The common security weak spot

Unknown Device

⚠ Operating system out-of-date

⚠ Automatic OS updates disabled

⚠ Browser out-of-date

⚠ Disk Encryption disabled

⚠ Lockscreen disabled

+40%
of the devices used for work are **unknown / unsafe**

1/3
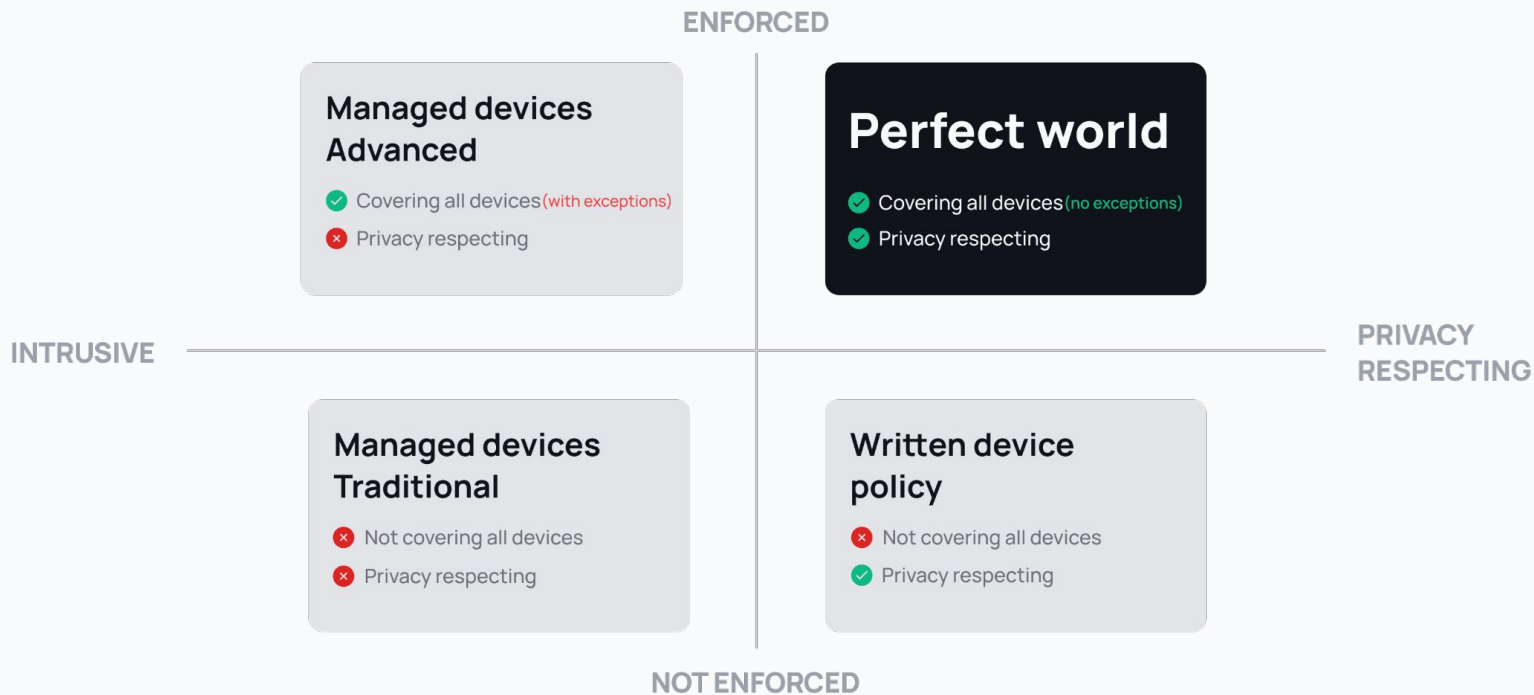Security incidents are **related to devices**

Ransomware Malware Phishing Theft

‹ **Reality of "edge cases":**
Personal devices/BYOD, devices from freelancers & partners, …

XFA

Device security landscape

ENFORCED

Managed devices Advanced

- ✅ Covering all devices (with exceptions)
- ❌ Privacy respecting

Perfect world

- ✅ Covering all devices (no exceptions)
- ✅ Privacy respecting

INTRUSIVE

PRIVACY RESPECTING

Managed devices Traditional

- ❌ Not covering all devices
- ❌ Privacy respecting

Written device policy

- ❌ Not covering all devices
- ✅ Privacy respecting

NOT ENFORCED

XFA

XFA, ensures that only safe devices can be used for work

True optimal device security
Broad compatibility & enforced security checks

Scalable compliance
Simplifying ISO 27001, SOC2, NIS2, DORA, ...

Easy on IT teams
User-friendly, self-onboarding

Privacy respecting (modern HR)
Supports BYOD, accepted by freelancers & partners

Work @ home   VS   Office

XFA

XFA Solution, how it works
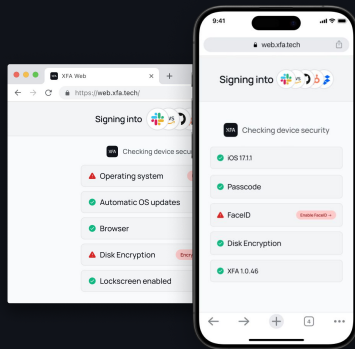
1

Authentication
User authenticates with existing identity provider.
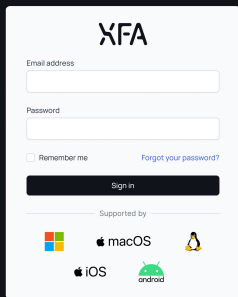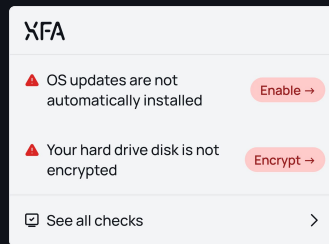
2

Security check
XFA performs **essential device security checks**, and approves/rejects access.

3

Remediation
User is guided by XFA to resolve device security issues.

4

Secure Access
Only secure devices have access to your organization's applications.

Integrates with: **Microsoft** · **okta** · **onelogin** by ONE IDENTITY · **Google Workspace** Pending Support

XFA