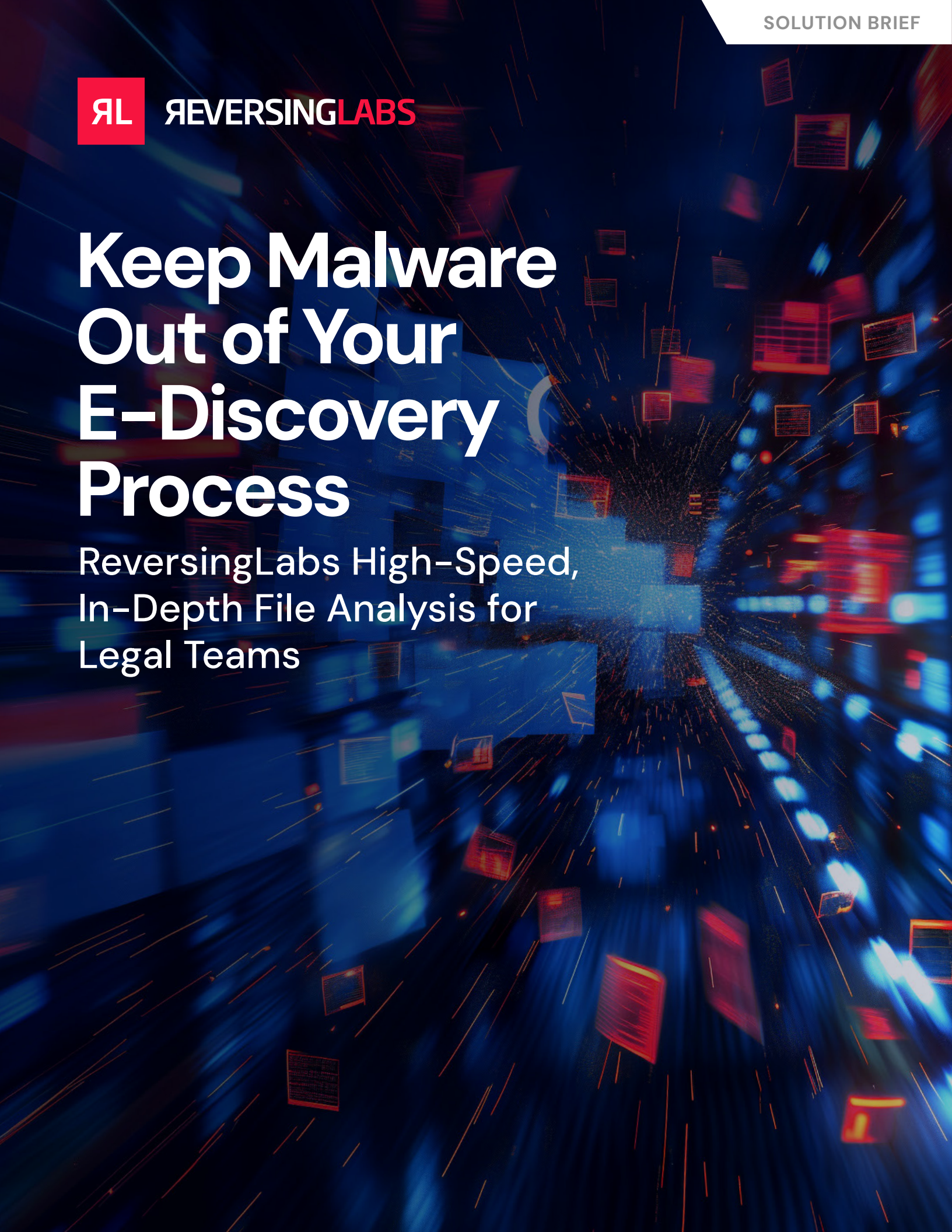
SOLUTION BRIEF

REVERSINGLABS

Keep Malware Out of Your E-Discovery Process

ReversingLabs High-Speed, In-Depth File Analysis for Legal Teams



Overview

It is more crucial than ever for organizations of all types and sizes to fortify their security controls against advanced malware threats. This is especially true for legal organizations that are bringing in files from external sources as part of their daily workflow.

Law firms and legal teams have become increasingly appealing and lucrative targets of malware attacks due to the nature of their business. They store and share vast amounts of sensitive data, such as confidential corporate data, personally identifiable information, intellectual property, financial documents, and more. For threat actors, this is a treasure trove of high-value information waiting to be exploited, and they are seizing every opportunity to do so.

Attackers are taking advantage of insufficient security measures and monitoring and detection gaps at law firms, especially when it comes to e-Discovery and the large volumes of files and data exchanged between external entities on a daily basis. It's the perfect entry point for advanced malware to slip into the organization. Unfortunately, existing security tools meant to detect malware and ensure file hygiene are struggling to keep up as the amount of data and complexity of files continues to grow at an exponential rate. As a result, highly sensitive information is being put at risk.

New strategies for combating malware threats must move beyond existing detection approaches to focus on filling gaps that allow zero-day, polymorphic, and evasive malware attacks to succeed regularly. These gaps occur because existing malware analysis tools (anti-virus, EDR/EPP, email security, and dynamic analysis or 'sandboxes') are too narrow in focus, too slow, too reactive, too easily defeated, or a combination of all these problems.

The reality is that advanced malware threats, especially ransomware attacks, have become increasingly successful in the legal sector as existing security tools fall short in their ability to effectively protect organizations.

The True Impact of a Data Breach

Trust and confidentiality are everything in the legal industry. As such, it's imperative that sensitive client data and other private information remain protected from cybercriminals. The impact of a data breach can have severe ramifications that go beyond monetary costs and result in substantial damage to the reputation and integrity of a business, not to mention legal liabilities and regulatory penalties.

It is vital for law firms and legal teams to understand all the potential consequences of a breach, both direct and indirect, including:

- **Data Breach Notification Costs:** Organizations may be required by law to notify affected individuals and regulators in case of a data breach. These notification costs can include sending out notifications, providing identity theft protection services, and any legal fees for defending against lawsuits resulting from the breach.
- **Regulatory Fines and Penalties:** Many regulatory bodies can levy fines and penalties for non-compliance with security and privacy regulations. Organizations that fail to comply with these regulations may face significant fines and penalties.
- **Legal Fees and Settlements:** The organization may face significant legal fees and settlement costs if a security breach results in lawsuits or other legal action.

- **Reputational Damage:** A security breach can damage an organization's reputation, making it harder to attract new customers, employees, and investors.
- **Loss of Revenue and Business Opportunities:** Damage to an organization's reputation erodes customer trust, resulting in a loss of revenue and business opportunities. This can be especially damaging for legal organizations, which rely on customer trust and confidentiality to do their jobs effectively.

The consequences are very real, as evidenced by a growing list of high-profile attacks on legal organizations, including eight law firms that made headlines in 2023 after experiencing data breaches that exposed sensitive client and firm data. These particular breaches resulted in very costly fallouts that included large ransom payments and spawned multiple class action lawsuits.

Challenges Facing Today's Legal Teams

It's not uncommon for hundreds or even thousands of files to be exchanged as part of the e-Discovery process for a single case. In addition to the sheer volume of data, modern legal discovery involves more complex file structures, larger file sizes, and a multitude of file formats. The need for high-speed, in-depth file analysis has become essential to protect against advanced malware threats.

Unfortunately, many law firms and legal teams are hindered by inefficient and ineffective malware analysis solutions. An all-too-common scenario is the reliance (often over-reliance) on endpoint security tools and sandboxes to keep their organizations safe. And, while these solutions have an important role to play in an organization's security infrastructure, they're buckling under the growing file analysis demands placed on them. They simply lack the scale, breadth, and performance requirements to handle the volume, formats, sizes and overall complexity of files and data associated with today's e-Discovery process.

The limitations of these security tools have led to backlogged processing queues, bottlenecks in workflows, and even worse, files going unanalyzed. All the while, dangerous malware is slipping through the cracks with the potential to cause detrimental impact to the business.

It's evident that the legal industry needs a new approach to cybersecurity and malware detection. A successful solution must be fast, accurate, and scalable, while seamlessly fitting into existing workflows and processes. This is where Spectra Analyze excels.

ReversingLabs' High-Speed, Complex Binary Analysis

ReversingLabs Spectra Analyze is powered by a proprietary malware analysis engine that uses AI-powered complex binary analysis to rapidly assess large volumes of complex files and data objects, including obfuscated files that can evade other security systems. Spectra Analyze can identify more than 4,800 file formats across Windows, MacOS, Linux, iOS, and Android platforms and unpack over 400 file formats, including archives, emails, documents, multimedia, and software packages—providing the widest coverage in the industry.

Our complex binary analysis technology recursively unpacks and fully dissects the internal contents of files in milliseconds without execution, obviating the need for dynamic analysis in most cases. Files are checked against billions of malware and goodware samples in our continuously growing file reputation database to provide the most up-to-date, authoritative file intelligence with verifiable threat classification, enabling organizations to make quick and informed decisions.

Very importantly, Spectra Analyze replaces slow manual workflows by providing a robust API and built-in connectors for automated analysis process integration. This includes direct integration with cloud storage, network file shares, and email platforms for automatic file ingestion, as well as seamless integration with leading SIEM and SOAR platforms and third-party sandboxes. The result is more efficient, more effective, and more intelligent workflows.

Finally, in contrast to other popular platforms, ReversingLabs provides extensive privacy controls including private file analysis and private content repositories that ensure sensitive and confidential data does not become publicly accessible and remains secure from prying eyes.

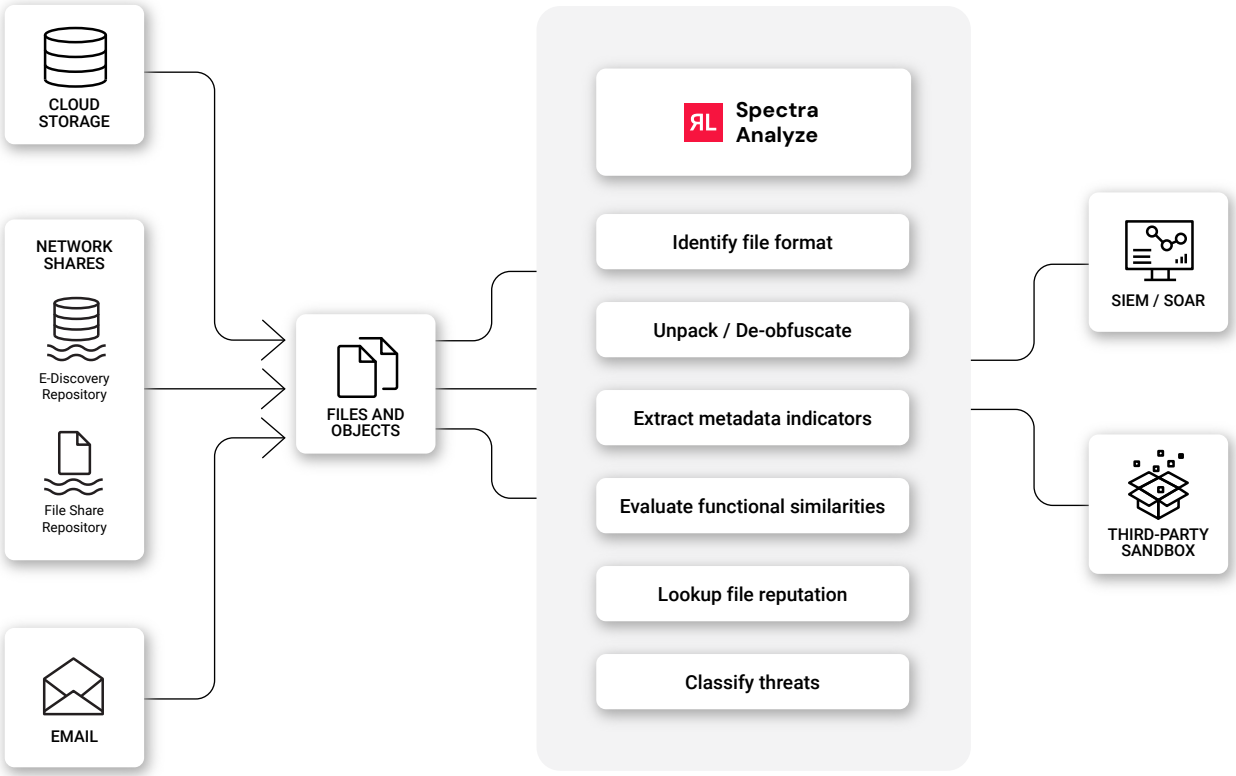


Figure 1: ReversingLabs High-Speed Complex Binary Analysis

Key Features

- Proprietary AI-powered, complex binary analysis
- Files analyzed in milliseconds to support real-time, high-volume processing
- Unmatched visibility into complex file structures to detect embedded malware at the deepest levels
- Broadest coverage in the industry with the ability to identify 4800+ file formats and unpack over 400 file formats
- Largest accessible repository of goodware and malware with tens of billions of files, and millions more added daily
- Continuously monitored for the most up-to-date file reputation status and intelligence
- Private file analysis for sensitive and confidential data requirements
- REST API for automated analysis process integration
- Direct integration with network file shares, cloud storage, email, SIEM/SOAR, and third-party sandboxes
- Multiple deployment options, including on-premises virtual appliance, cloud-based appliance, or hosted service

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

Get Started!

See how ReversingLabs can help detect and analyze even the most complex malware threats hiding in your files.

REQUEST A DEMO

www.reversinglabs.com

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com