Zero Trust and the Future of Privileged Access Management

Ray Mills – Territory Manager – Mediterranean

Zero Trust PAM facts & figures

83% increase in the number of identities within an organization in the past year

– 2021 Identity Security Alliance Report

Only **17%** of organizations are securing all their Privileged Accounts in a PAM solution and only **12%** of organizations have protected all their endpoints with Privilege Elevation

– 2022 CyberEdge Report & 2020 Delinea State of PAM Report

“By 2023, **75%** of security failures will result from inadequate management of identities, access, and privileges, up from **50%** in 2020”

- Gartner

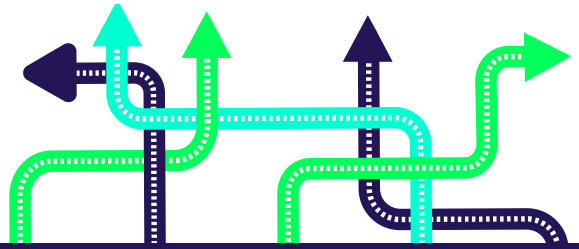
Why security risks are increasing around Identity

Accelerating IT Complexity

- Remote is the new normal
- Explosion of IT infrastructure
- Complexity and lack of visibility with SaaS adoption and cloud access
- Exploding number of human and non-human identities

Expanding Threat Landscape

- The new IT landscape has constant increases in threats and the sophistication of those threats
- Expansion across identities, environments and locations increases attack surface

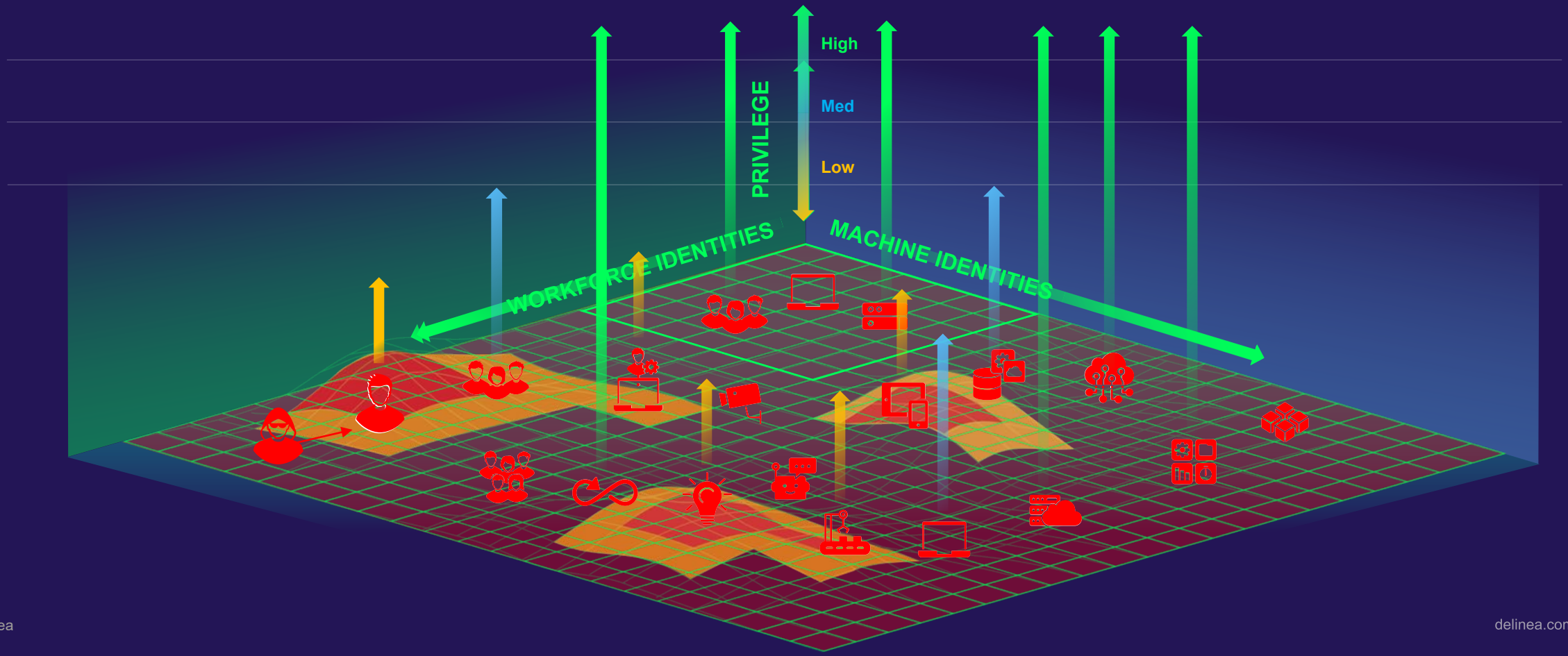


Security Vendors Proliferating

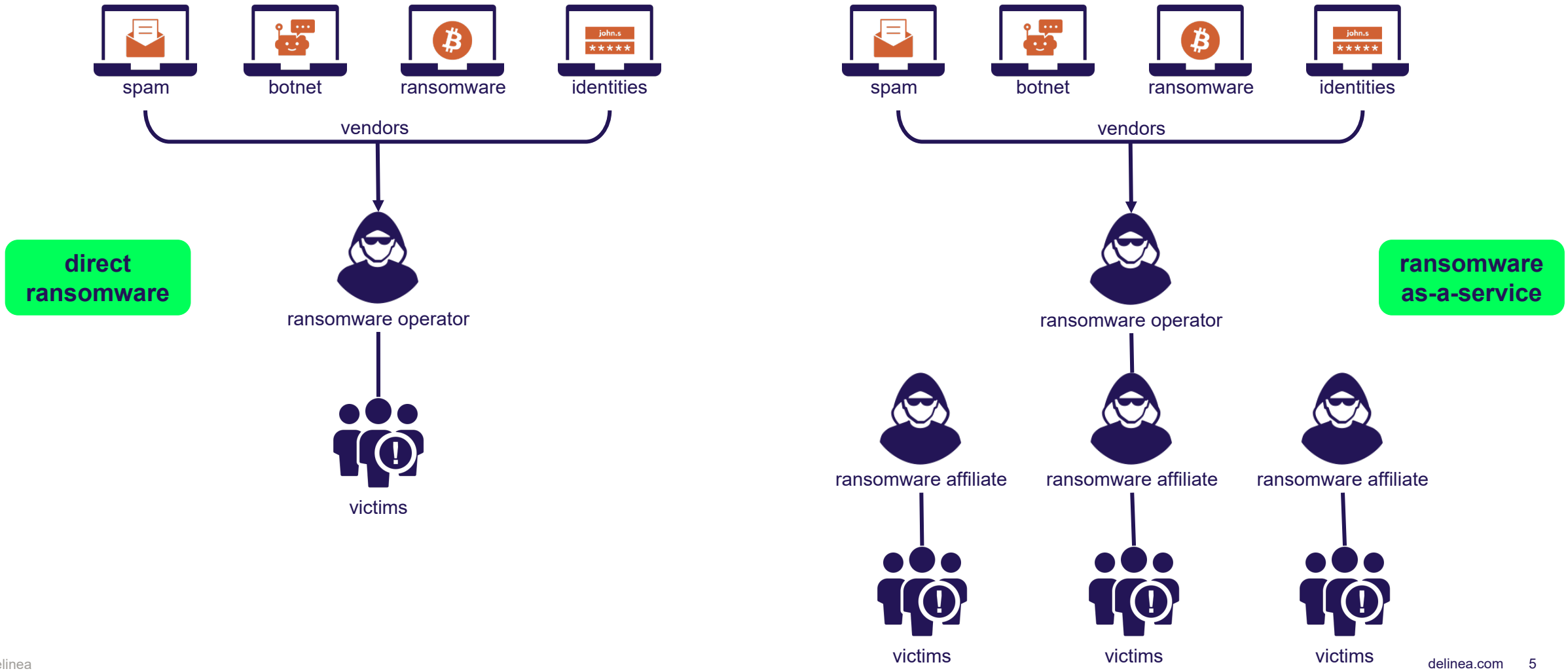
- A wide array of solutions are deployed for endless use cases
- Current technologies are focused on specific attacks

…but breaches still occur, mostly from credential theft

Everything has an Identity
Identities are expanding
Identities must be secured



Ransomware as-a-service is enabling scale



Ransomware: An equal opportunity attack

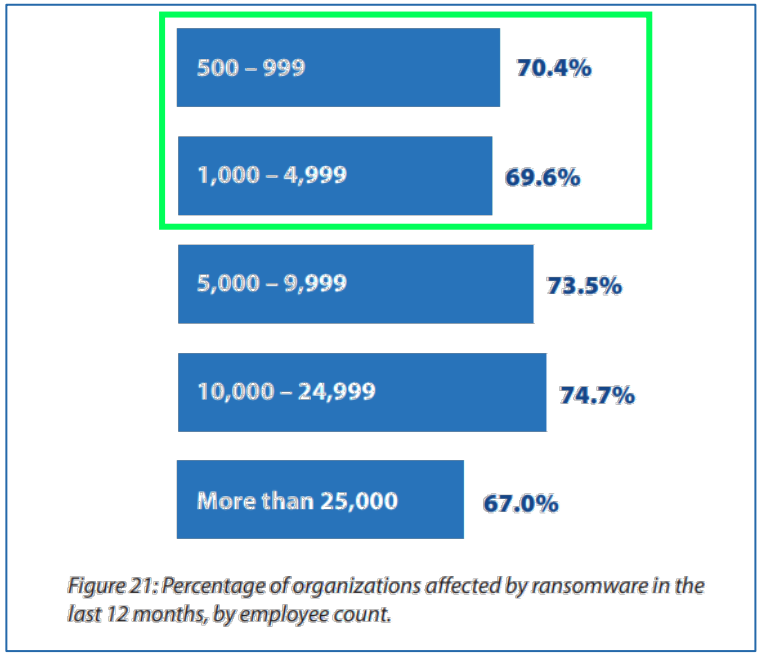


Figure 21: Percentage of organizations affected by ransomware in the last 12 months, by employee count.

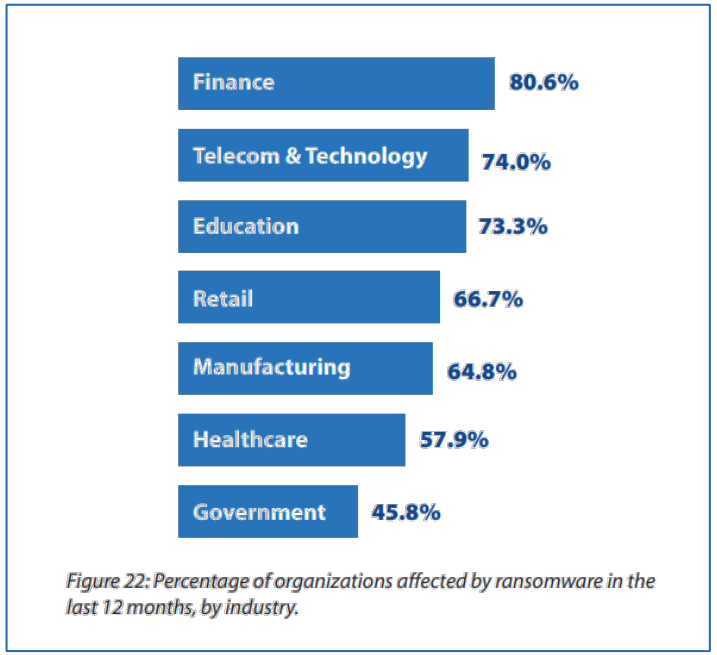


Figure 22: Percentage of organizations affected by ransomware in the last 12 months, by industry.

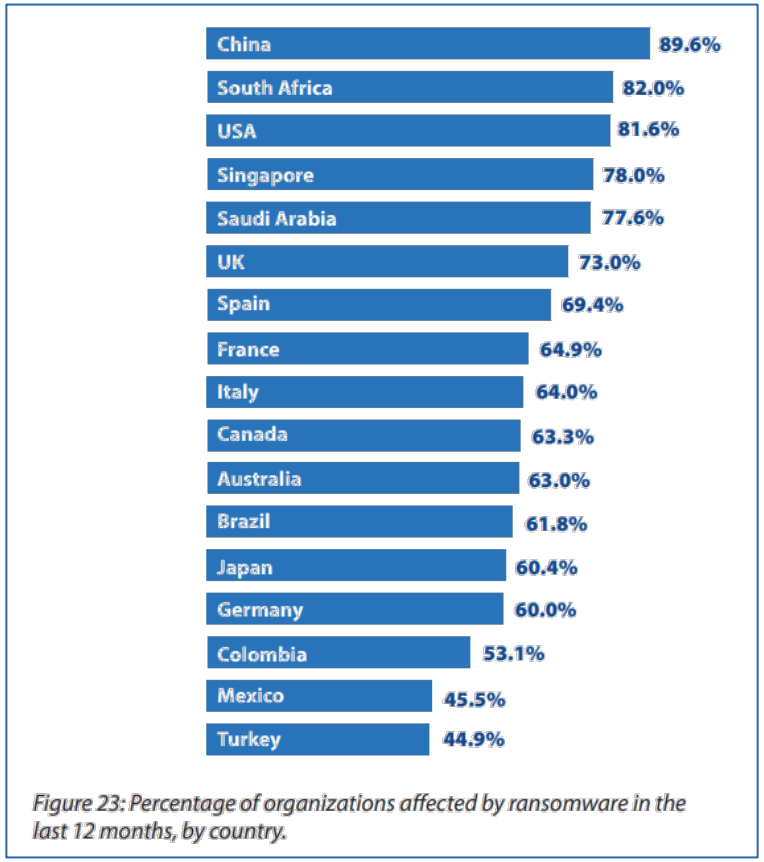


Figure 23: Percentage of organizations affected by ransomware in the last 12 months, by country.

“A vicious cycle”

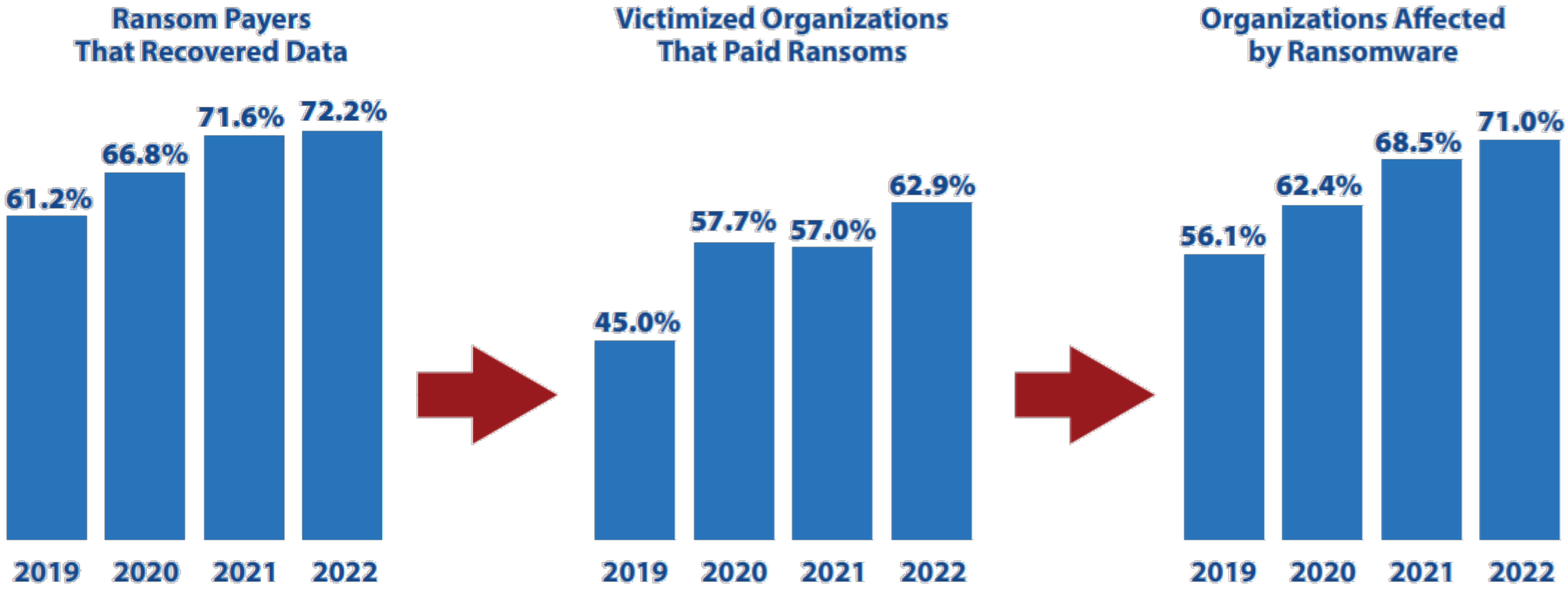
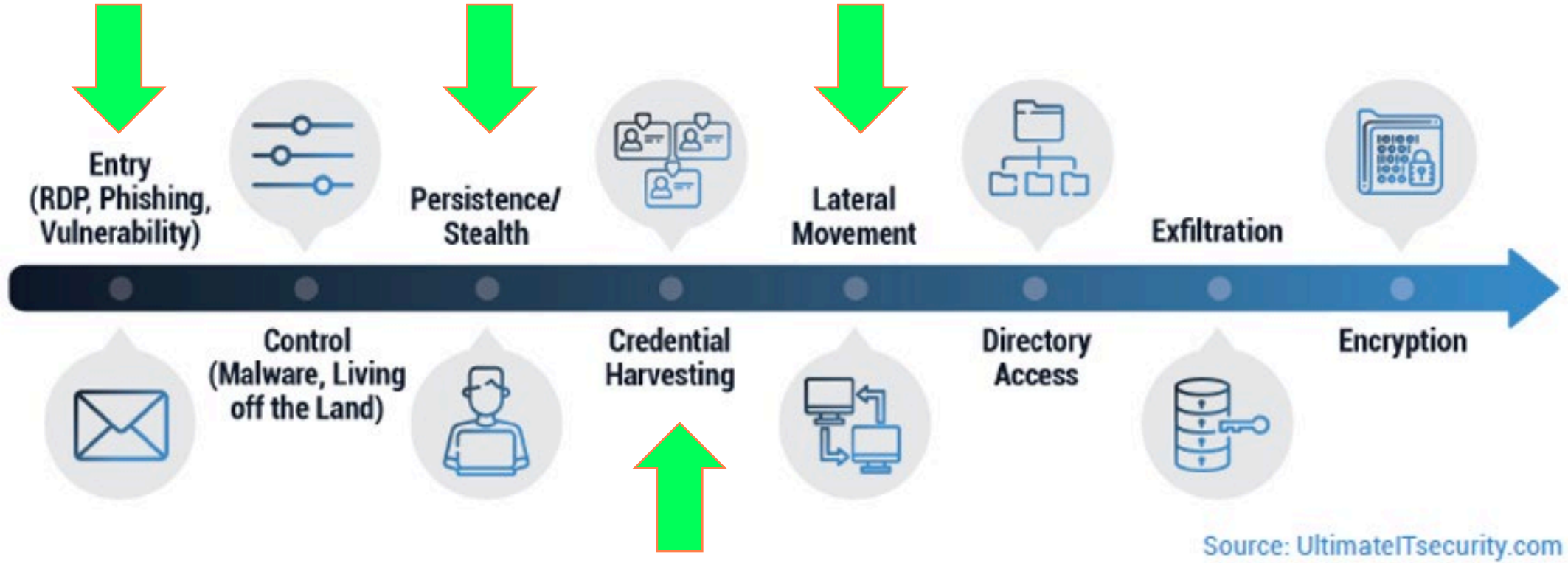


Figure 20: The ransomware vicious cycle: increased odds of recovering data … entice more victims to pay ransoms … which motivates more ransomware attacks.

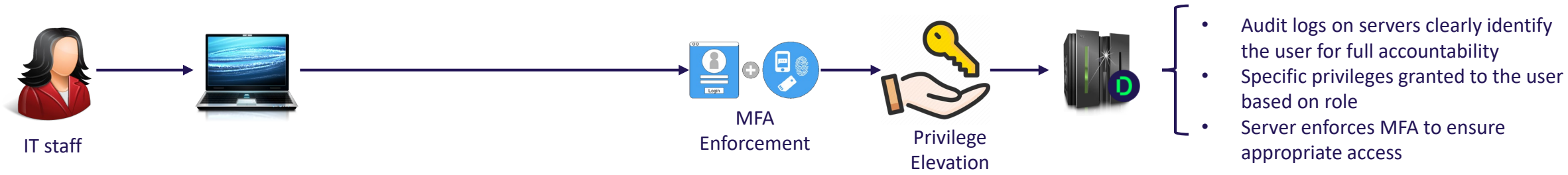
A Typical Ransomware Attack Pathway



What does Zero Trust look like?

Example of Zero Trust PAM: Server Access

- **Reduce the number of shared accounts & passwords**
- **Reduce your attack surface;** by reducing points of ingress & limits accidental damage or scope of a breach if attackers do breach
- **Give full accountability;** people log in using their **personal** account, no shared account, no ambiguity
- **Grant just enough privilege** to do the job of the persona. Rights can be scoped to users/applications/services vs. shared accounts



Example of Zero Trust PAM: Workstation Least Privilege

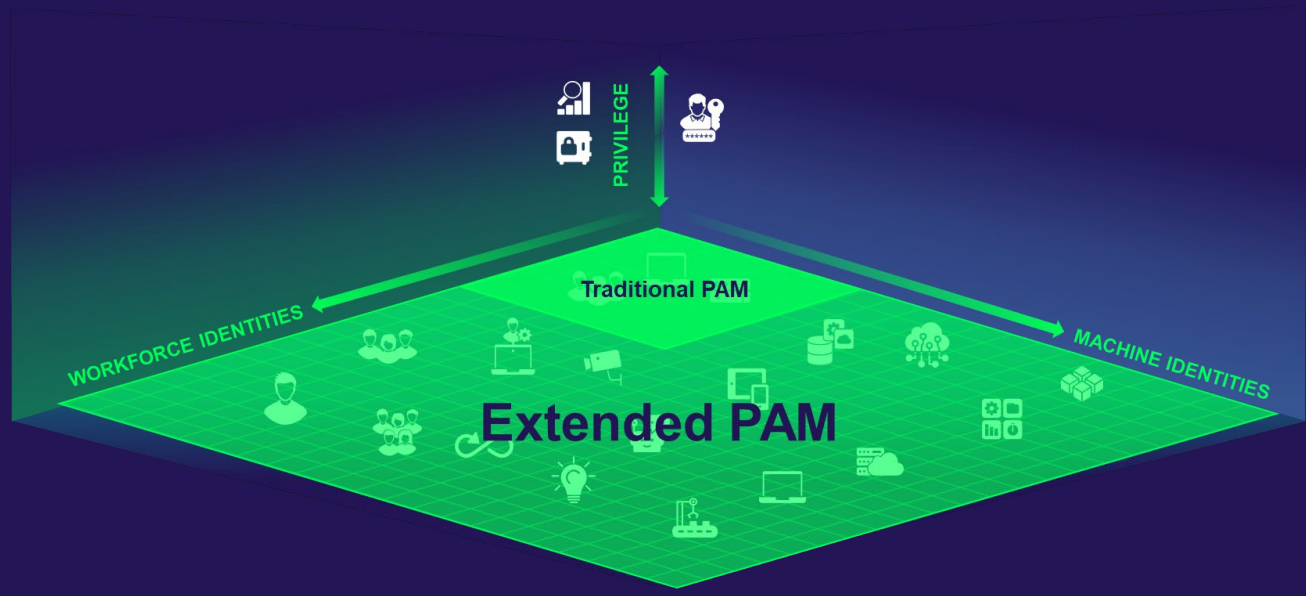
- **Eliminate ALL Local Admins on workstations**
- **Reduce your attack surface;** by eliminating powerful privileged which are the top target for Ransomware
- **Maintain productivity;** grant users access to approved applications and processes which require admin rights, without the human user ever operating in the context of a privileged user
- **Facilitate request workflows:** grant user a simple workflow to request permission to run unknown or not yet approved applications and processes

Modern PAM enforces security best practices:

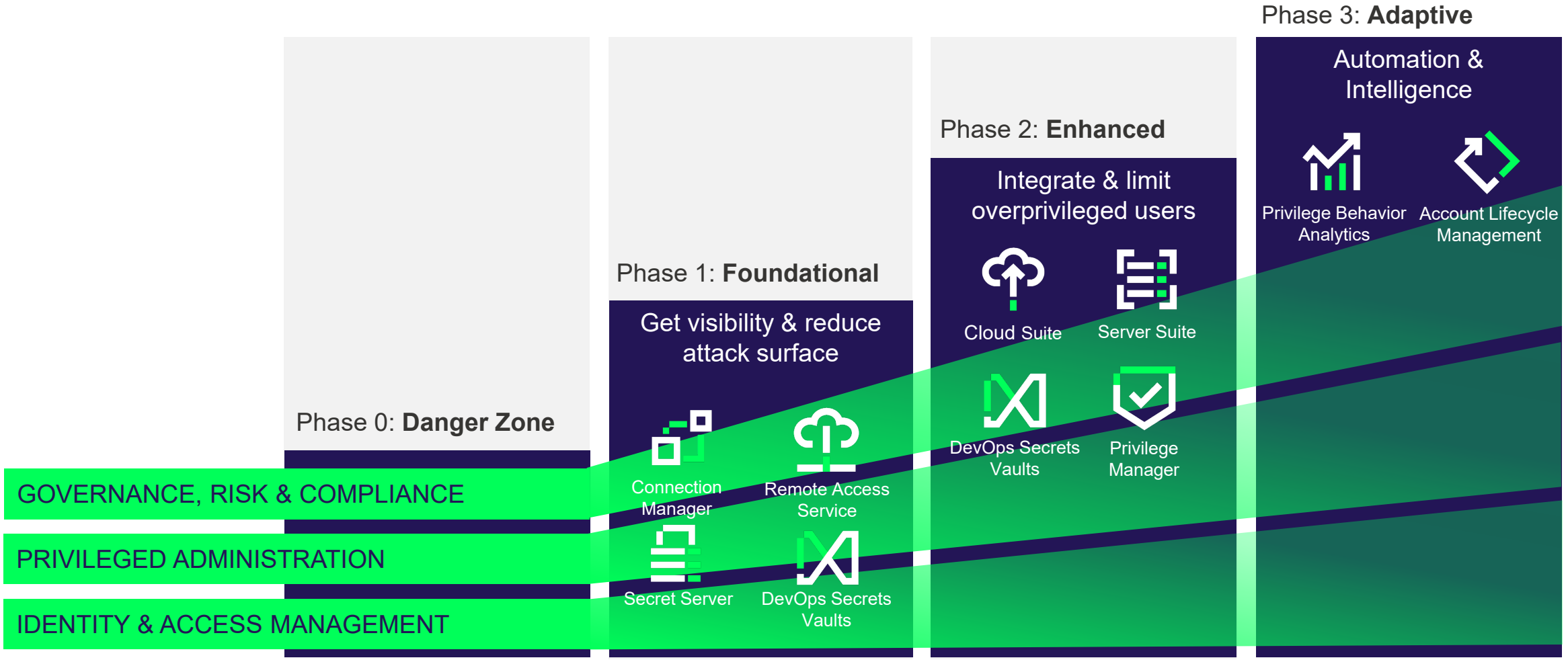
- ✓ Establish trust, always verify, enforce least privilege
- ✓ Redefining Privileged Access Management

The Delinea vision for Extended Zero Trust PAM

- Prevent identity/credential theft by increasing visibility and discovery across all identities
- Establish controls over all internal/external privileged access to restrict unnecessary lateral movement
- Limit privilege escalation by adapting access when and where needed with analytics-informed policies



Delinea Zero Trust PAM Maturity Model



Zero Trust and the Future of Privileged Access Management

Ray Mills – Territory Manager – Mediterranean