inetum realdolmen
Positive digital flow

Zero Trust

Key take-aways en hoe nu verder?

11,8% of Flemish companies

indicate they have been a victim in the past year

Smaller companies are more vulnerable

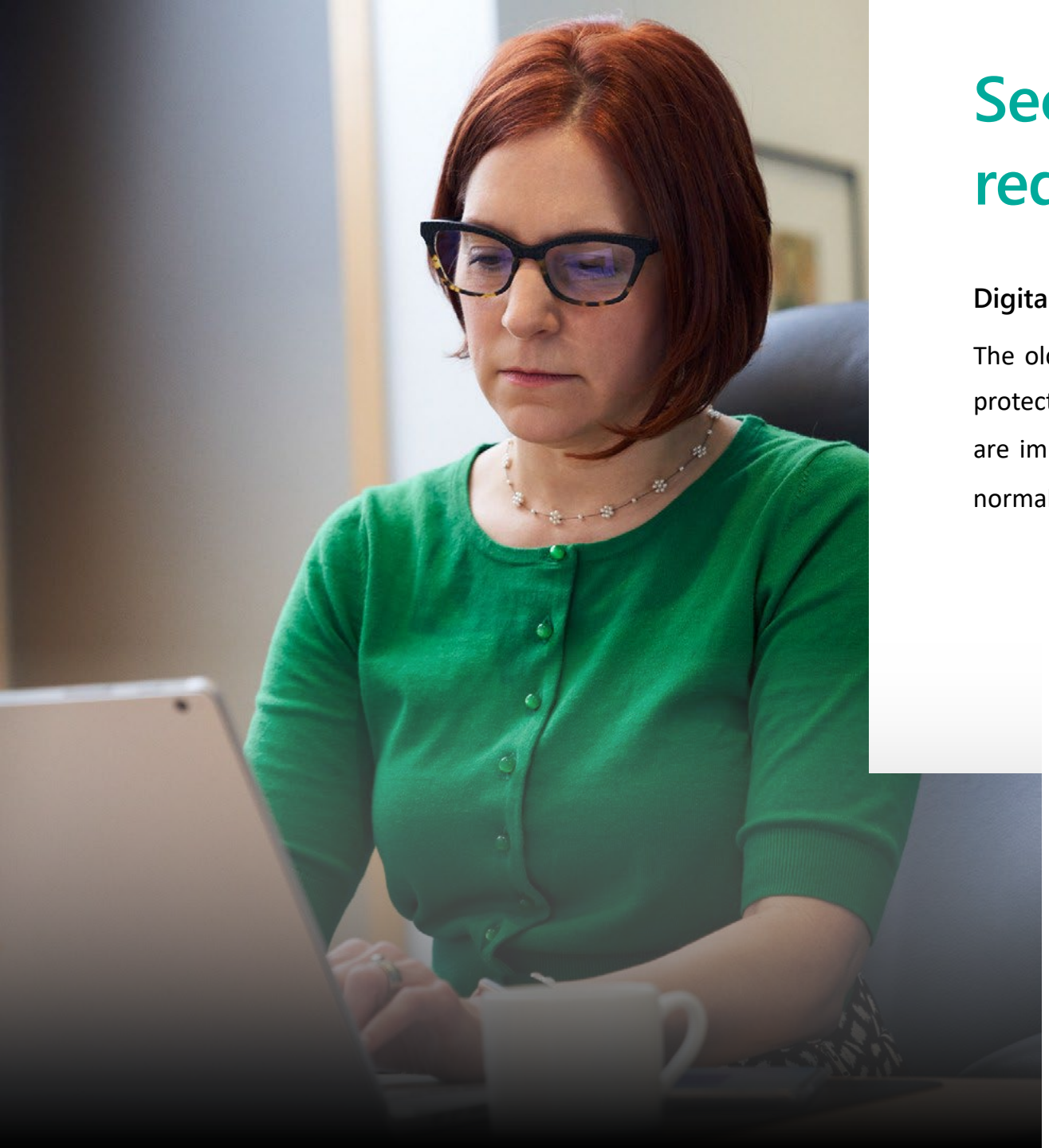
and have greater operational consequences

23,5% of impacted companies

experienced corporate data destruction

13,3% of impacted companies

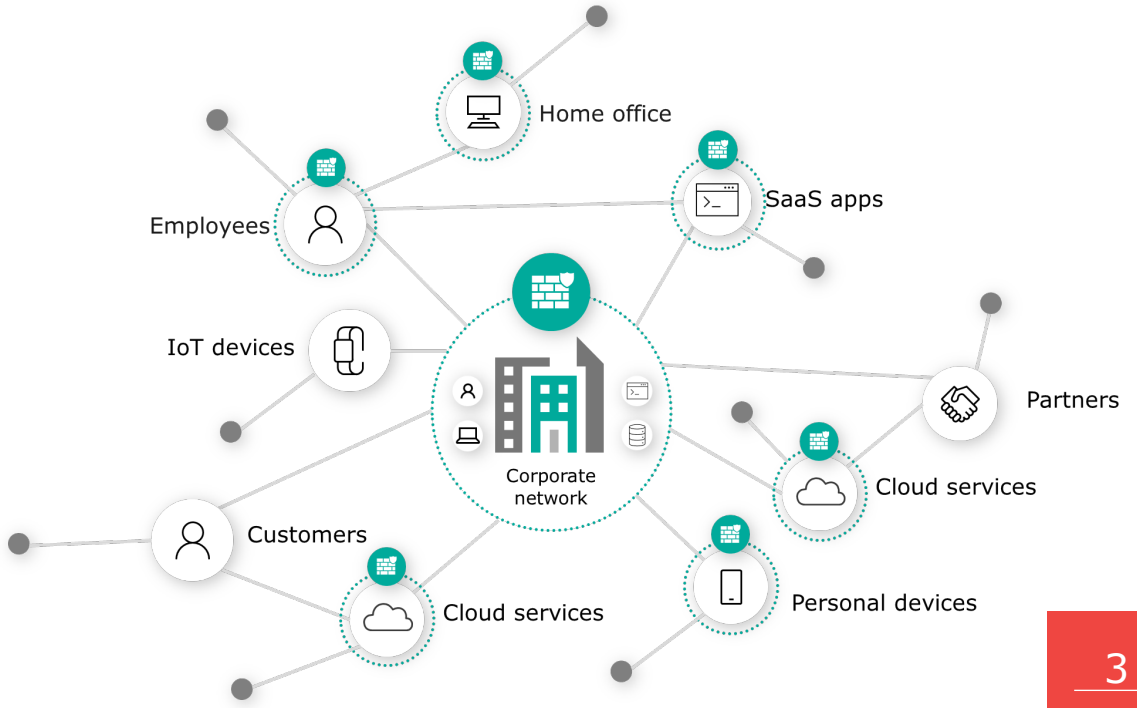
experienced corporate data theft



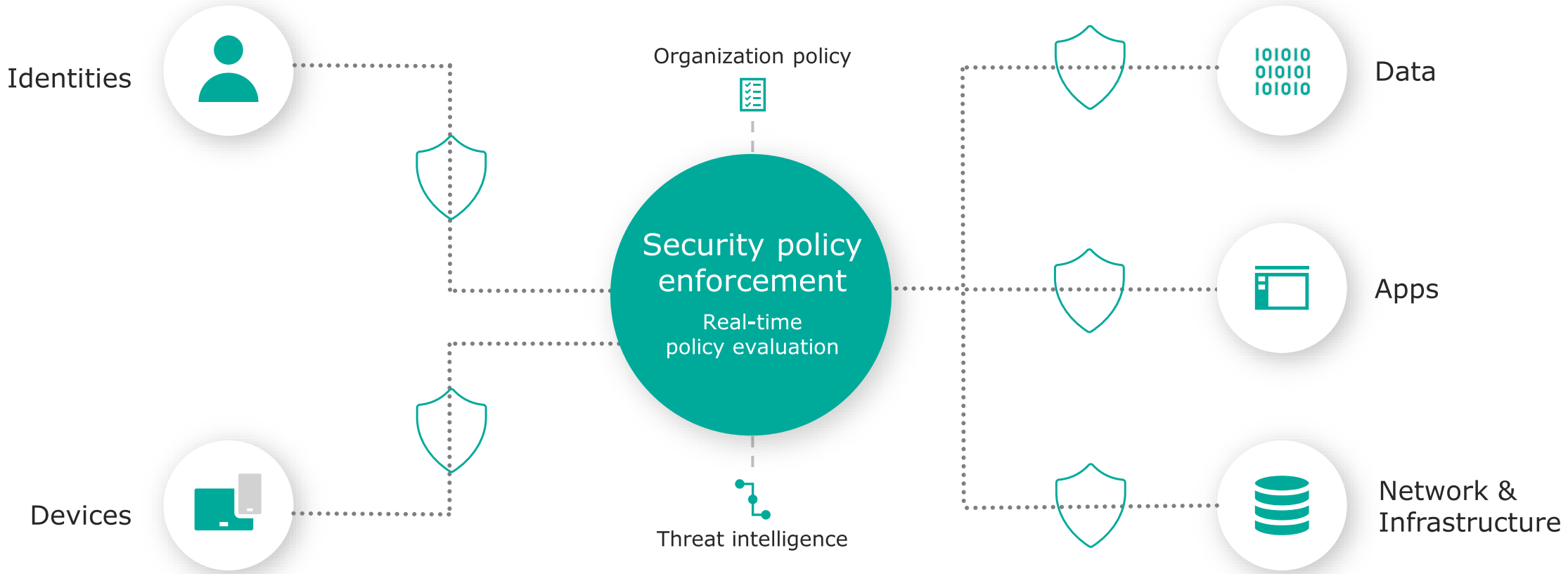
Securing digital transformation requires Zero Trust

Digital transformation forces re-examination of traditional security models

The old way of security does not provide business agility, user experiences, and protections needed for a rapidly evolving digital estate. Many organizations are implementing Zero Trust to alleviate these challenges and enable the new normal of working anywhere, with anyone, at any time.



Zero Trust Architecture



Zero Trust Roadmap

First stage

- Are you reducing password risks with strong auth methods like MFA and providing SSO access to cloud apps?
- Do you have visibility into device compliance, cloud environments, and logins to detect anomalous activity?
- Are your networks segmented to prevent unlimited lateral movement inside the firewall perimeter?

Significant progress

- Are you using real-time risk analytics to assess user behavior and device health to make smarter decisions?
- Can you correlate security signals across multiple pillars to detect advanced threats and quickly take action?
- Are you proactively finding and fixing vulnerabilities from misconfigurations and missing patches to reduce threat vectors?

Most mature stage

- Are you able to dynamically enforce policies after access has been granted to protect against violations?
- Is your environment protected using automated threat detection and response across security pillars to react more quickly to advanced threats?
- Are you analyzing productivity and security signals to help drive user experience optimization through self-healing and actionable insights?

Zero Trust Roadmap

	Identities	Devices	Network & Infrastructure	Applications	Data
TRADITIONAL	No SSO between cloud and on-premises apps Visibility into identity risk is very limited	Devices are domain joined No overview and inventory of devices	Flat open network with unencrypted traffic Minimal threat protection	On-premises apps and no cloud apps No overview of shadow IT	Access is governed by perimeter Unencrypted and without classification
ADVANCED	Basic conditional access policies with basic MFA Cloud identity federation and visibility into identity risk	Devices are registered with a cloud identity provider DLP policies for BYOD	Basic network segmentation Cloud native filtering and threat protection	Apps configured with SSO + discover shadow IT Critical apps are monitored	Access is governed by classification Encrypted and classified via keywords
OPTIMAL	Password less authentication Phishing-proof MFA User behavior is analyzed in real time Enforce least privilege access	Endpoint threat protection is used to monitor device risk Access control is gated on device risk Continuous risk-based asset management	Micro segmentation ML-based threat protection and filtering All traffic is encrypted	Apps are available using least privilege access In-session monitoring and response Assess the security posture of cloud apps	Classification by AI DLP policies based on classification Access governed by cloud security policy engine

Visibility, analytics, automation & governance

Security adoption

Adopting Zero Trust

Think big, start small, move fast

Security Roadmap

Maturity assessment with clear overview of risks and their mitigations including budget & projects mapping

Implementation

Start with quick wins and move forward on the road to zero trust

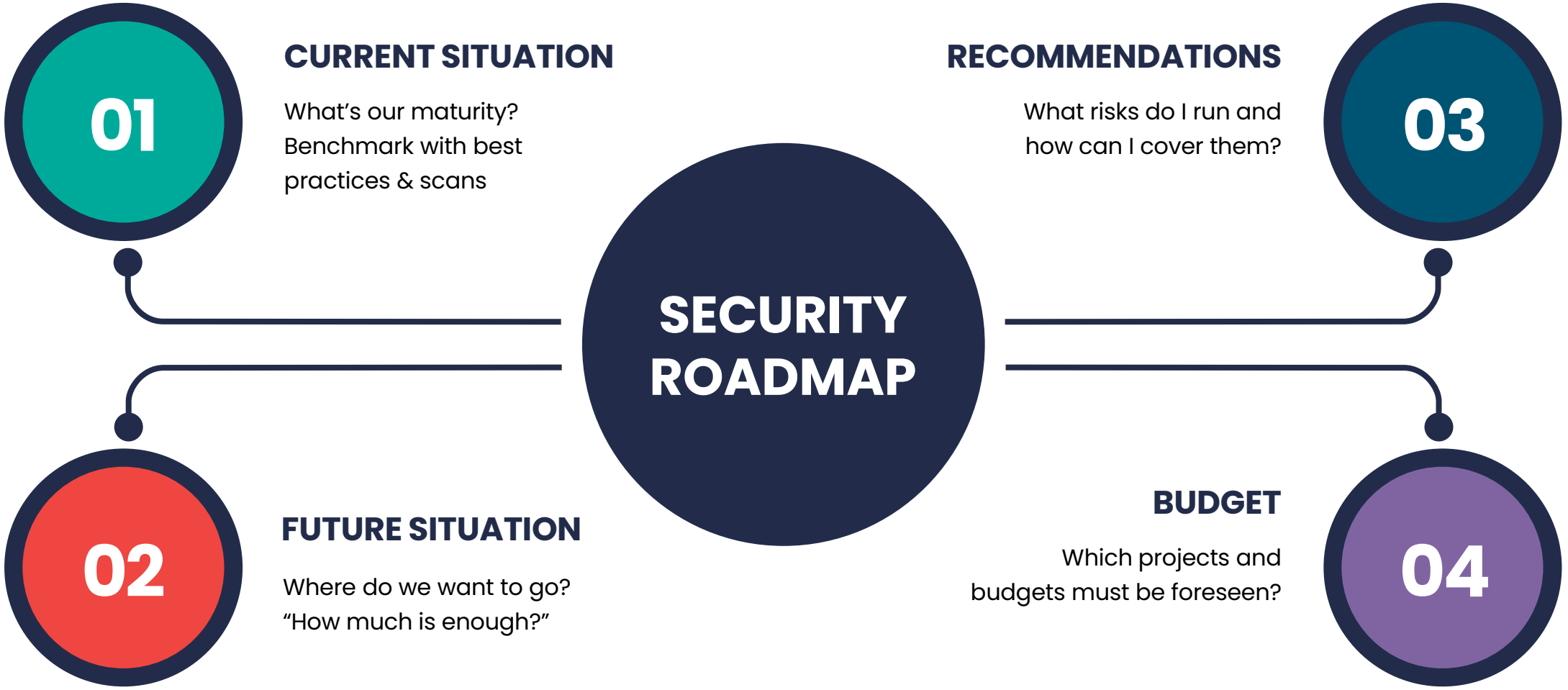
Managed Services

Visibility and analytics are key to a successful zero trust adoption

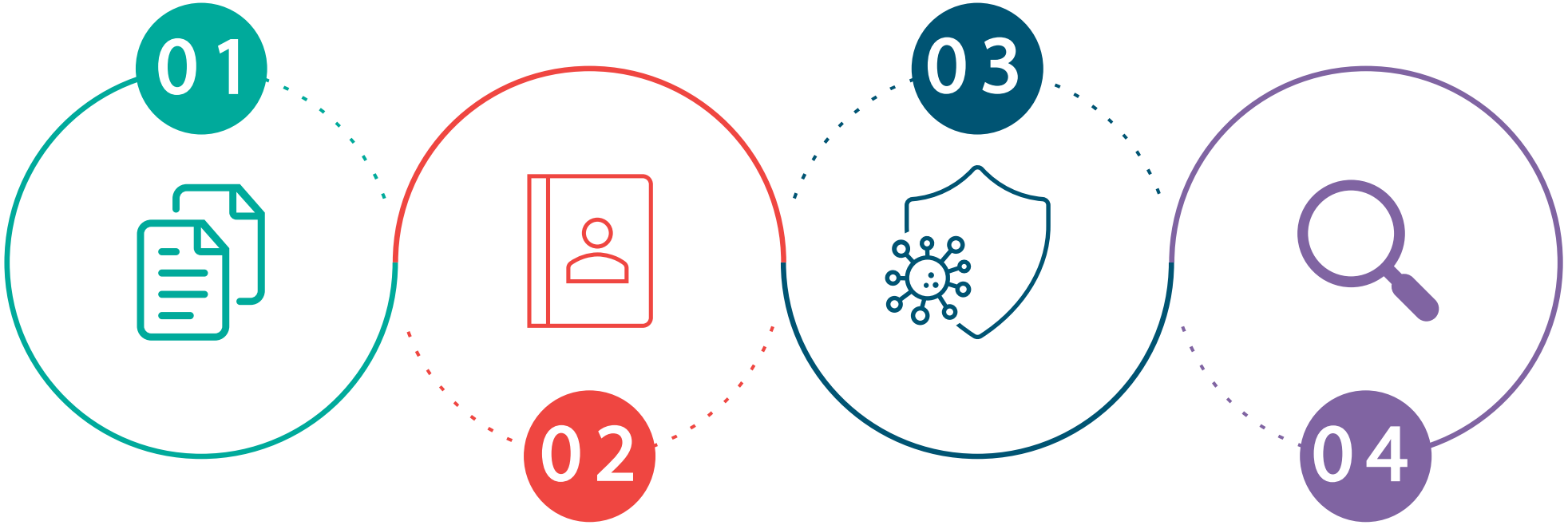
Technology Specific

Focus on specific technologies & platforms like firewalling, networking, M365, Azure, back-up, ...

Security Roadmap



Security Roadmap



Benchmark

170 best practices over 18 topics divided in 3 levels

AD Security Scan

Security assessment of the **Active Directory** environment

Vulnerability Scan

Identifying all **vulnerabilities** in the IT infrastructure

External Scan

Analysis of all **external IP's** & open ports

Security Roadmap

4.6. Access Control Management

Global score: 50,00%
Standard score: 62,50%
Advanced score: 50,00%
Premium score: 0,00%

✓ [redacted]

NIST CSF controls (partially) scored:

PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.IP-11 | Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

✗ [redacted]

NIST CSF controls (partially) not scored:

PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-7 | Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
PR.AC-3 | Remote access is managed

Recommendation	Risk	Level	NIST CSF
[redacted]	H	Std	PR.AC-1 PR.AC-7 PR.AC-3
[redacted]	M	Adv	PR.AC-1

4.3. Data Protection

Global score: 53,85%
Standard score: 83,33%
Advanced score: 20,00%
Premium score: 50,00%

✓ [redacted]

NIST CSF controls (partially) scored:

PR.IP-6 | Data is destroyed according to policy
PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition

✗ [redacted]

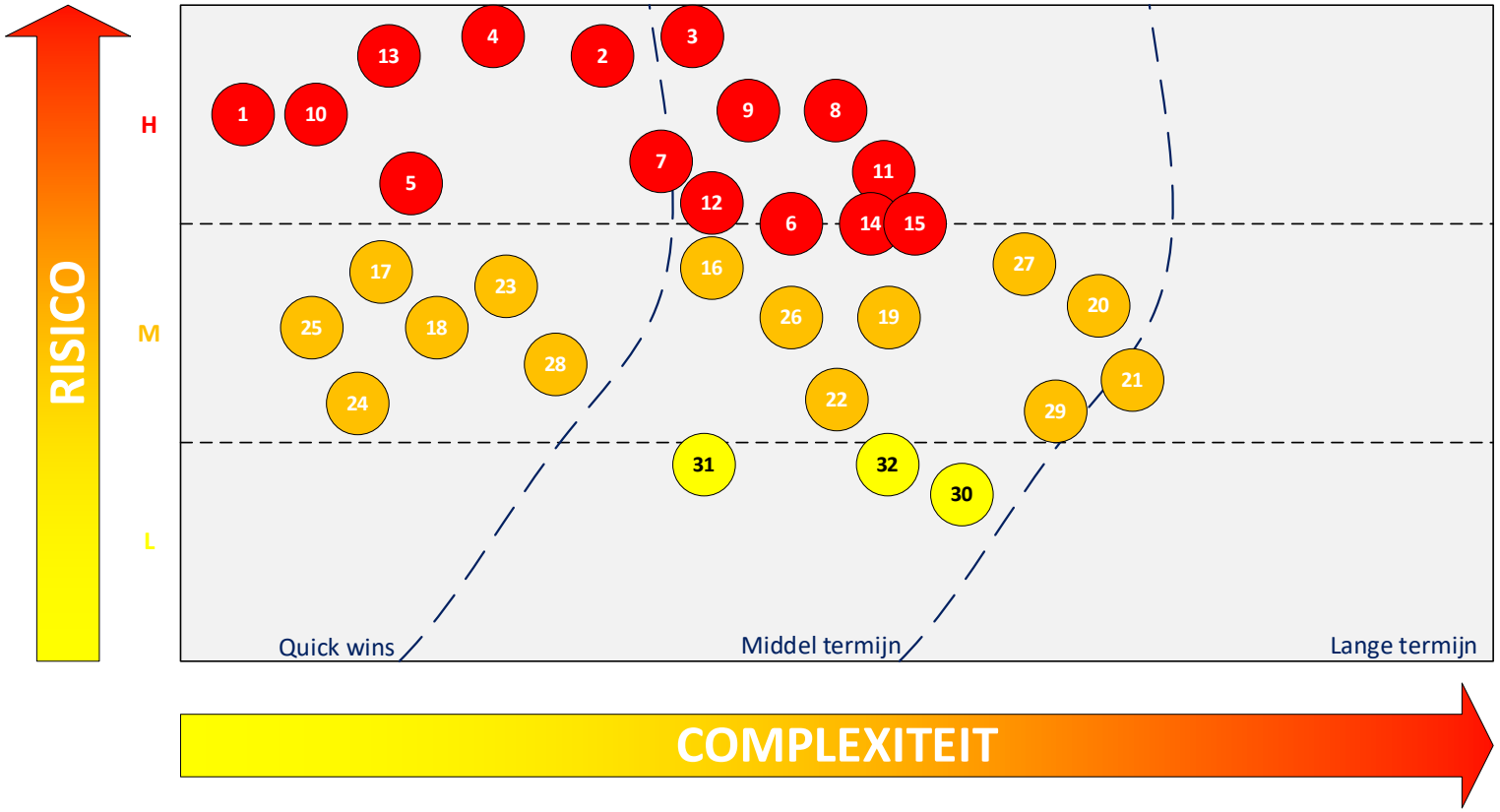
NIST CSF controls (partially) not scored:

ID.AM-5 | Resources (e.g., hardware, devices, **data**, time, personnel, and software) are prioritized based on their classification, criticality, and business value
DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed
ID.AM-3 | Organizational communication and data flows are mapped
PR.PT-2 | Removable media is protected and its use restricted according to policy
PR.DS-5 | Protections against data leaks are implemented
PR.AC-5 | Network integrity is protected (e.g., network segregation, network segmentation)

Recommendation	Risk	Level	NIST CSF
[redacted]	H	Std	PR.IP-6
[redacted]	M	Adv	ID.AM-5
[redacted]	M	Adv	DE.AE-1
[redacted]	M	Adv	PR.PT-2
[redacted]	L	Adv	PR.AC-5
[redacted]	L	Prm	PR.DS-5

Security Roadmap

ID	Aanbeveling	Risico	Impact	Niveau
1	[redacted]	H	L	Std
2	[redacted]	H	L	Std
3	[redacted]	H	M	Std
4	[redacted]	H	L	Std
5	[redacted]	H	L	Std
6	[redacted]	H	M	Std
7	[redacted]	H	M	Std
8	[redacted]	H	M	Std
9	[redacted]	H	M	Std
10	[redacted]	H	L	Std
11	[redacted]	H	M	Std
12	[redacted]	H	L	Std
13	[redacted]	H	L	Adv
14	[redacted]	H	L	Adv
15	[redacted]	H	L	Adv
16	[redacted]	M	L	Std
17	[redacted]	M	L	Std
18	[redacted]	M	L	Std
19	[redacted]	M	L	Std
20	[redacted]	M	L	Adv



The road to secure success

We offer different solutions, a quick glance

IDENTIFY

Gaining insights into your IT resources and associated risks. In concrete terms, knowing what you have and what risk this entails.

- Security Assessments & Roadmaps
- Vulnerability Management
- Penetration testing
- Phishing simulation

PROTECT

Preventing security incidents with appropriate measures and resources.

- Endpoint Protection
- Patch Management
- Network Protection
- Multicloud Protection
- Identity Protection
- E-mail Protection

DETECT

Detecting and identifying suspicious behaviour and security incidents.

- Managed Detection & Response (MDR)
- SOC / SIEM
- Endpoint Detection & Response (EDR)

RESPOND & RECOVER

Responding to incidents and restoring operations after an incident.

- Managed Services
- CSIRT Response Team
- Back-up & Recovery
- M365 Back-up

GOVERNANCE

Overseeing the cybersecurity strategy to reduce risk.

- Workshops
- CISO
- Guidance

Upcoming Webinars

Woensdag 14/12/2022 @ 11:00u
Identity Protection: meer dan enkel een wachtwoord

Woensdag 25/01/2023 @ 11:00u
Privileged accounts: een gemakkelijk doelwit voor hackers?

Woensdag 01/02/2023 @ 11:00u
Hou grip op uw documenten met Azure Information Protection

Woensdag 08/02/2023 @ 11:00u
Microsoft 365 Defender Threat Protection: een gedegen security-oplossing

Woensdag 15/02/2023 @ 11:00u
Aan de slag met big data? Beheer de overvloed aan data met Azure Purview