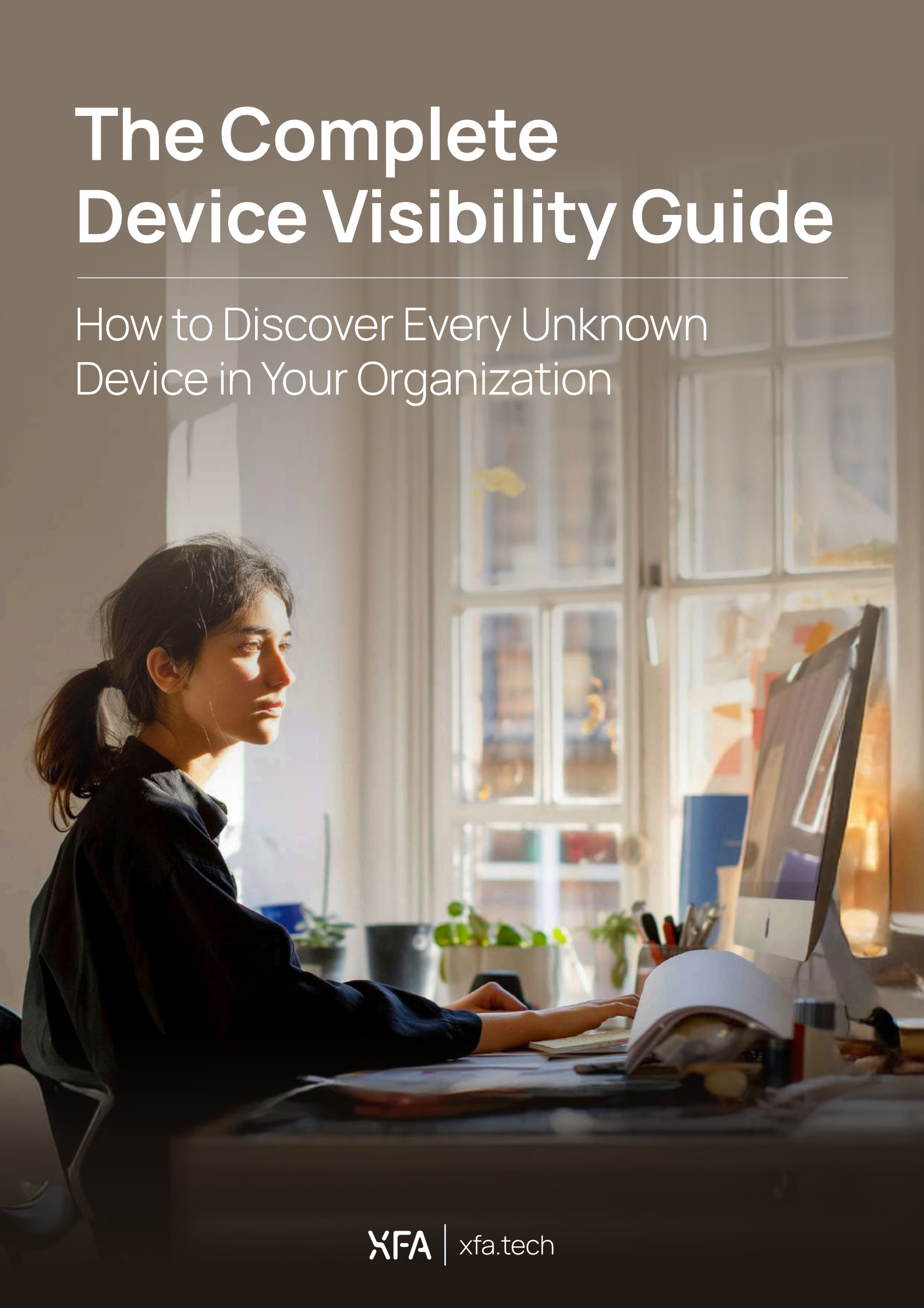
The Complete Device Visibility Guide

How to Discover Every Unknown Device in Your Organization

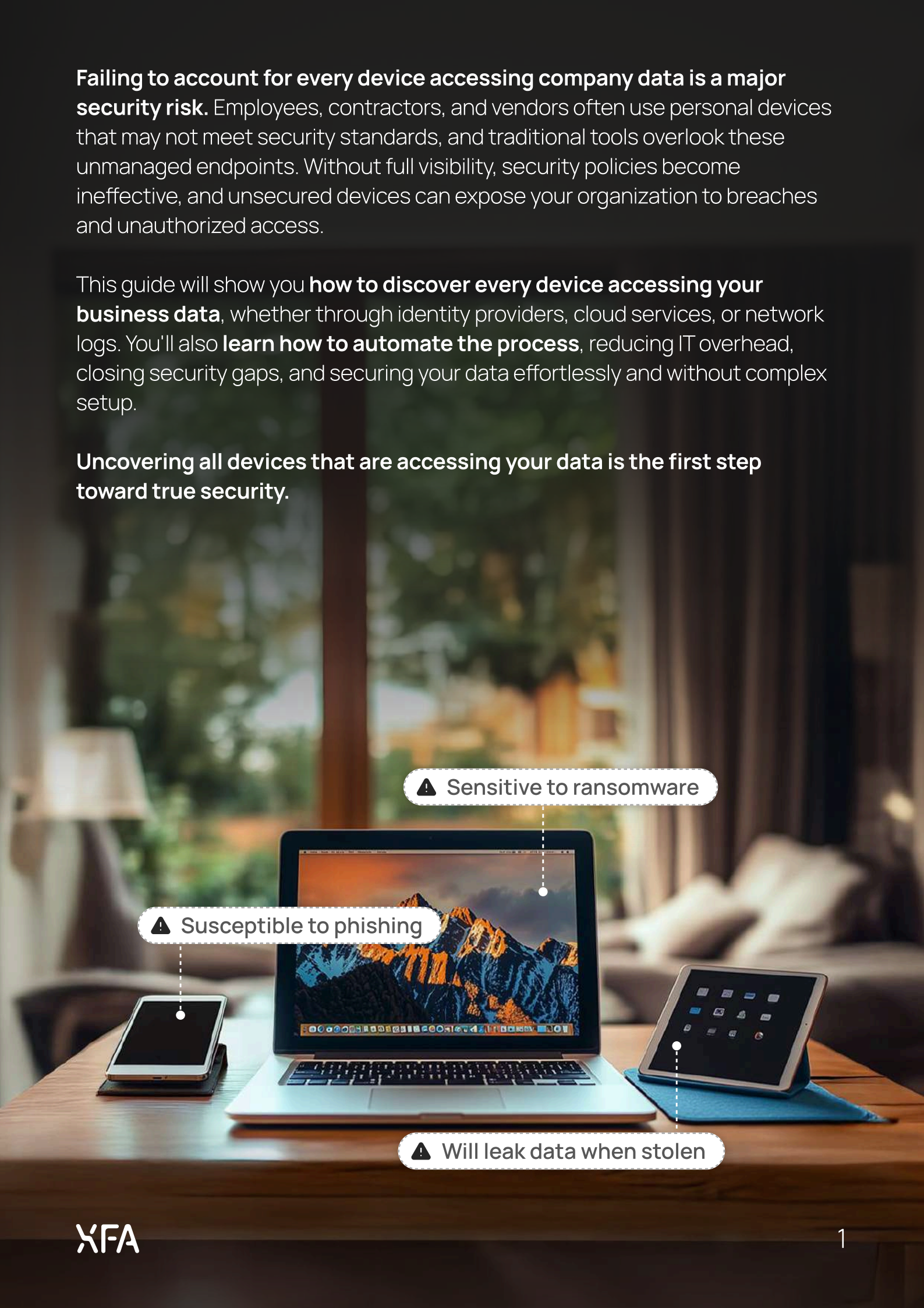


XFA | xfa.tech

Failing to account for every device accessing company data is a major security risk. Employees, contractors, and vendors often use personal devices that may not meet security standards, and traditional tools overlook these unmanaged endpoints. Without full visibility, security policies become ineffective, and unsecured devices can expose your organization to breaches and unauthorized access.

This guide will show you **how to discover every device accessing your business data**, whether through identity providers, cloud services, or network logs. You'll also **learn how to automate the process**, reducing IT overhead, closing security gaps, and securing your data effortlessly and without complex setup.

Uncovering all devices that are accessing your data is the first step toward true security.



Device Access Logs Analysis

To discover all devices accessing your business data, you need to **analyze multiple sources of logs** across identity providers, cloud applications, and network security tools. Each of these sources provides valuable insights. Manually gathering and analyzing this data can be time-consuming, complex, and prone to human error.

Option A

Identity Provider Logs (The Most Reliable Data Source)

Microsoft Entra (Azure AD) → Sign-in logs show every device used to access.
Okta System Logs → Tracks all logins and devices.
Google Workspace Admin Console → Reports login activities across devices.

Best for tracking all user logins & devices accessing your data.

These logs contain massive amounts of raw data, requiring manual filtering to extract meaningful insights.

Option B

Cloud Security Logs (For Cloud-Based Access)

Google Drive Audit Logs → Security → Login Audit
Microsoft 365 Security Logs → Compliance Center → Audit Logs
AWS CloudTrail Logs → Tracks AWS service access

Useful for detecting unauthorized cloud access.

Different platforms have different log formats, requiring IT teams to manually cross-reference logs to get a full picture. Some services only retain logs for a limited time, making historical investigations difficult.

Option C

Network Logs & Endpoint Security

Firewalls & VPN Logs (Palo Alto, Fortinet, Cisco Meraki)
EDR/XDR Security (CrowdStrike, Microsoft Defender)
MDM Solutions (Intune, Jamf, Workspace ONE)

Best for tracking all user logins & devices accessing your data.

These logs contain massive amounts of raw data, requiring manual filtering to extract meaningful insights.

How to Easily Discover Devices in Minutes (Without Manual Work)

Manually checking logs in multiple systems might be an overwhelming, inefficient, and time-consuming option. Fortunately, you can **automate device discovery** and gain full visibility in just a few steps, without deep technical expertise or hours of log analysis.

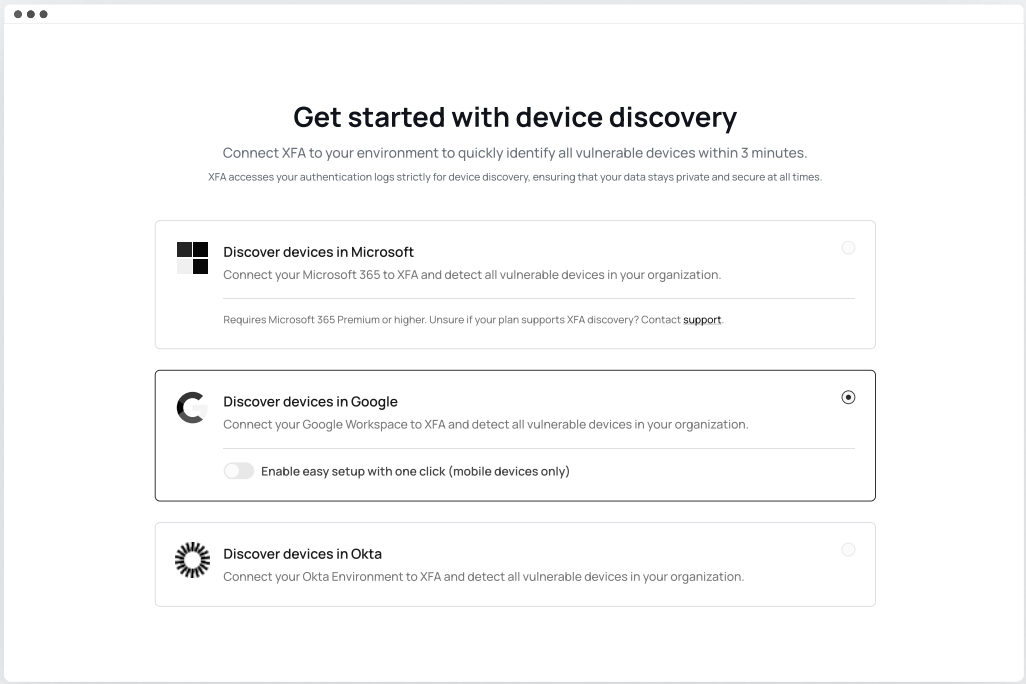
Using **XFA**, you can instantly scan your organization's authentication logs and generate a **comprehensive device overview** in just minutes.

How It Works:

1 Connect Your Identity Provider

To get started, you'll select your organization's **Identity Provider (IdP)** - the system that manages user logins: **Microsoft, Google, or Okta.**

This step allows XFA to securely connect and extract authentication logs to identify all unique devices accessing your business data.



2 Grant Secure Read-Only Permissions

To proceed, you'll need to **authorize XFA** to read your organization's authentication logs.

What does this permission allow?
→ Read-only access to authentication logs (No changes to settings, no data modifications)
→ Securely retrieves a list of devices without exposing sensitive company data
→ Protects against unauthorized access with industry-standard security measures

💡 **Concerned about permissions?** XFA only requests the minimum access needed to generate your device inventory and follows strict security best practices.

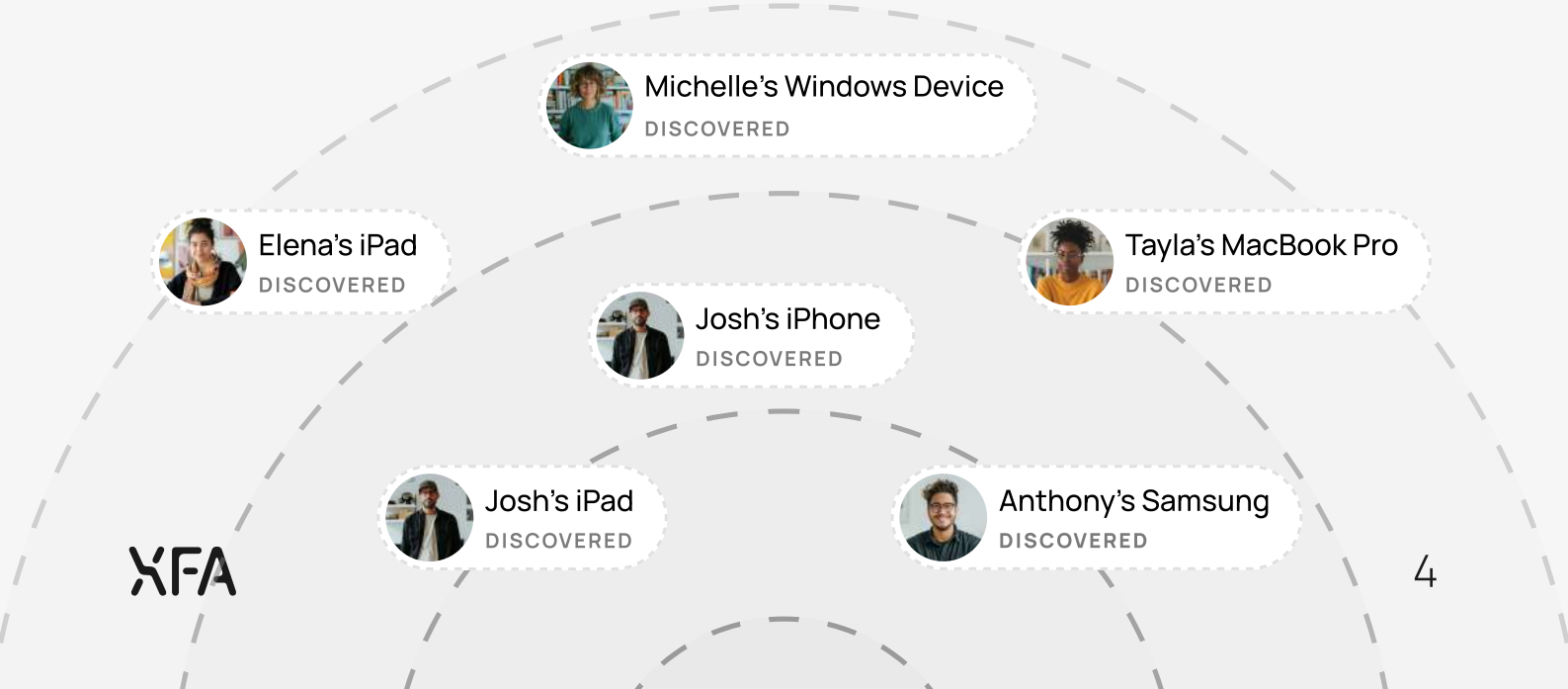
3 Automated Device Discovery

Once access is granted, XFA immediately starts scanning:
→ **Analyzing authentication logs** across Microsoft, Google, or Okta
→ **Identifying all unique devices** (company-owned, personal, unmanaged)
→ **Checking for security risks**, such as unauthorized or outdated devices

⏳ **How long does it take?** In most cases, the full discovery process takes less than 15 minutes.

4 Get an overview of Devices in Your Company

Once the scan is complete, you'll get:
→ A comprehensive **overview** on the security health of devices accessing your business data
→ **Potential security risks**



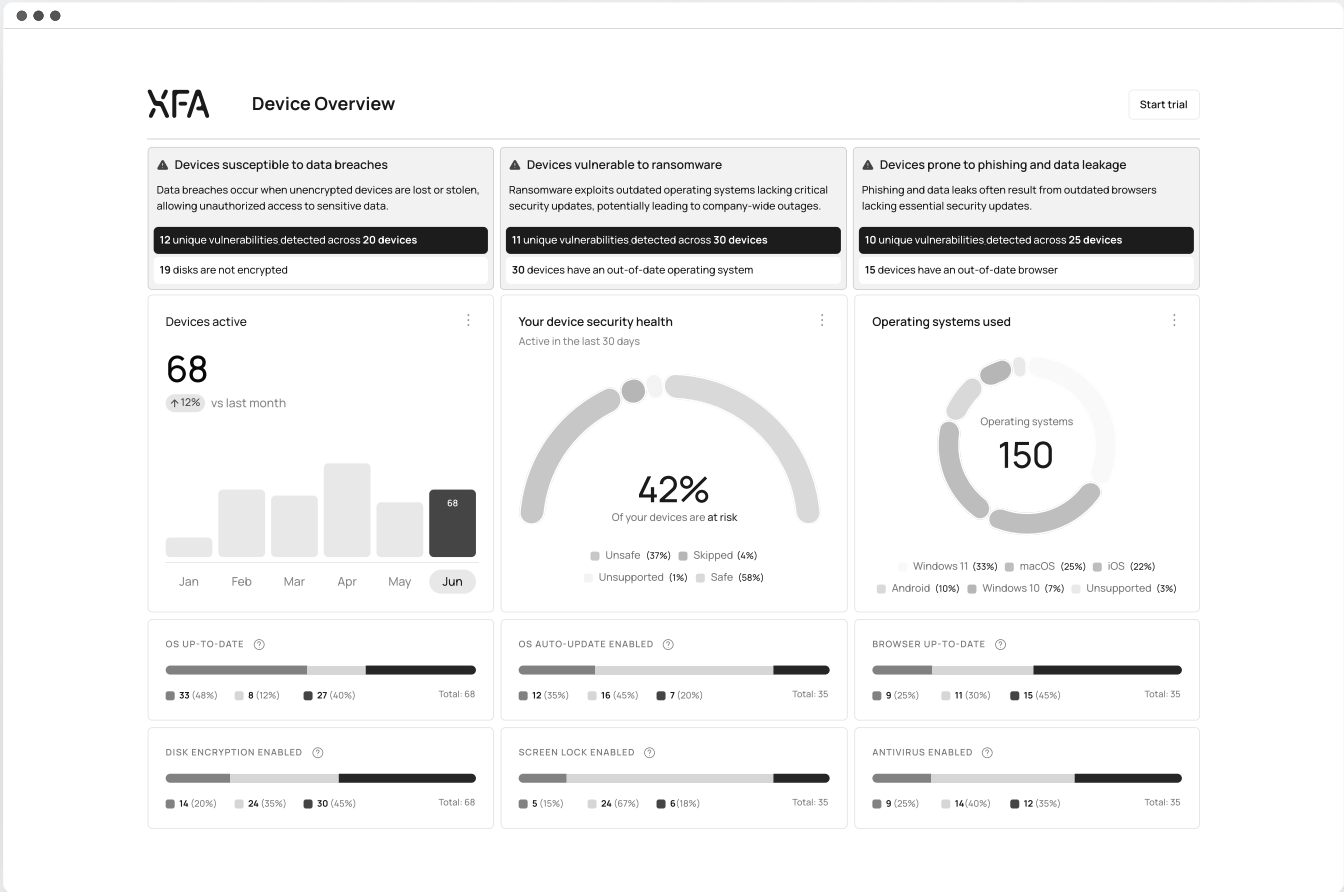
Want to Try It Out?
It's Free and Requires No Commitment!

Want to make the first step towards securing your organization's business data? Try out XFA device discovery for free and get a **real-time device security report in minutes.**

📌 Your report will include:

→ **Number of devices accessing your data** (company-managed & personal)
→ **Device OS** (Windows, MacOS, iOS, Android, Linux)
→ **Potential security risks** (Outdated operating systems, disk encryption disabled, screen lock disabled and more)

Get Your FREE Discovery Report



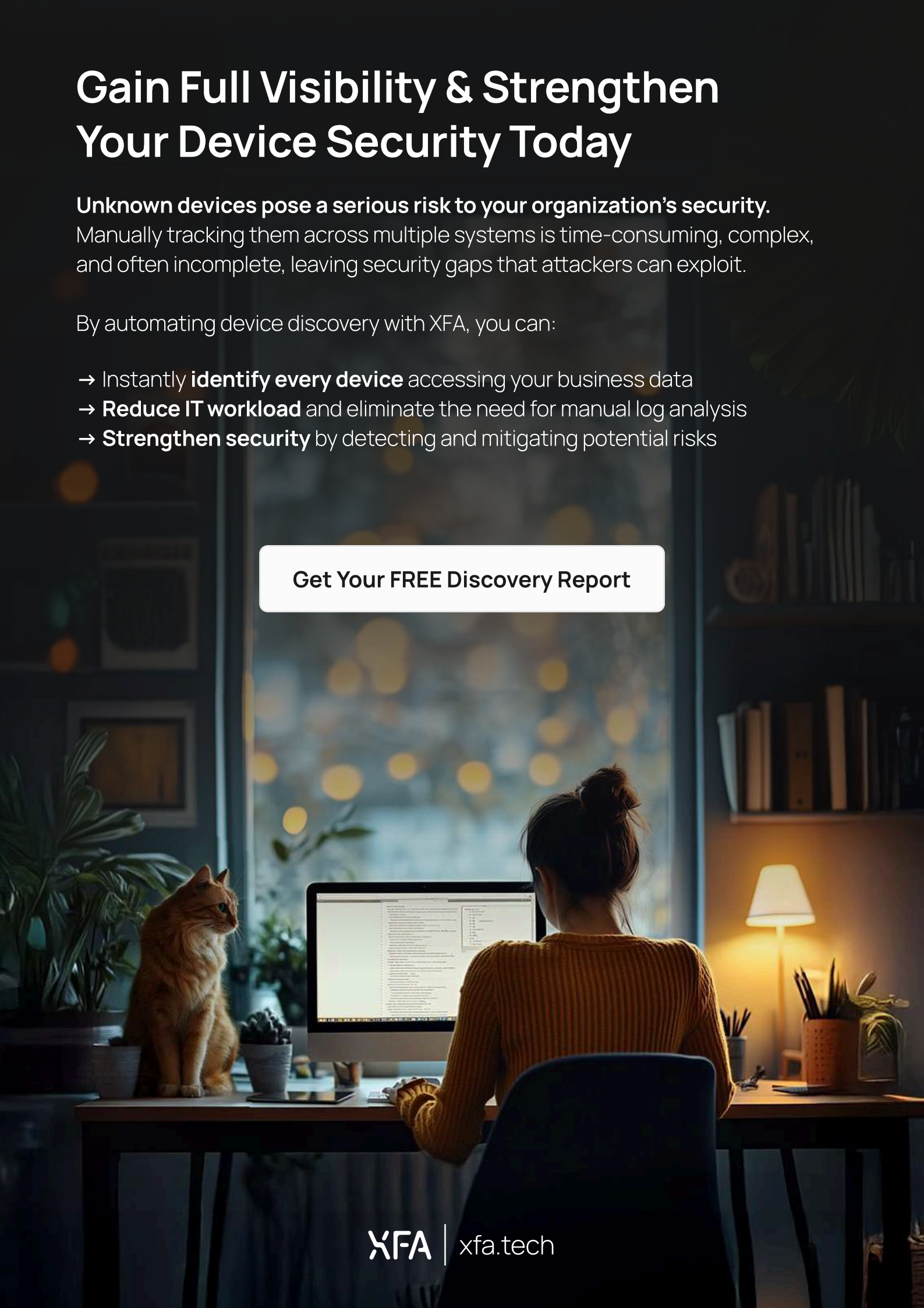
Gain Full Visibility & Strengthen Your Device Security Today

Unknown devices pose a serious risk to your organization's security. Manually tracking them across multiple systems is time-consuming, complex, and often incomplete, leaving security gaps that attackers can exploit.

By automating device discovery with XFA, you can:

→ Instantly **identify every device** accessing your business data
→ **Reduce IT workload** and eliminate the need for manual log analysis
→ **Strengthen security** by detecting and mitigating potential risks

Get Your FREE Discovery Report



XFA | xfa.tech