amentum

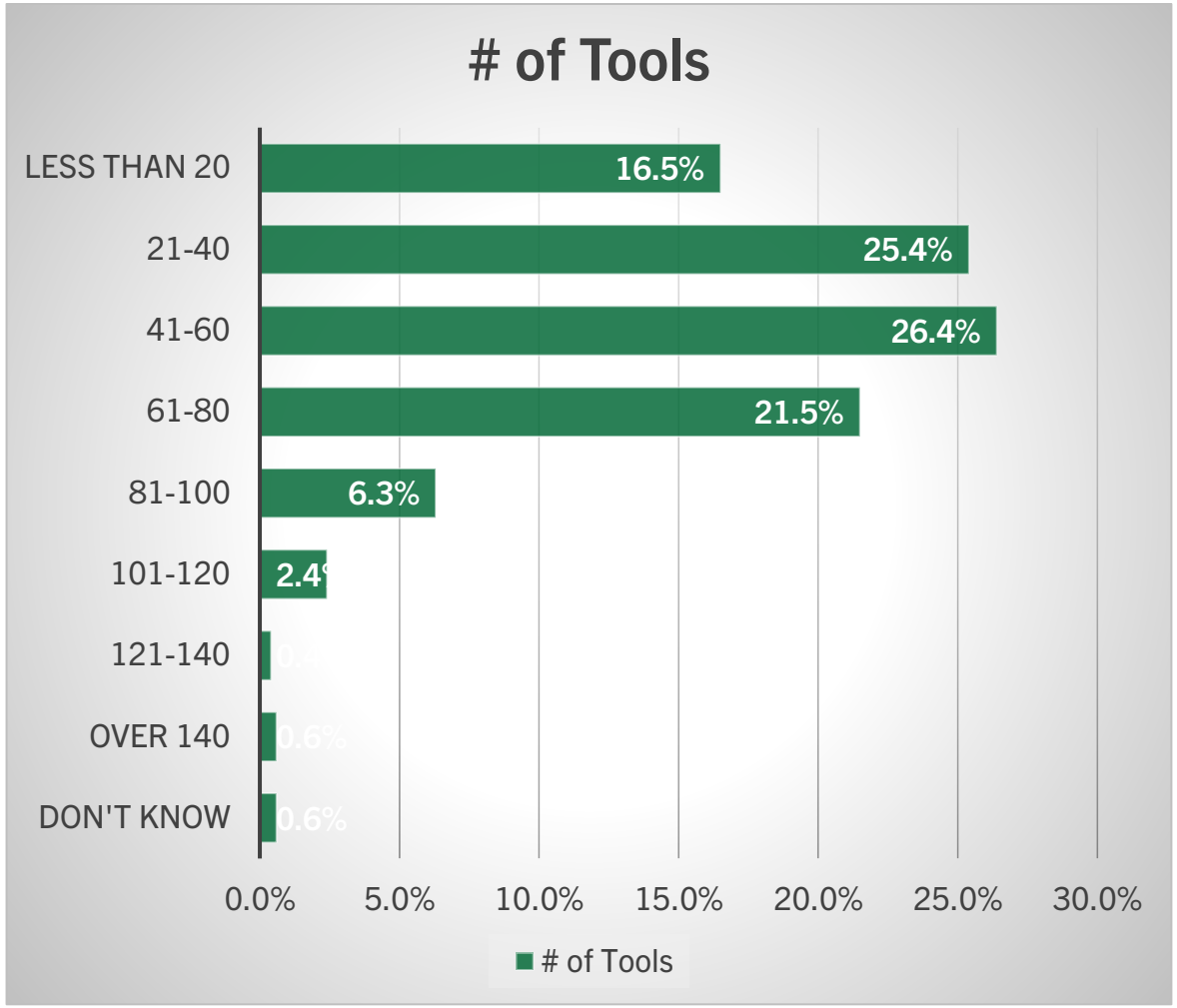
Technology Rationalization

Managing the Tech Stack Chaos

Max Shier, CISSP-ISSMP, C|CISO, C|EH
VP, Chief Information Security Officer

The Problem: Tool Sprawl

- According to Gartner, organizations use an average of 45 cybersecurity tools
- Over 3,000 cybersecurity vendors in the market
- Tool sprawl causes:
  - Tools partially deployed or redundant
  - Lack of integration
  - New tools may create more gaps
  - Increased complexity and cost
  - Alert fatigue
  - Longer MTTR due to added complexity or gaps



https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025
https://www.cio.com/article/3496811/can-you-have-too-many-security-tools.html

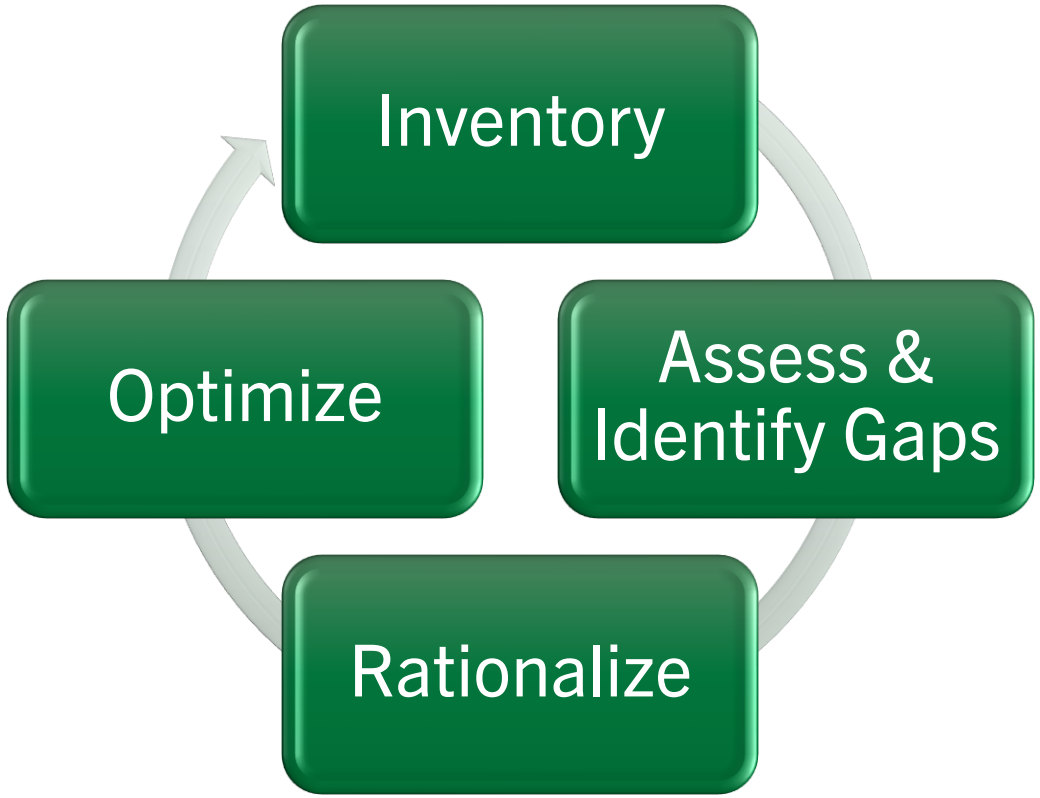
What is Technology Rationalization?

“Tech rationalization is the strategic process of analyzing an organization's technology landscape—including software, hardware, and applications—to identify and eliminate redundancies, improve efficiency, reduce costs, enhance security, and better align technology with business goals. It involves deciding which technologies to keep, replace, consolidate, or retire to create a simpler, more effective technology stack.”

Technology Rationalization – The Process

Initiators:

- Personnel changes
- Renewals
- Budget Planning
- Adding capability
- Use case changes
- Environment changes
- Technology changes
- Business changes
- Regulatory changes (CMMC)

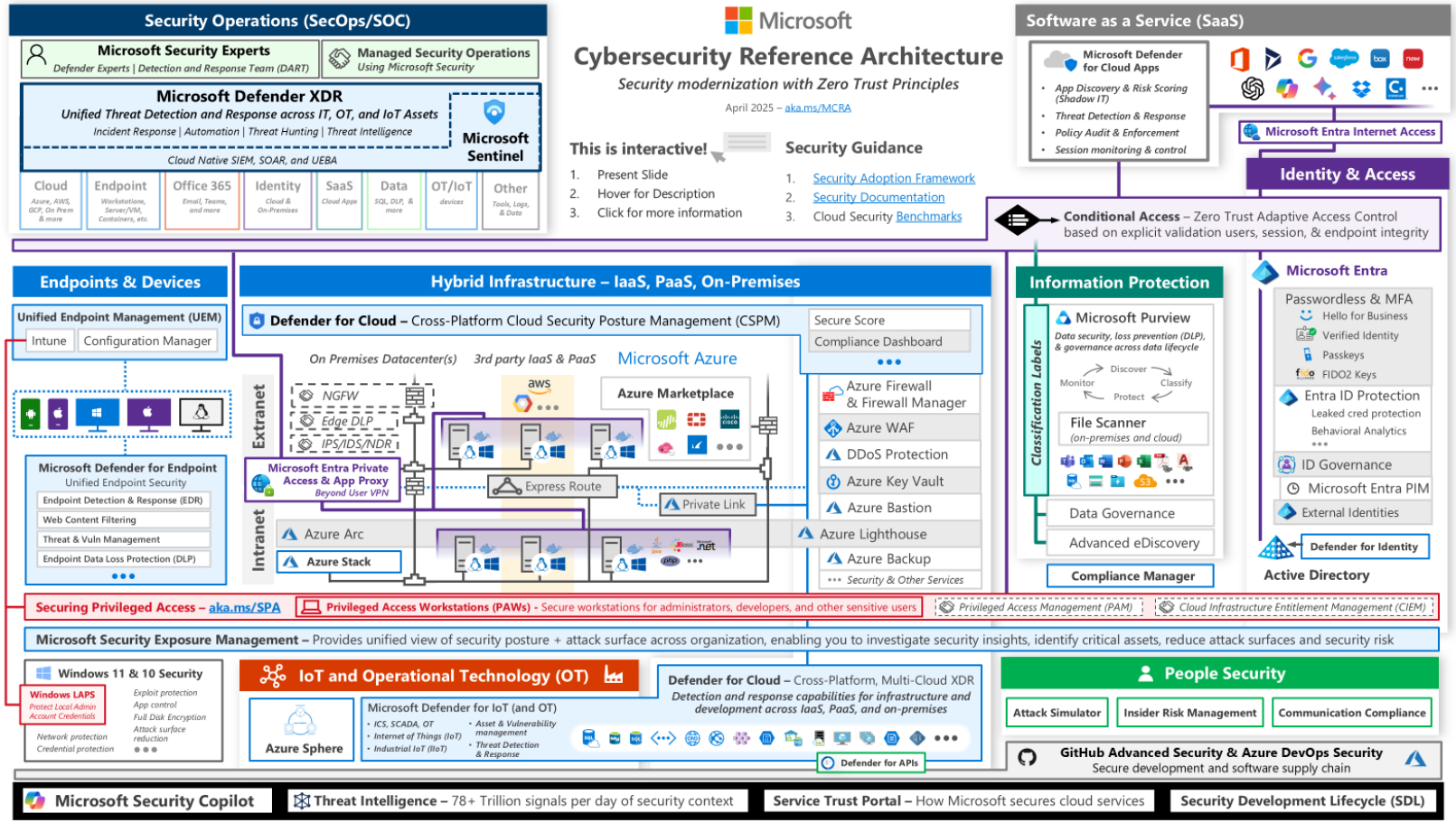


Outputs:

- Streamlined, integrated toolset
- Less complexity; Reduced cognitive load and console fatigue
- Increased team efficiency
- Identify technical gaps & functional deficiencies
- Lower total cost of ownership
- Clear visibility into ROI

Step 1: Inventory

- Catalog tools, modules, and services
- Capture cost, usage, owners, dependencies, stakeholders
- CMDB can help identify:
  - Shadow IT
  - Program managed apps
- Exercise can help map the cybersecurity reference architecture & data flows



https://learn.microsoft.com/en-us/security/adoption/mcra

Step 2: Assess & Identify Gaps

- Use tools/references like Optiv's Market System to map capabilities, overlap, and use cases
- Vendors may also be able to provide a mapping to controls and/or use cases
- Functional fit and integration
- Operational supportability
- Usability and operator load
- Map to Regulatory Frameworks
  - SOX, PCI-DSS, HITRUST, ISO, etc.
  - NIST CSF, 800-53 (FEDRAMP/RMF), 800-171 (CMMC)

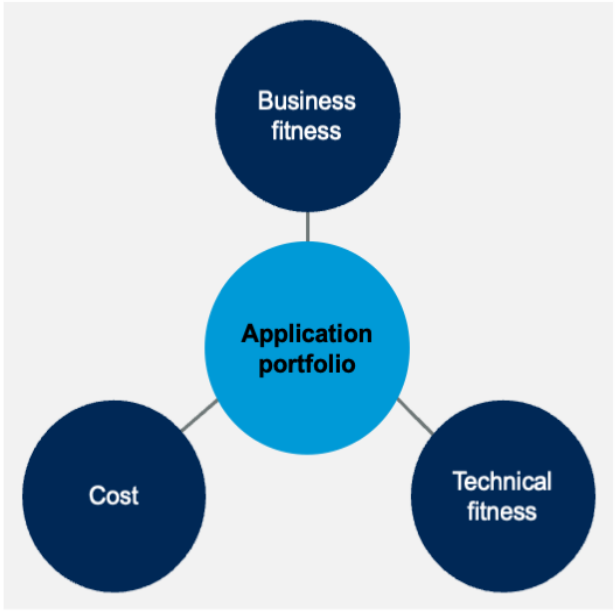
https://www.optiv.com/company/press-releases/optiv-market-system-groundbreaking-single-reference-architecture

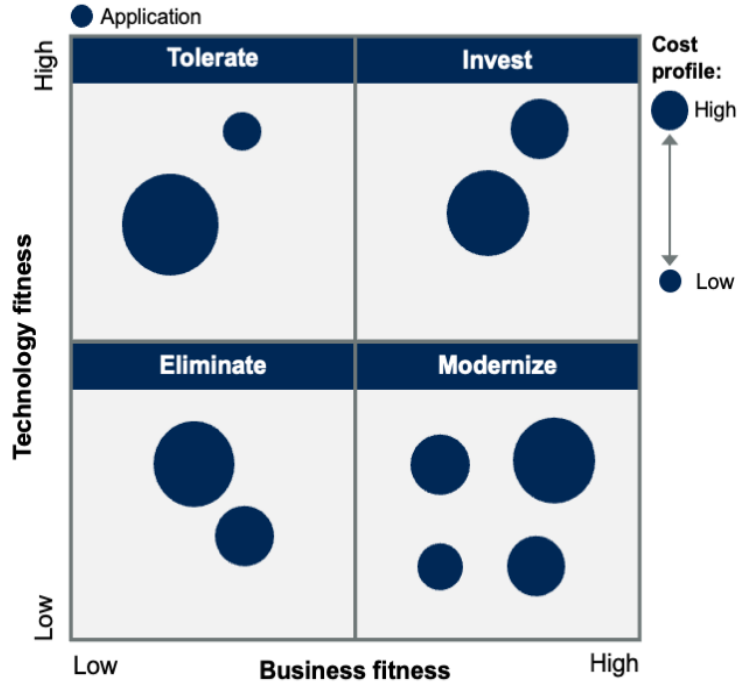
Step 2: Assess & Identify Gaps

- Develop a scoring methodology and score the applications & services
  - Ability to meet business needs
    - User friction
    - On-prem vs. cloud
    - High admin overhead
  - Ability to meet technical use cases
    - Interoperability/Integration
    - Ease of use
  - Total cost of ownership (TCO)

- Determine whether app or service should be:
  - Tolerated; Keep product, but mature
  - Invested; Grow with product or platform
  - Modernized; Move to SaaS or newer version
  - Eliminated; Terminate product or move to another vendor

Use TIME to Assess the Fitness of an Application



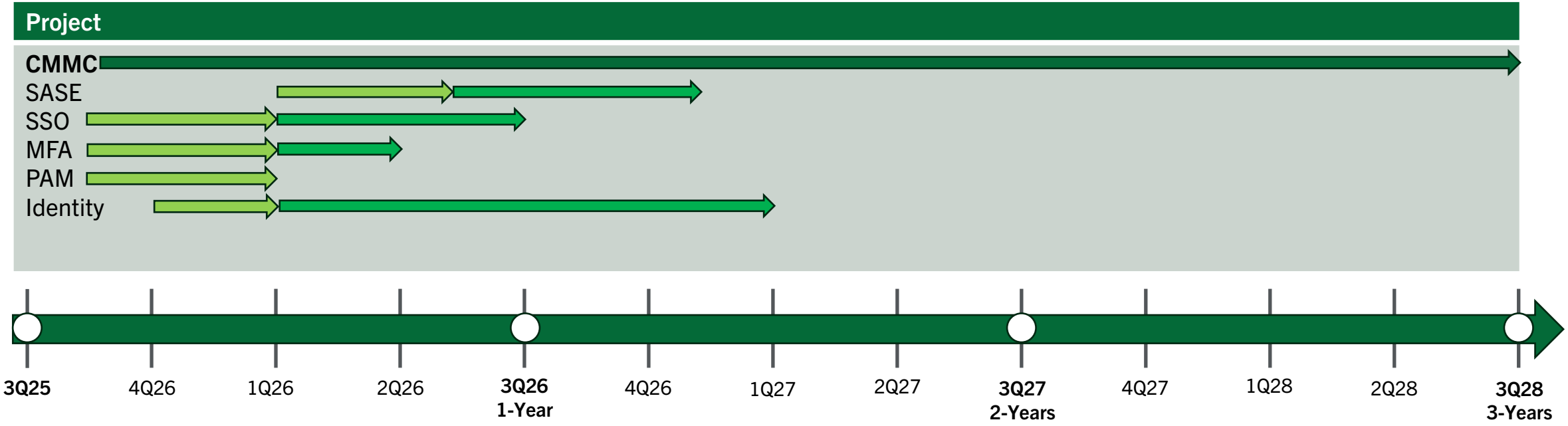


Source: Gartner
834382

Gartner

Step 3: Rationalize

- Develop an Action Plan
  - Eliminate redundant or legacy tools
  - Migrate to better tools or platforms
  - Ensure projects are in strategic alignment with cybersecurity project roadmap & budget
  - May need to be integrated into the larger IT planning and roadmap
- Phased transition
  - Ensure appropriate resourcing (both IT & Cyber)
  - Budget planning may necessitate a multi-year deployment
  - Regulatory requirements may drive a quicker timeline (CMMC)
  - Re-assess tools as they come up for renewal



Step 4: Optimize

- Track KPIs (tool count, cost, savings, MTTR)
- Review quarterly / annually
- Re-assess use cases & develop new use cases as requirements change
- Track with a dashboard or other centralized method of tracking

Sample Internal Rationalization Dashboard

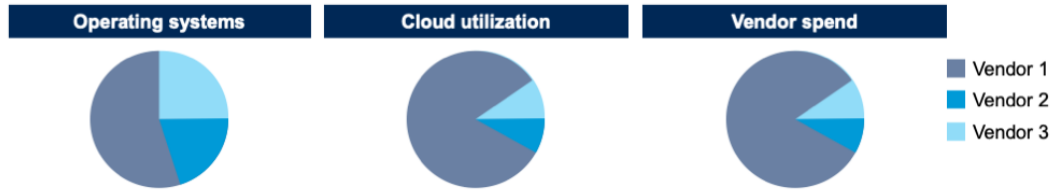
Summary

Total number of applications	Operating cost	Applications added YTD
2214	$10.2m	12
Rationalization opportunities	**Costs avoided YTD**	**Apps decommissioned YTD**
256	$1.2m	20

Work in progress

Source application	Target application	Progress	Target completion	Benefits
Application W	Application C	100%	Q4 2025	Reduction in policy input time by 15%
Application X	Application B	50%	Q1 2026	Customer user journey improvements, conversion rate +5%
Application Y	Application A	33%	Q1 2026	All brands using single application, reducing recharge by 20%
Application Z	Application A	50%	Q2 2026	All brands using single application, reducing recharge by 20%

Utilization overview



CIO/CTO
Tracking progress against cost goals and understanding scale

Business leaders
Showing planned and delivered business benefits aligned with their objectives and goals

I&O complexity
Quick reference in line with IT strategic priorities

Source: Gartner
834382

Gartner

Common Mistakes

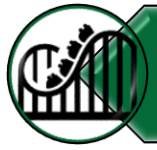

Treating tech rationalization as a one and done project


Focusing solely reducing costs

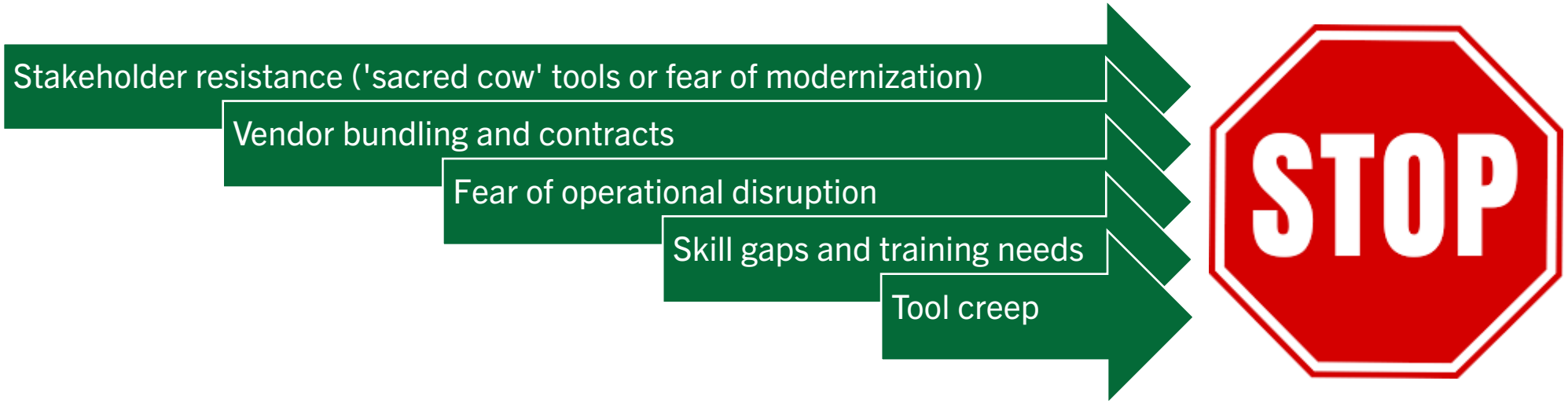

Leaving out stakeholders


Working from incomplete or incorrect data


Ignoring shadow IT or unique business cases

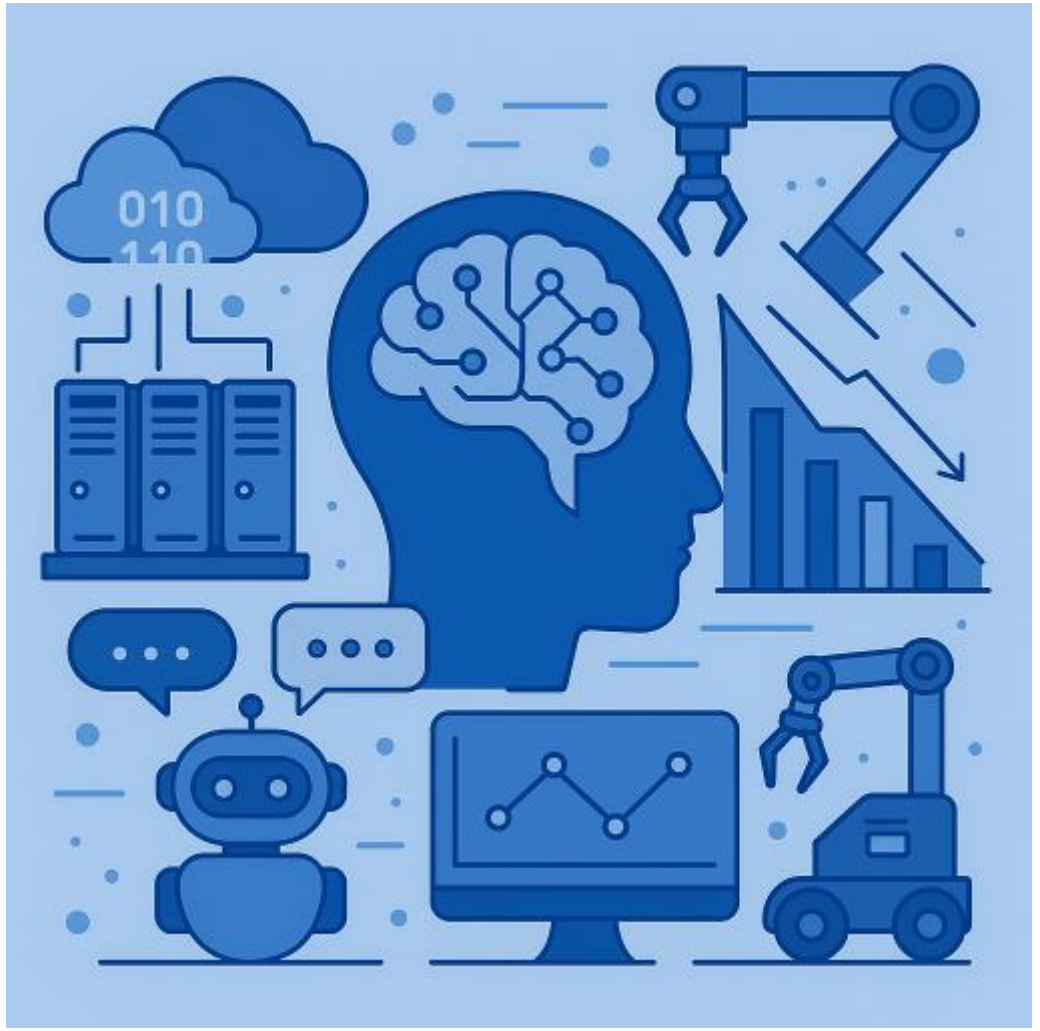

No organizational change management

Typical Roadblocks to Success



Future Cybersecurity Tooling Trends to Consider

- Platformization across the industry
  - CloudStrike, Palo Alto, Cisco, Microsoft, Google
- AI integrations into cybersecurity tooling
  - “Copilots”
  - Natural language searching/processing
- Protecting against AI
  - AI identities
  - Data loss/spillage into open models
  - Deepfakes, phishing, fake employees, etc.
- Tighter integrations
  - Native API integrations across vendors and tools
- Post-Quantum Cryptography



Thank you.

amentum

amentum.com