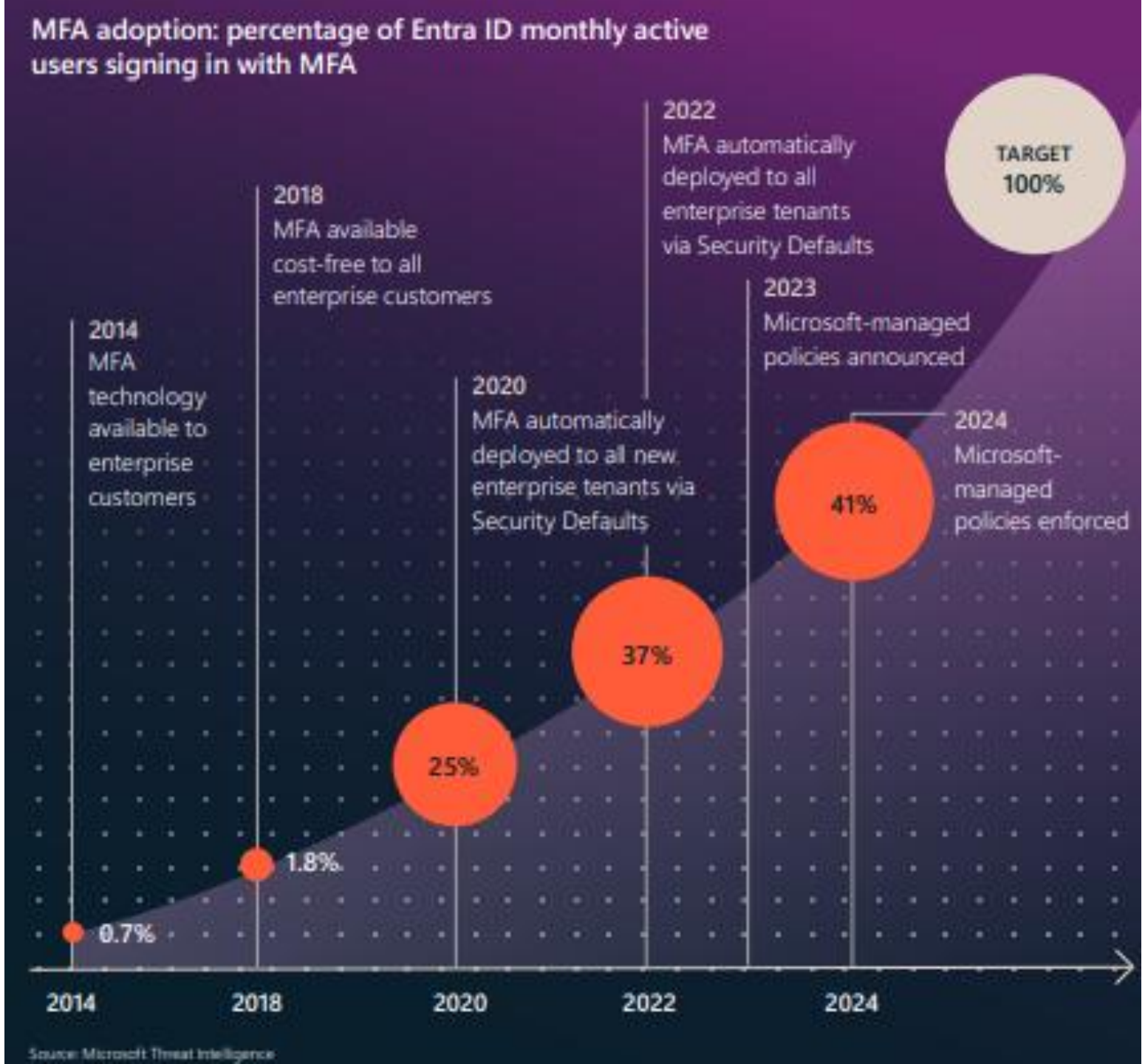

Security


4
L


MFA adoption: percentage of Entra ID monthly active users signing in with MFA
2014
MFA technology available to enterprise customers
2018
MFA available cost-free to all enterprise customers
2020
MFA automatically deployed to all new enterprise tenants via Security Defaults
2022
MFA automatically deployed to all enterprise tenants via Security Defaults
2023
Microsoft-managed policies announced
2024
Microsoft-managed policies enforced
TARGET
100%
0.7%
1.8%
25%
37%
41%
2014
2018
2020
2022
2024
Source: Microsoft Threat Intelligence

Attack Surface Reduction (ASR) Rules

Minimize the attack surface

Attack surface reduction (ASR) rules help to control entry points to your Windows devices using cloud intelligence, such as behavior of Office macros.

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block only Office communication applications from creating child processes

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

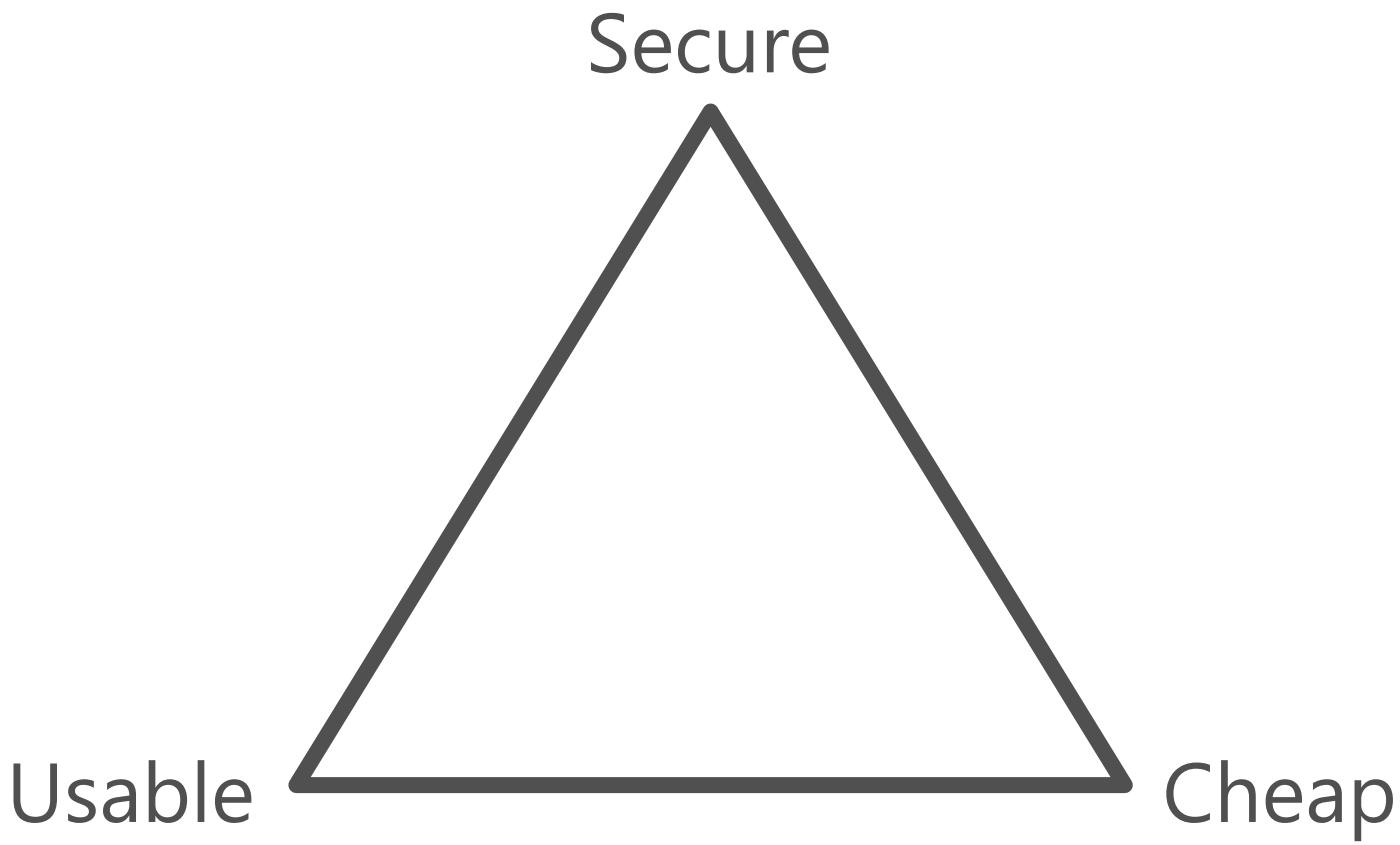
Polymorphic threats

- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware

Lateral movement & credential theft

- Block process creations originating from PSExec and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription

The Security Dilemma




SECURITY
QUIET
HTML
php
git
LARACON
NODE


12
5
20
1
18

Australian Government

Australian Signals Directorate

ASD's Blueprint for Secure Cloud

	Essential Eight	ASD Cloud Blueprint
Purpose	Broad cybersecurity hardening across systems (general security maturity).	Specific guidance for securing cloud environments, especially government workloads.
Focus	Primarily endpoint protection and hardening.	Deep configuration guidance for cloud services (like Microsoft 365, Azure).
Audience	All organizations (private and public).	Primarily government or highly regulated sectors using cloud.
Detail Level	Tactical – focused on 8 key mitigation strategies (patching, MFA, backups, etc).	Strategic and detailed – covers cloud architecture, identity, logging, information classification, etc.
Microsoft 365 Coverage	Indirect (only as part of your endpoints and apps).	Direct — includes explicit Microsoft 365 and Azure security configurations.

https://bit.ly/cia-asd-bsc