SignPath

Built, Signed, Delivered.

Microsoft Office Macros
A Weak Spot in Endpoint Security

Use SignPath to sign your Office macros – and never worry about macro-based malware again.

Macros are everywhere

Office macros are in wide use in most enterprises. From complex Excel calculations to content generation and extraction, teams use the simple programming tools provided by Office to automate core business processes.

Flexibility over Security?

This decentralized and accessible approach boosts productivity and agility, but it also presents a clear risk: Office macros can carry hostile code, and the flexibility of the Visual Basic engine in Office applications has opened the door for too many attacks.

Social Engineering

Users often don't think twice before opening documents from coworkers – real or impersonated. They don't look like the programs they have been warned about, and what else are they supposed to after all? Warnings are easily ignored, especially if the email or the document itself says so. Macros are a social engineer's dream.

Macros are Super Spreaders

Documents are shared – that's what they for. Users will send them along further when asked. Nothing spreads faster than malicious program code in a macro.

SignPath

Built, Signed, Delivered.

The Solution: Sign Path

SignPath provides policy-driven code signing for Office macros.

With code signing in place, administrators can simply lock down Office security policies to prevent execution of unsigned macros.

No matter where documents and templates are stored, signatures reliably identify safe macros and prevent unauthorized modification.

Social engineering is prevented by hard policies instead of relying on weak warnings. Only approved macros will be executed, no matter who really sent that email.

Users can edit the contents of documents and templates without breaking the macro signatures. Updates to macros require new signatures.

Policy-Driven Code Signing

SignPath is a professional solution for code signing. It covers you from basic physical key security to flexible signing process to auditing. Policies are centrally defined, but locally executed and automatically enforced.
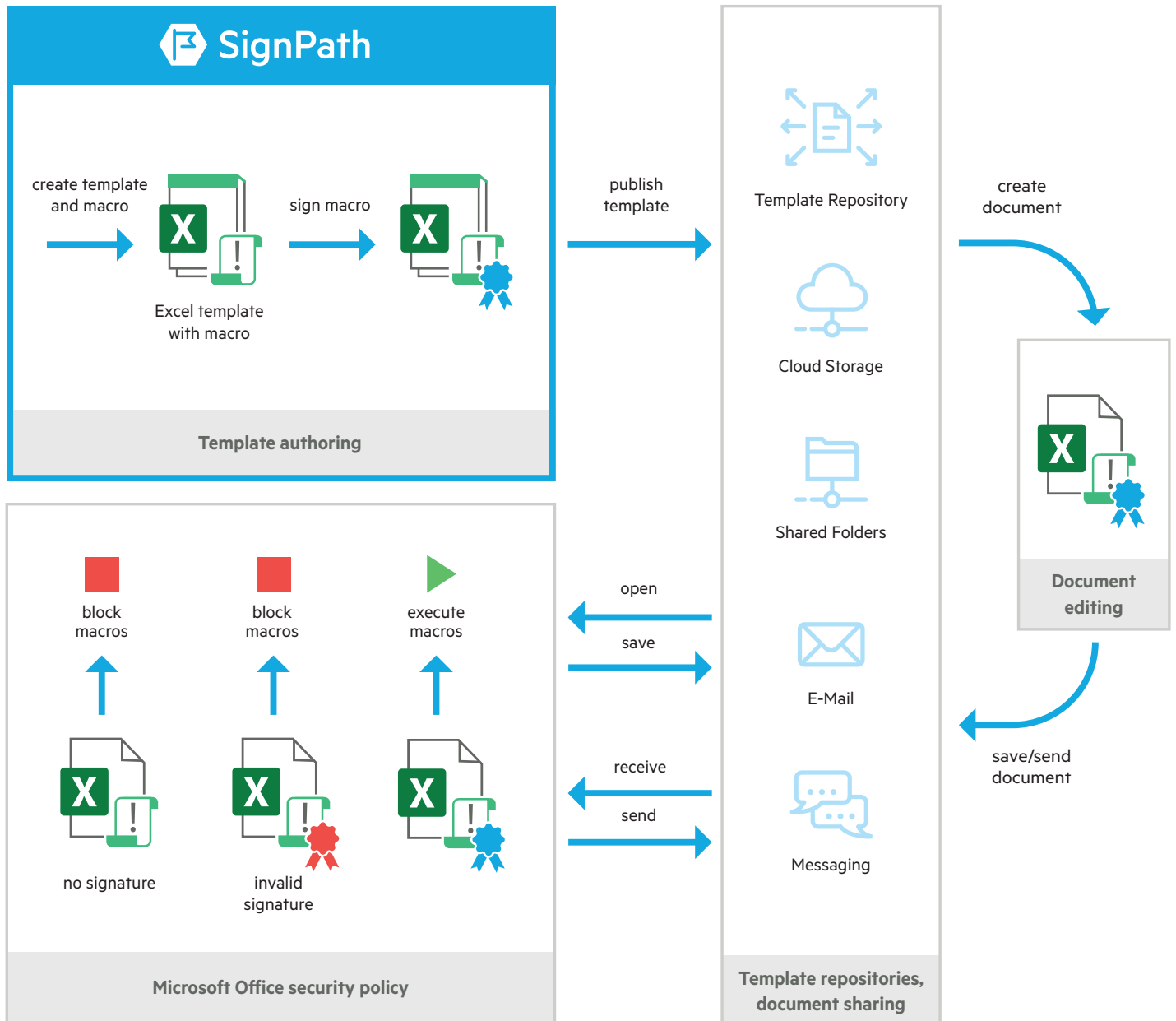
The organization sets the policy. Assign signing permissions to macro and template authors, define additional approval requirements, or integrate macro signing in a formal code review process – SignPath has you covered.

Workplace Security Policies

Administrators can globally control macro execution via code signing policies, or they can use differentiated policies. Maybe some macros are only used by the finance department, so why allow them in the legal department?
With SignPath, you can assign different signing permissions, processes and polices for these groups.

When you roll out the policies to your Office users, only the source of the macros matters. Whether a document was generated from a template on a file share, downloaded from SharePoint or received via email doesn't matter. A valid signature alone will allow macro execution.

SignPath

Built, Signed, Delivered.

SignPath

Template authoring

create template and macro → Excel template with macro → sign macro → publish template

Microsoft Office security policy

block macros ← no signature

block macros ← invalid signature

execute macros

Template repositories, document sharing

Template Repository

Cloud Storage

Shared Folders

open / save

E-Mail

receive / send

Messaging

create document

Document editing

save/send document

Excel ✓   PowerPoint ✓   Project ✓   Publisher ✓   Visio ✓   Word ✓

www.signpath.io

SignPath

Built, Signed, Delivered.

A Threat on the Rise

Many technologies have improved their security footprints. For example, while internet browsers occasionally need security updates, they are continuously tested, inspected, and improved by security experts around the world. Other dangerous technologies, such as Flash, just disappeared. It should not come as a surprise that hackers focus on other technologies.

Office macros are a powerful tool. Developers can use the full feature set of Visual Basic for Applications, read and write files, access the Internet, use COM objects, and start processes.

On the other hand, users don't expect that kind of power from a simple Office document. This combination makes Office macros attractive for hackers, at the same time as other technologies become harder to exploit.

Changing Security Landscape

In February 2022, Microsoft announced that macros would be blocked by default. While this was applauded by security researchers, that announcement was withdrawn after massive customer feedback. Too many organizations are not ready yet.

Signing your Office macros does not only prepare you for future changes, it also puts you in control. Once you provide secure macro signing to your organization, you can ignore the defaults and just turn off insecure macros for all users.

Your risk landscape will never be the same.

Get in contact with us

Did you know?

SignPath also offers build chain security and code signing for

- ✔ **Microsoft Office add-ins**
- ✔ **Windows PowerShell, VBScript, and JScript files**
- ✔ **Container images (Docker/Notary)**
- ✔ **Various executable, driver, installer, and package formats**

sales@signpath.io
+43 1 35 30 330

SignPath GmbH
Werdertorgasse 14
1010 Vienna

www.signpath.io