the data they find?"

The Entrust Approach: Protect the Data Itself; Enhance Cyber Resilience

Entrust helps law firms reduce ransomware and data exfiltration risk by protecting sensitive legal data directly – not just the systems around it.

With the Entrust Cryptographic Security Platform, firms can protect sensitive legal data through a combination of data-centric file encryption, with HSM as root of trust, centralized key management, and governance controls. This helps ensure privileged information remains protected wherever it resides while giving firms greater control over who can access it, how it is protected, and how cryptographic policies are enforced across the organization.

Entrust helps firms:

Protect sensitive legal data with strong encryption

Apply persistent, data-centric protection to privileged client information, litigation records, deal documents, intellectual property, and other sensitive legal content, so it remains protected even if accessed, copied, or exfiltrated.

Reduce exposure if access is compromised

Shift from relying solely on prevention to protecting data in an assume-breach scenario, helping ensure sensitive information remains unusable without authorization.

Control encryption keys and access centrally

Use centralized key management and policy controls to govern access to protected information, improving consistency, oversight, and control across distributed environments.

Enhance cyber resilience with automated self-healing data

When data is altered, encrypted, or deleted as a result of ransomware or other malicious activity, Entrust automatically reconstructs affected data using trusted fragments stored across multiple locations. This process is transparent to applications and users, allowing organizations to maintain business continuity while remediation activities are underway.

Demonstrate governance and defensibility

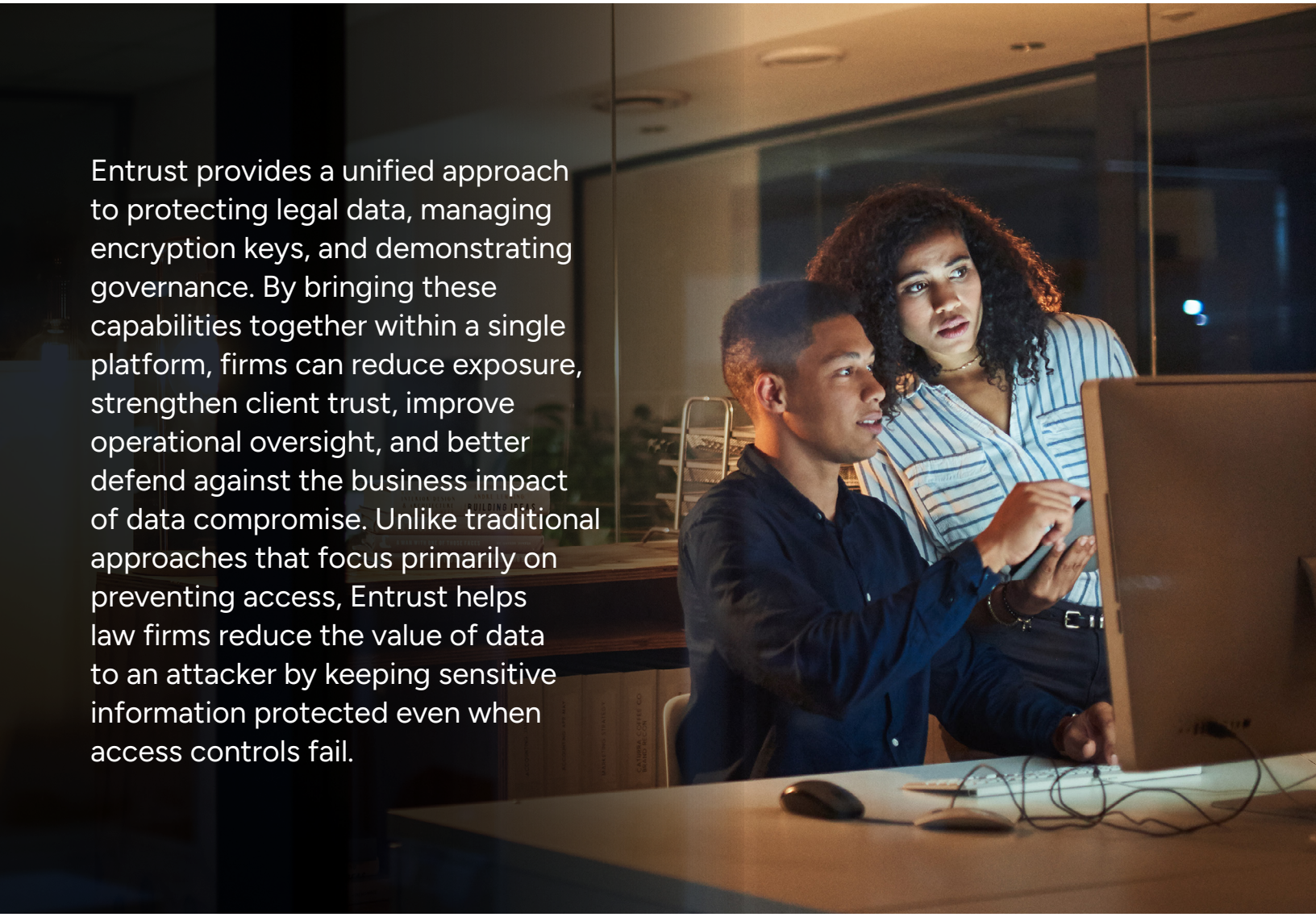
Improve visibility into how sensitive legal data is protected while supporting audit readiness, regulatory requirements, incident response, and client expectations around confidentiality.

Protect	Control	Prove
Apply strong data-level encryption to help keep sensitive files unintelligible if accessed.	Manage encryption, access, and key control centrally – without relying on agent-heavy deployment models.	Support governance, audit readiness, and incident response with visibility into how data is protected.

Why Entrust

Entrust helps law firms protect privileged legal information directly, without adding unnecessary operational complexity. Through the Entrust Cryptographic Security Platform, firms can combine data-centric file encryption, centralized key management, and governance controls to protect sensitive information across distributed environments while maintaining visibility and control over how data is accessed and protected.

Entrust file encryption's agentless approach is especially important for large law firms, where sensitive information spans users, matters, file shares, cloud environments, backups, and collaboration workflows. There are zero application changes required, and it's completely transparent to end-users. As a result, the system can be deployed within hours. By helping keep data encrypted and controlled even if access is compromised, Entrust supports a more resilient approach to ransomware and data exfiltration risk.



Entrust provides a unified approach to protecting legal data, managing encryption keys, and demonstrating governance. By bringing these capabilities together within a single platform, firms can reduce exposure, strengthen client trust, improve operational oversight, and better defend against the business impact of data compromise. Unlike traditional approaches that focus primarily on preventing access, Entrust helps law firms reduce the value of data to an attacker by keeping sensitive information protected even when access controls fail.

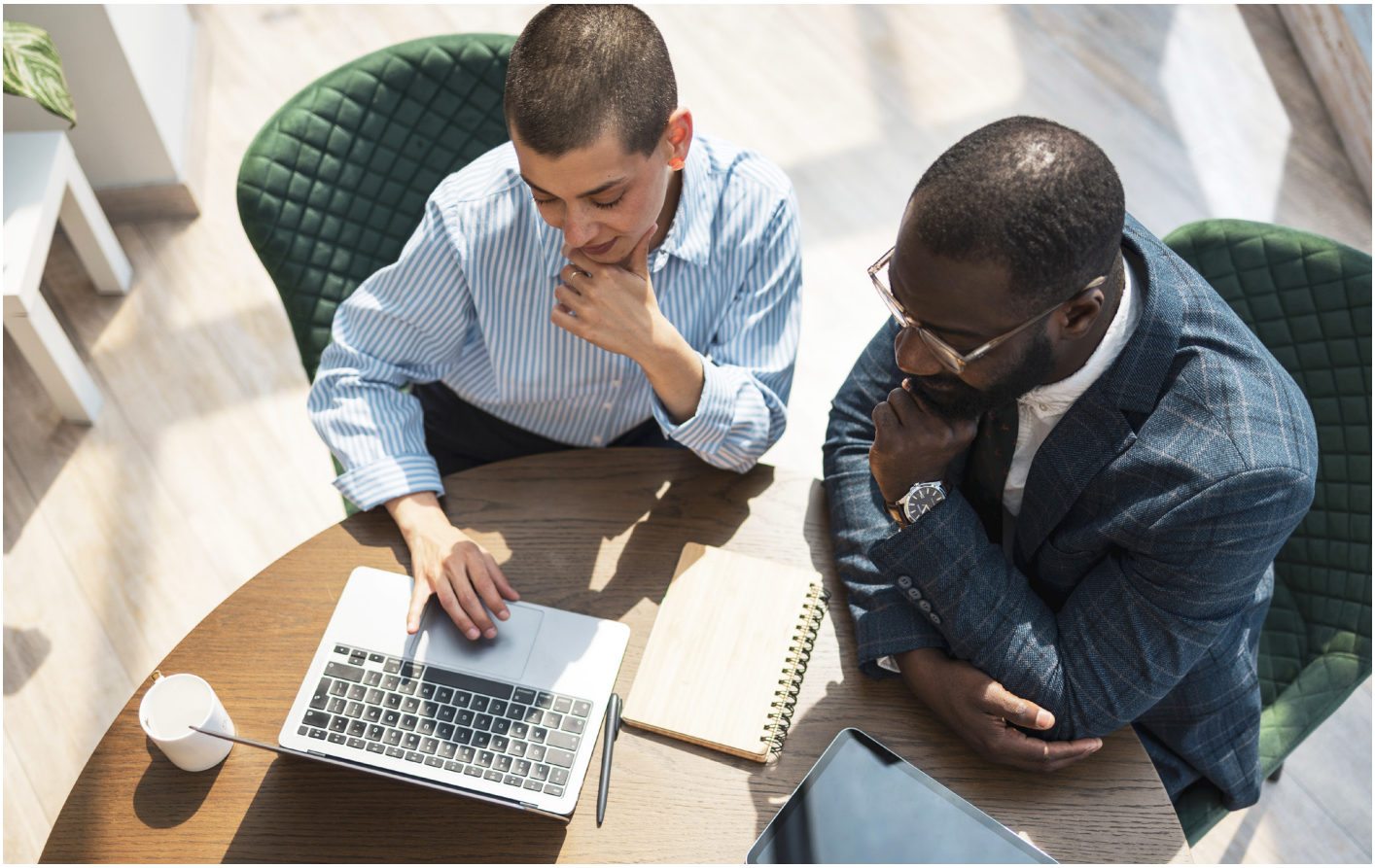
Business Outcomes

With Entrust, law firms can:

- **Reduce ransomware-driven data exposure risk** by protecting sensitive data directly
- **Help keep privileged legal information unusable if accessed** through strong encryption and cryptographic controls
- **Strengthen client trust and confidentiality** by improving protection for sensitive matter, clients, and firm data
- **Improve governance and visibility** across distributed data environments and fragmented ownership models
- **Support incident response and defensibility** by reducing the impact of compromised access

Law firms cannot prevent every access risk. But they can reduce what is exposed when access is compromised.

Protect your firm's privileged legal data at the source by **connecting with one of our data security experts**. Explore how you can strengthen your ransomware resilience, preserve client trust, and reduce the business impact of data exfiltration.



ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

©2026 Entrust Corporation. All rights reserved. Entrust, Datacard, and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. DS27Q2-crytographic-security-platform-for-law-firms-sb

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION