How is your organisation managing Office macros?

Blocking all macros

Blocks all the risk (but doesn't really)

- Severely impacts productivity
- Users forced to circumvent controls
- Creates frustration

VS

Allowing all macros

Everything runs (including malware)

- Hard to keep on top of and teaches users bad habits
- Waste time and money with incident response
- Highly likely something will be missed

VS

Manually assessing

Macros can run (but with delay)

- Very security resource intensive
- Slows users (reducing the benefit of macros)
- Advanced payloads with sneak through

We created a better way

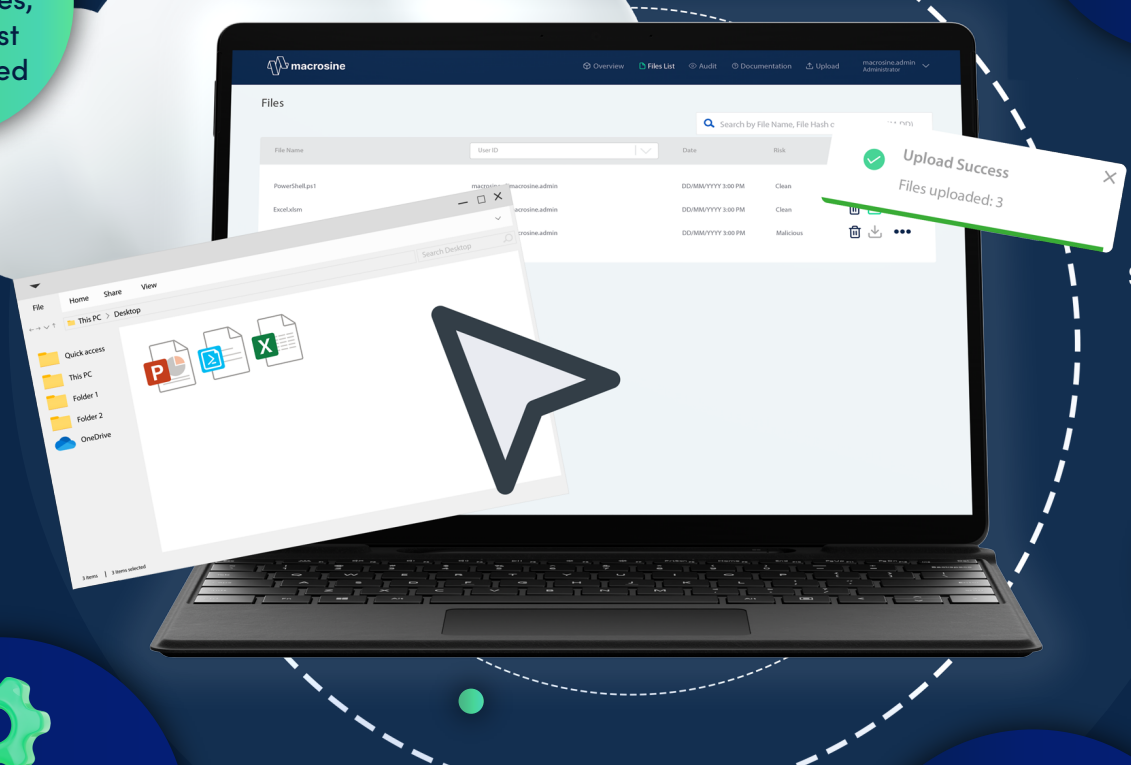
macrosine

Detailed logging and auditing

Enhanced cybersecurity

Reach **Essential 8** Maturity Level Three

Empower users to secure their own files, no specialist skills required



Integration with **Service Management** tools

Bulk upload and queued file scanning

FORTINET
Powering the Macrosine threat assessment

Automate security scanning and digital code signing

Configurable user permissions

Streamlined process of ensuring **PowerShell** scripts are safe and trusted.

Data stays within your **environment**

Ongoing product support and updates

Meet regulatory **compliance:**

- ACSC — The Australian Cyber Security Centre — Essential 8
- ADHA — The Australian Digital Health Agency
- AESCSF — Australian Energy Sector Cyber Security Framework
- PSPF — Australian Protective Security Policy Framework

Discover how Macrosine can help you save time and enhance security

macrosine

Created by oobe, a Fujitsu company

Book a demo

Macrosine.com.au

Only Macrosine offers enhanced cyber security by mitigating the risk associated with Microsoft Office macro and PowerShell code.