FUJITSU

Office macro security made simple

Powered by macrosine®

If macros are not controlled ...

they represent a security risk as malicious actors can embed malware and try to bypass security controls and gain access to systems.

Macro risk dilemma

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.

Macrosine is trusted by Government Departments and organisations across Australia.

We created a better way

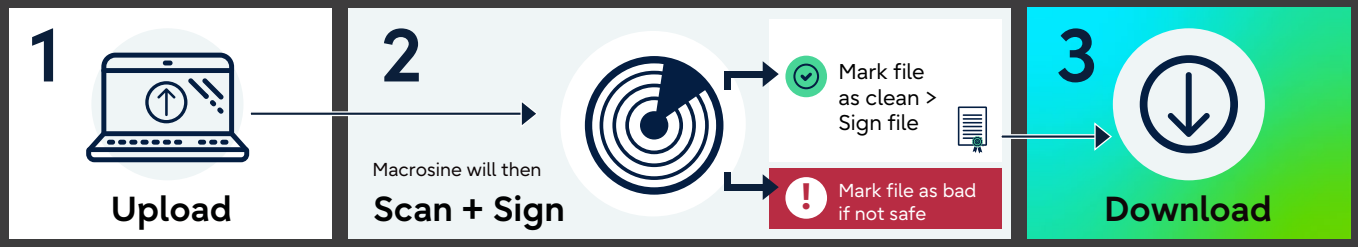
Introducing Fujitsu's macro tool 'Macrosine' Combining an intuitive portal interface and a world class security scanning capability, Macrosine has all the tools you need to assess and secure Microsoft Office macros. Installed either on-premises or in Microsoft Azure, it provides a simple, self-service portal to risk assess code, reduce the risk of cyber-attacks, and help you meet regulatory compliance obligations.

Securing productivity without compromise

- Automate security scan and signing
- Meet regulatory compliance
- Eliminates unauthorised access
- Data stays within your environment

How it works

Users upload macro-enabled files, which are automatically scanned, digitally signed, and returned safe to open and compliant with security policies.



Upload the file via the web portal

File is assessed via a sandbox

Download the signed file

macrosine®

Continuous macro protection

"Macrosine has successfully detected potentially malicious code in our files, providing us with much-needed security assurance. It's a critical part of our threat detection strategy."

Macrosine customer

Automate security scan and digital code signing

Sandbox/detonate suspicious macros and ensure that only secure and authentic codes (macros and PowerShell scripts) are allowed to run in the environment.

Meet regulatory compliance

Australian Cyber Security Centre (ACSC), Australian Energy Sector Cyber Security Framework (AESCSF), Australian Digital Health Agency (ADHA), Uplift Essential Eight Maturity level.

Eliminates unauthorised access

Proven deployment that focuses on business role and file type-based permissions.

Data stays within your environment

Deployed within customer's on-premise infrastructure or in their Microsoft Azure environment honouring data sovereignty requirements.

Improved user experience

Low-touch operation for customers that allows for bulk upload, queued file scanning and self-service portal capabilities.

Cost effective based solution

The most efficient deployment and support approach to securing macros with integration into service management tools.

- Supports Word, Excel, PowerPoint, and more
- Support for files beyond macros, including PowerShell
- Support via the portal, knowledgebase and release notes
- Detailed operating guides
- Granular access control
- Detailed logging and auditing
- Flexible deployment options
- Easy to use self-service portal
- Saves time and effort

Fujitsu is the only authorised provider capable of deploying Macrosine, including in Azure Protected and on-premises configurations.

Get in touch

Fujitsu Cyber

www.fujitsu.com/au/services/security

Macrosine.com.au