REVERSINGLABS

SOLUTION BRIEF

ReversingLabs Solutions for Managing your Web & Mobile App File Upload Risks

BRINGING TRUST TO YOUR DIGITAL BUSINESS

DIGITAL TRANSFORMATION HAS BEEN DEFINED AS:

> The process of using digital technologies to create new - or modify existing - business processes, culture, and customer experiences to meet changing business and market requirements.

Digital Transformation

Organizations are embracing digital transformation because it’s essential to optimizing their business processes, creating compelling customer experiences, and providing resilience to changing business climates. Digital transformation requires creating a digital business and using technology to achieve competitive advantage. And by having meaningful data generated through these new digital systems enables actionable business decisions.

Industries have begun to realize this transformation, as evidenced by the following scenarios where digital technology has become an integral part of their business processes:

- **Media** - leveraging digital channels to accelerate archive and distribute rich media files to broadcasting and streaming companies, as well as consumers.
- **Design & Manufacturing** - collaborating across global teams to accelerate the design-to-production cycles, to the point of cost effectively“personalizing” products and services.
- **Financial Services & Banking** - enabling mobile and Internet banking to expedite transactions like mobile deposits and payments, as well as online document processing for loan applications.
- **Retail & eCommerce** - moving the entire shopping experience online through digital catalogs, digital shopping cards, order processing and fulfillment.
- **Healthcare** - providing telemedicine and electronic medical records, including digital lab and radiology results that support a better doctor-patient engagement.
- **Insurance** - accelerating claims processing by streamlining field appraisals, facilitating remote estimates and adjustments, and ultimately dispersing funds to policy holders in the case of an accident.
- **Oil & Gas** - supporting field contractors surveying remote natural gas and oil sites in their resource discovery and management, and uploading seismic and well data to the central office for analysis and development.
- **Architecture, Engineering & Construction** - facilitate collaboration across numerous disciplines, including structural, HVAC, electrical, etc. to coordinate massive build projects.

These specific Line of Business (LoB) activities have been achieved through digital processes and the sharing of digital files. And with these new digital business models come new threat vectors which place the responsibility for security back on the businesses. These digital transformation investments often came with the realization that "we have to build our digital platform," which requires both software development as well as a plan to secure these digital assets.

THE CLOUD AND YOUR DATA

Digital transformation isn't possible without an investment in the cloud because cloud is the enabler for your digital journey- as well as Mobile which benefits from access to cloud resources. And while cloud is the enabler for digital transformation, data is the backbone. Having a data-driven business, collecting and analyzing data about your customers as well as measuring what's happening inside your company is table stakes. You need timely access to substantive information to make strategic as well as tactical decisions often centered on accelerating time to market, prioritizing resources and investments, satisfying markets served, and reducing costs.

But data is more than transactional, digital content is now core to your business - it is an asset that defines your competitive advantage. Digital documents, images, videos, design & engineering diagrams, etc drive your new digital processes and are constantly in motion both inside and outside your organization. These "files" are the common denominator across digital business processes, and they are getting increasingly larger and more complex as more data is "packed" into these discrete objects to enrich and share.
And as these files are shared, trust is paramount. That requires consideration for ensuring good hygiene of these digital resources and maintaining the integrity of the digital process. Retaining trust across this new digital ecosystem is paramount, and without it the process breaks.

It's about Your Files

Files are the fuel that drive digital business and facilitate the exchange of information. They make your data portable, enable better collaboration and decision making, and keep your digital processes moving forward. Files are associated with formats which define a structure and carry content which applications can read and act upon, yet their content may also include unstructured data often generated by the user.

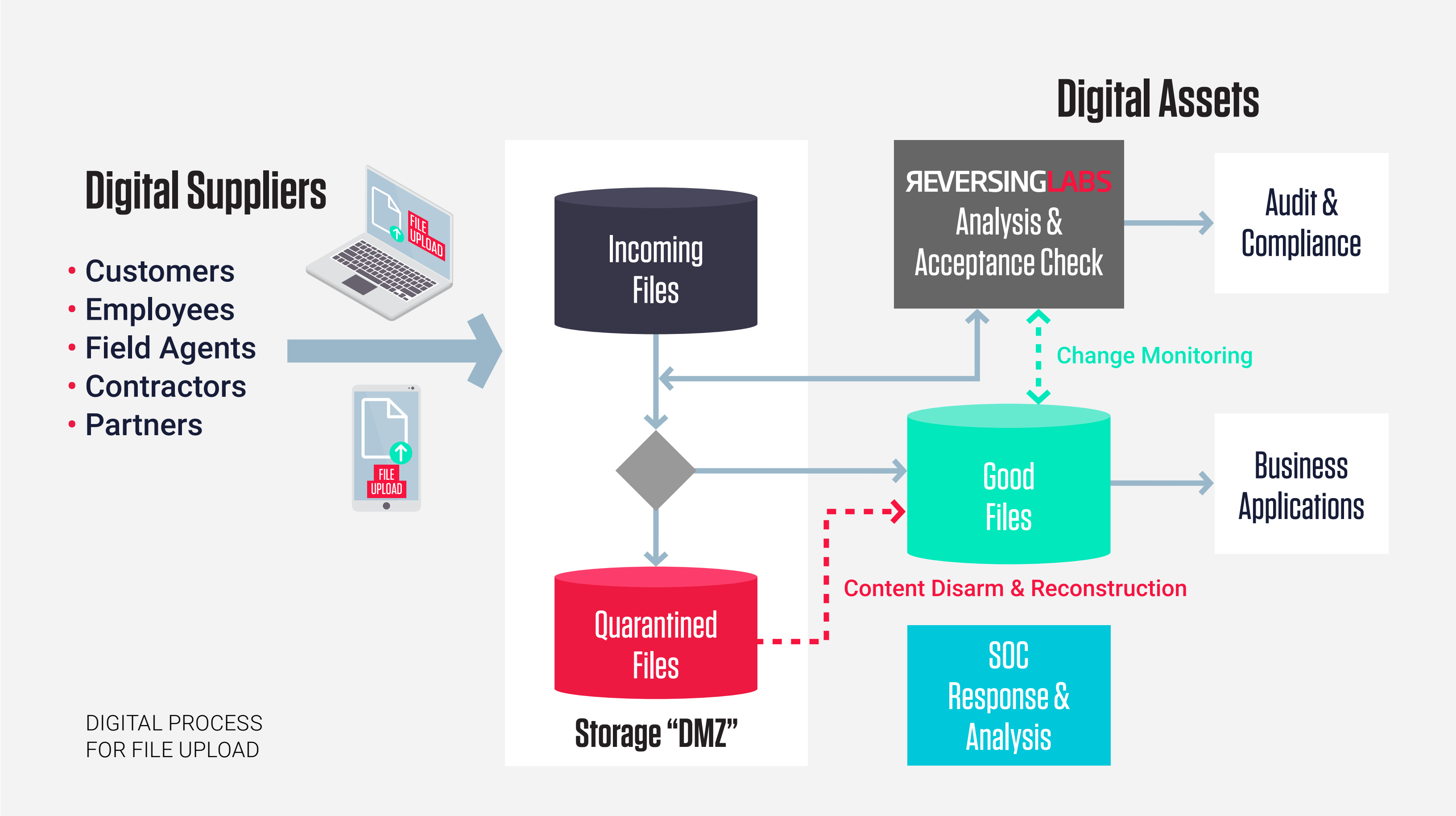
As more and more data is being assembled into a file, attackers find opportunities to introduce malware or malicious content- transforming the file into a destructive object. The term "files'' really represents all your binary objects, which can also represent compound and recursively packed files with numerous types of digital data. With today's increasingly content-rich environment, and its numerous formats and structures, these objects can potentially be transformed into "destructive objects" as attackers find new ways to compromise these binaries and deliver their payloads to their targets.

NEW INITIATIVES FOR FILE UPLOADS

An emerging use case in digital process workflows is the concept of a "Storage DMZ" as a place to receive incoming files and inspect before entering the secure zones within the enterprise.

The security architecture to support this use case typically requires 3 key folders, e.g. AWS S3 buckets, as part of the file upload analysis process:

- **Incoming** - receives files from digital suppliers, perhaps over the web or via mobile apps
- **Good** - receives verified clear files following analysis and quality checks
- **Quarantine** - receives files identified as malicious or suspicious requiring further investigation



And there are several levels of integration that connect this analysis service to the various file repositories:

- Access files in **Incoming** folders - enables the analysis service to inspect files.
- Route files to **Good** folders - directs good files for ongoing use by applicable business applications and processes.
- Route files to **Quarantine** folders - directs malicious files to an isolated folder for further investigation, and potential cleaning and subsequent "good" re-routing.
- Access files in **Quarantine** folders - enables further investigation by the security operations team or any cleaning/sanitizing resources available.
- Access files in **Good** folders - enables ongoing monitoring of files to ensure any changes in classification as a result of new malware discoveries are applied to prior inspected files.

YOUR FILE RISKS

Digital content is increasing in every key metric - volume, format, size, and complexity and these trends pose challenges for legacy security controls.

Volume

As more digital content is shared and exchanged, and demand for richer content grows, the size and volumes of these files is increasing. Analysts predict over 60% CAGR of the world's datasphere, or the collective sum of the world's data, with 50% of this data expected to reside in public cloud storage by 2025. Legacy systems often lack the efficiencies and elastic architectures which can scale to meet these challenges.

Format

There are thousands of file types out there representing document, graphic, Microsoft Office, scripted, archive, virtual machine, container, multimedia, audio, video and streaming formats (the ReversingLabs supported formats list for reference). And there are numerous legacy and deprecated formats that remain in use supporting old systems and applications or perhaps proprietary business activities, which are no longer supported by legacy security engines.

Size

Files are increasing in size and complexity, and playing an important role in making data “portable”. With larger files it takes more time to decompose and parse in order to find malicious indicators - many security technologies simply pass over these files (e.g. AVs traditionally have a 200MB limit).

Complexity

Files can be recursively packed in order to compress size and make them more efficient in transport and storage, however these same techniques can be used to obfuscate malicious intent and content. The concept of compound objects, or files that comprise many different components within them, is common practice within legitimate document structures so it’s prudent to completely unpack and examine all elements of these objects for any hidden malware.

Other Risk Factors

There are additional risks encapsulated within digital objects that can easily go unchecked, including:

- Malformed and expired certificates.
- Embedded URLs.
- Untrusted or unverified sources (representing content from 3rd party sources which lack a chain of trust and may introduce unwanted or malicious content unknowingly - e.g. common cloud file shares and software supply chain repositories).

While both networks and storage have expanded incrementally to address these factors, modern security defenses have not always been factored into the solution architecture.

WHERE DOES LEGACY SECURITY BREAKDOWN

The problem of threat detection is a complicated one, and addressing all the formats available to attackers is challenging. There are thousands of different formats, themselves complex in nature with different structures making it difficult to decompose and inspect. Many security solutions opt to focus on a subset, however this leaves a sort of backdoor for attackers to pursue.

Legacy solutions such as anti-virus (AV), and in special cases sandboxes, have a role to play in the security ecosystem, but not necessarily as the default solutions to address the high capacity file analysis needs of digital business and modern architectures. They simply lack the scale, breadth, and performance requirements to process the volumes, formats, sizes and complexity associated with file upload activities. These AV and sandbox security technologies simply can’t deal with the vast array of binary formats, extensive packing, and large sizes which are leveraged by attackers today. And should these objects go unanalyzed due to lack of support, a backlogged queue, or simply cost too much to scale, this represents a problem.

Your Security Strategies for Modern Architectures

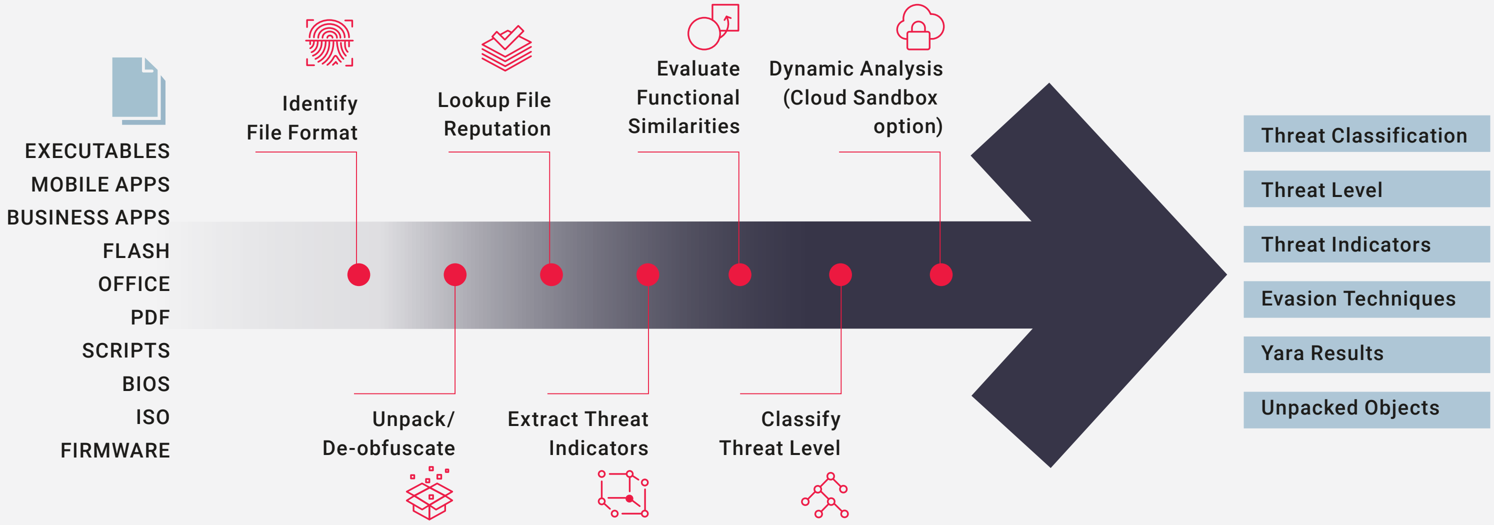
Given growing trends toward cloud-centric solutions, the need for new security strategies and new controls should be a top consideration among digital transformation stakeholders in addressing new and existing digital assets. Scalability, speed, breadth, and integration would be immediate topics that come to mind. Interestingly, Harvard Business Review concluded that many digital initiatives fail because they lacked the scalability needed to meet their business objectives, and that promises made during the POC (proof of concept) don’t materialize in the transition to large scale production. Despite AV and sandboxes being default security tools in nearly all enterprise environments, they simply lack the scalability for these high volume use cases- so don’t get caught by extrapolating small successes as fulfilling your full scale requirements.

So, if not AV or sandbox, what are the alternatives for confirming file uploads are safe? How does ReversingLabs scale, how does modern static analysis meet your security needs, and how can explainable threat intelligence optimize your operations?

WHY AUTOMATED STATIC ANALYSIS

I always say, you haven't seen static analysis until you experience ReversingLabs "automated" static analysis capabilities. ReversingLabs automates the process of unpacking, decomposing and extracting threat indicators at unprecedented speeds, across numerous operating environments (not just PE binaries). And we do all this without executing the files. Our breadth of coverage and ability to recursively decompose these complex objects to their base components, analyze all the different file types and scripts, and uncover threat indicators of compromise extremely fast, milliseconds in fact, is unique to ReversingLabs.

Stages of advanced Static & Dynamic Analysis



WHY EXPLAINABLE MACHINE LEARNING

ReversingLabs then takes action to classify these files, which includes many different analysis engines, including our patent-pending explainable machine learning. Ultimately we serve up intelligence that is human readable and actionable. We highlight not only our conclusion or conviction, but also the evidence behind our decision and explain how we came to our verdict. This explainable threat intelligence can then be applied by defenders and analysts, as well as the automated decision support systems that power response workflows and controls, to take action. By exposing not just a verdict or classification, but all the attribution behind our conviction, we deliver a level of transparency not available from other security solutions. An easy way to view this paradigm shift is the analogy of transitioning from a "black box" to a "glass box" solution approach. Why is this important- because there are Level 1, 2, and possibly level 3 analysts involved in responding to the alerts and security incidents flooding the SOC, and they require timely intelligence with actionable insights, and the supporting evidence to justify their actions. With the added confidence in these threat detections, verdicts, and classifications, analysts are better positioned to promote a much faster response and in many cases qualify actions to proceed automatically.

Conclusion

In evaluating your security strategies to manage your digital assets, your developing digital business processes, and your corresponding cloud architectures that support these resources, I wanted to offer 5 key factors to consider in incorporating security into your file upload architecture:

SPEED AND SCALE

Your solution should have minimal latency and scale to process the file volumes (potentially hundreds of millions of files per day), sizes (GB files), and complexity (recursive packing into the hundreds) to ensure your digital business remains responsive to your suppliers.

BREADTH

Your solution should have the capacity to support thousands of file formats, across numerous operating systems, with an architecture that is expandable to meet changing environments.

SIZE AND COMPLEXITY

Your solution should have the capacity to inspect large file payloads and recursively unpack complex objects to expose hidden malware.

CLOUD-READY

Your solution should support running in the cloud or hybrid-cloud environment you chose, so if you are planning to have your Storage DMZ in an AWS S3 bucket, your security solution should have the option to run in AWS.

SOC-ENABLED

Your solution should interface with your Security Operations Center (SOC) as your organization's central point for managing security alerts, events, and incidents - and formulating response plans to minimize file and process risks.

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com