FUJITSU

A daunting task of Office macro management

Faced with 900,000 files requiring macro based risk assessment, the agency pivoted to Macrosine, reducing costs and accelerating completion timelines

Challenge

Like many organisations, an Australian government agency faced the challenge of effectively assessing and managing a vast number of Office macros. The project uncovered a staggering 900,000 files requiring validation, far more than initially anticipated. Faced with the monumental task of manually assessing and securing these files, the agency deployed a sandbox environment to isolate and analyse the macros. However, despite these efforts, the project's scope and complexity quickly escalated, threatening to overrun both budget and timelines.

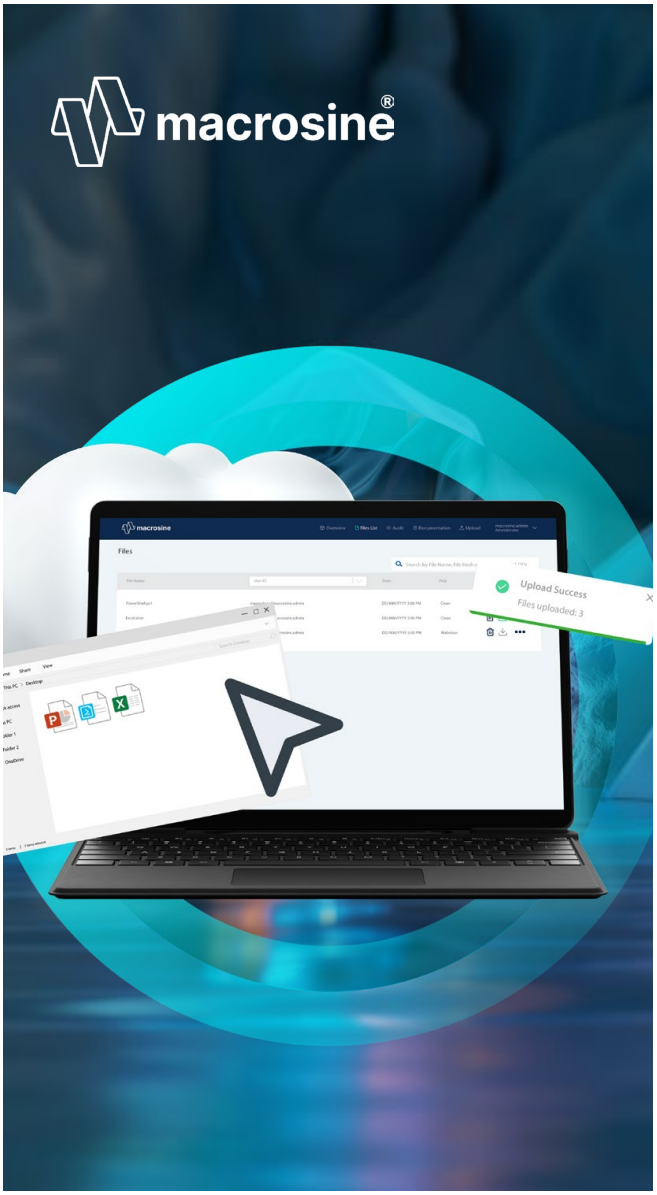
Solution

Fujitsu introduced Macrosine, a tool that automatically assesses and digitally signs Office macro files.

Key features included:

- **Automation at scale:** Eliminated manual checks, reducing human error.
- **Sandbox testing:** Ensured secure validation of macro behaviour.
- **Subscription model:** Delivered flexibility and cost efficiency.

By adopting Macrosine, the agency not only mitigated immediate risks but also built a foundation for continuous protection. This approach enabled the agency to pivot from reactive risk management to proactive security assurance.



Outcomes

Fast, cost-effective, and sustainable cybersecurity

The transition to Macrosine marked a turning point in the agency's cybersecurity strategy. Within a few weeks the agency experienced transformative results. Macrosine enabled the project team to address the risk with speed and efficiency. By providing automated self-assessment and certification of macros, the tool not only significantly reduced project costs but also eliminated the uncertainty around the project's completion. Macrosine offered a scalable and sustainable approach to managing macro-related risks and PowerShell files.

If Office macros are not controlled ...

Office macros represent a security risk as malicious actors can embed malware and try to bypass security controls and gain access to systems. Opting to block all macros may seem like a comprehensive risk mitigation tactic, but it's not entirely effective. While allowing all macros can inadvertently permit the operation of malicious software. The remaining alternative involves the manual evaluation of each macro, which demands a considerable amount of investment of time and resources, making it a less than ideal solution.

Automate security scanning and digital code signing

Data stays within your environment

Reach regulatory compliance, such as Essential 8 Level 3 for Australian businesses

Bulk upload and queued file scanning with configurable user permissions

Are you still manually assessing, blocking or allowing all macros?

Book a demo with one of our experts and experience Macrosine for yourself