Outlook for Cloud Security 2023

Craig Lawson

Gartner®

Gartner®

Key Issues

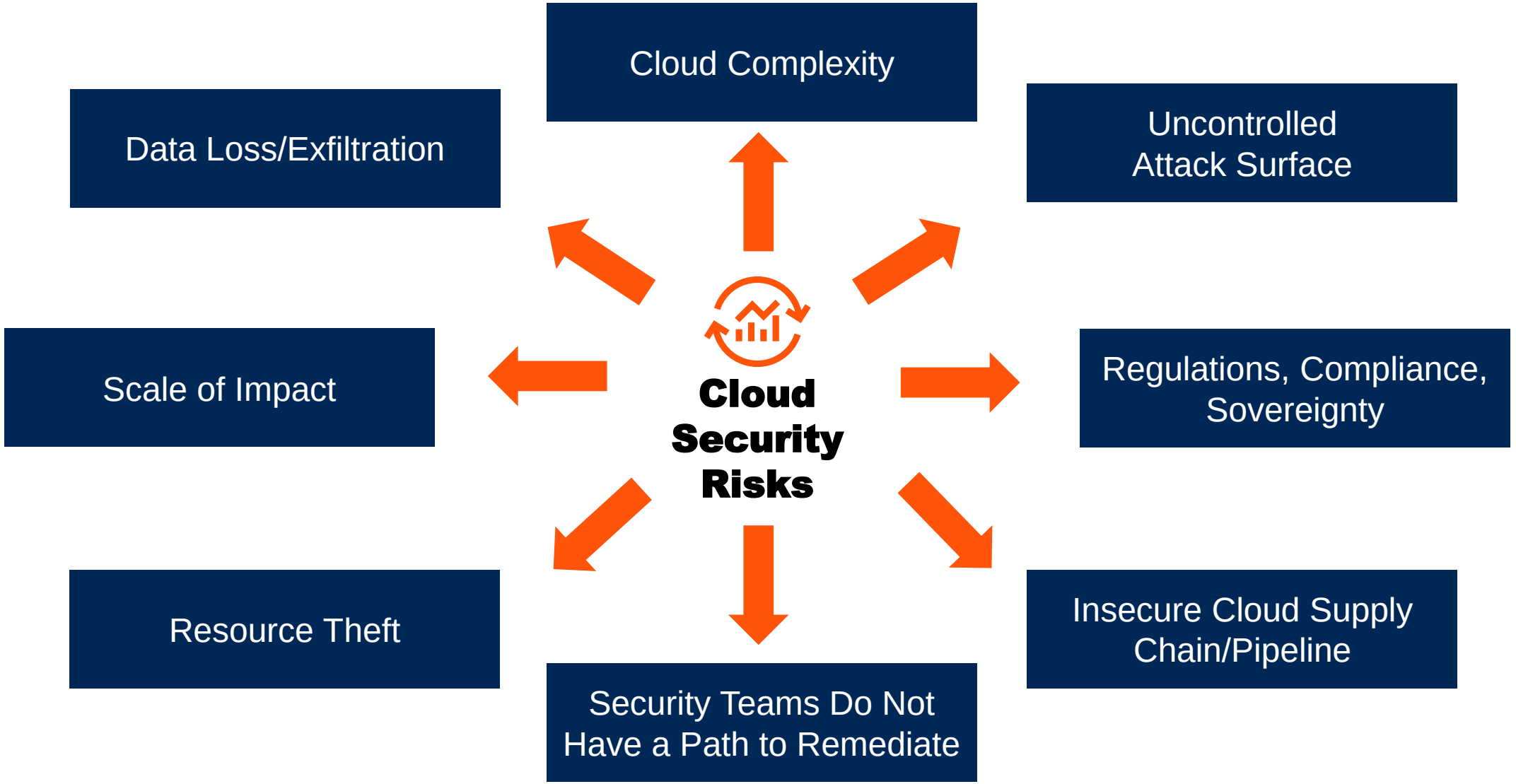
1. Cloud security challenges and risks today
2. Establishing effective cloud security
3. New trends in cloud security

Key Issues

1. **Cloud security challenges and risks today**
2. Establishing effective cloud security
3. New trends in cloud security

Gartner

Cloud Security Risks



Cloud Security Challenges ...

- Lack of Visibility
- Lack of Governance
- Policy Errors
- Speed of Change
- Skills Gaps
- Access and Entitlement Complexities
- Shared Responsibility Misunderstandings
- Misconfiguration
- Compliance Gaps
- Lack of Guardrails

Cloud Security Challenges

Gartner®

Key Issue Take-Away:

The risks you face in cloud might be similar to those you face with your data center.

However, the controls you deploy in cloud to treat those risks could be entirely different.

Gartner

Key Issues

1. Cloud security challenges and risks today
2. **Establishing effective cloud security**
3. New trends in cloud security

Cloud-Ready Approach

Cloud Pattern Security Needs

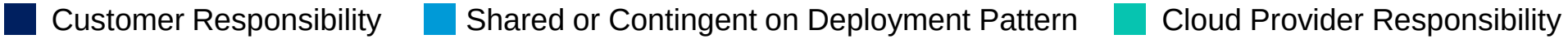
Upskilling for Cloud

Security Tooling

Protecting Hybrid Cloud

Gartner®

Shared Responsibility



	Private/ On-Premises	IaaS	CaaS	FaaS	PaaS	SaaS
Business Continuity						
Identity and Access Management						
Data						
Application						
Application API						
Workload						
Virtual Network						
Service Orchestration						
Virtualization/Cloud Infrastructure						
Physical						

Upskilling

- Establish a cloud center of excellence
- Upskill your security team
- Evangelize cloud security

Strategy and Arch	Cloud Native	Supporting Tech
Cloud Security Frameworks	Cloud Provider Security Capabilities	Container and Kubernetes Security
Cloud Risk Management	Security Service Edge	Cloud API and Application Security
Cloud Security Architecture & Patterns	Cloud-Native Application Protection Platforms	Infrastructure and Policy as Code
	Cloud DevSecOps	

Gartner®

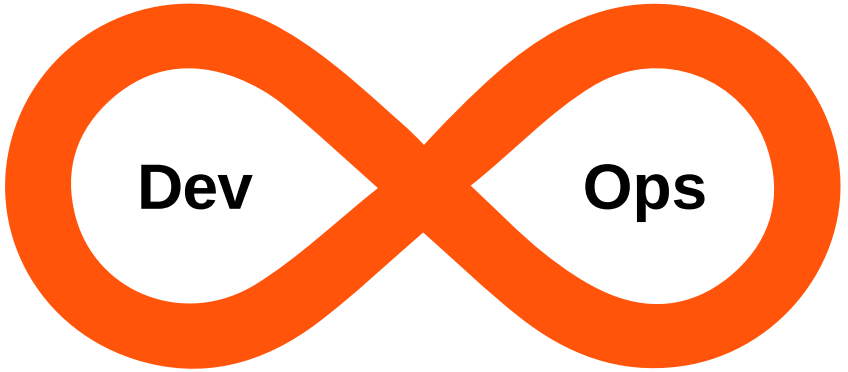
Cloud-Native Application Protection (CNAPP)

Artifact Scanning

(Application Code, API)

Exposure Scanning

Security



Cloud Configuration

Infrastructure as Code Scanning
Cloud Infrastructure Entitlements Management
Kubernetes Security Posture Management
Cloud Security Posture Management

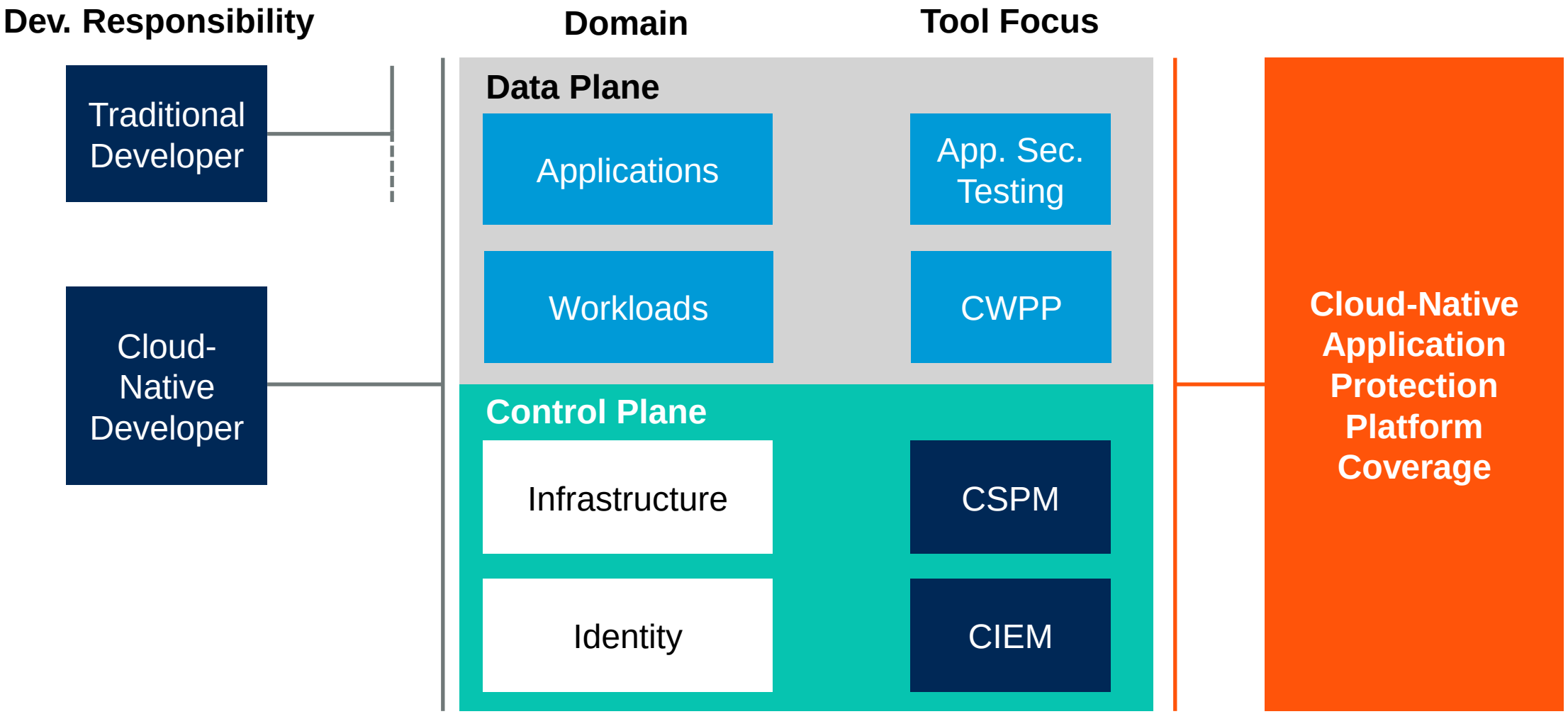
Runtime Protection

(Application and API, Cloud Workload Protection Platform, Network Segmentation)

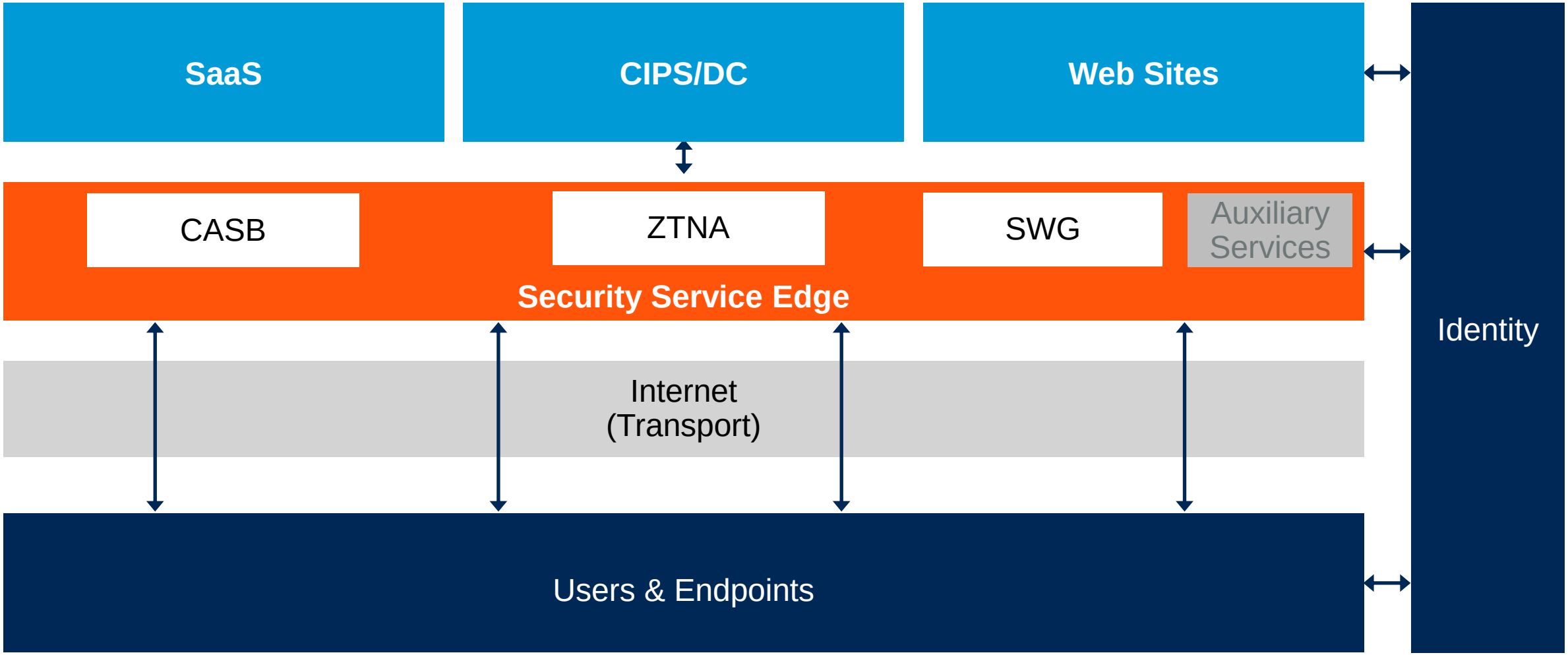
Exposure Scanning

Gartner®

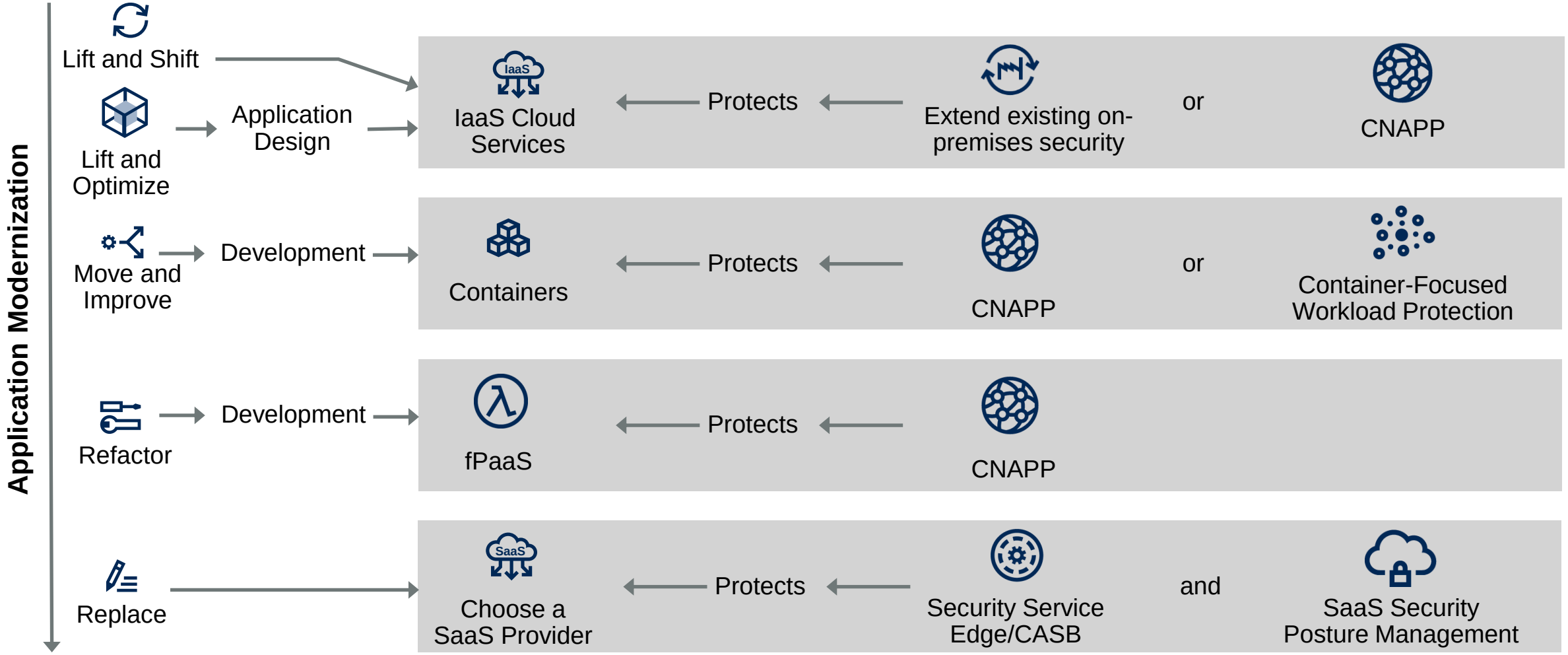
Iaas/PaaS — What Can CNAPP Provide?



SSE Coordinates Access to Cloud Services



Your Cloud Transformation Impacts Your Security Approach



Gartner®

Security Tooling Approaches

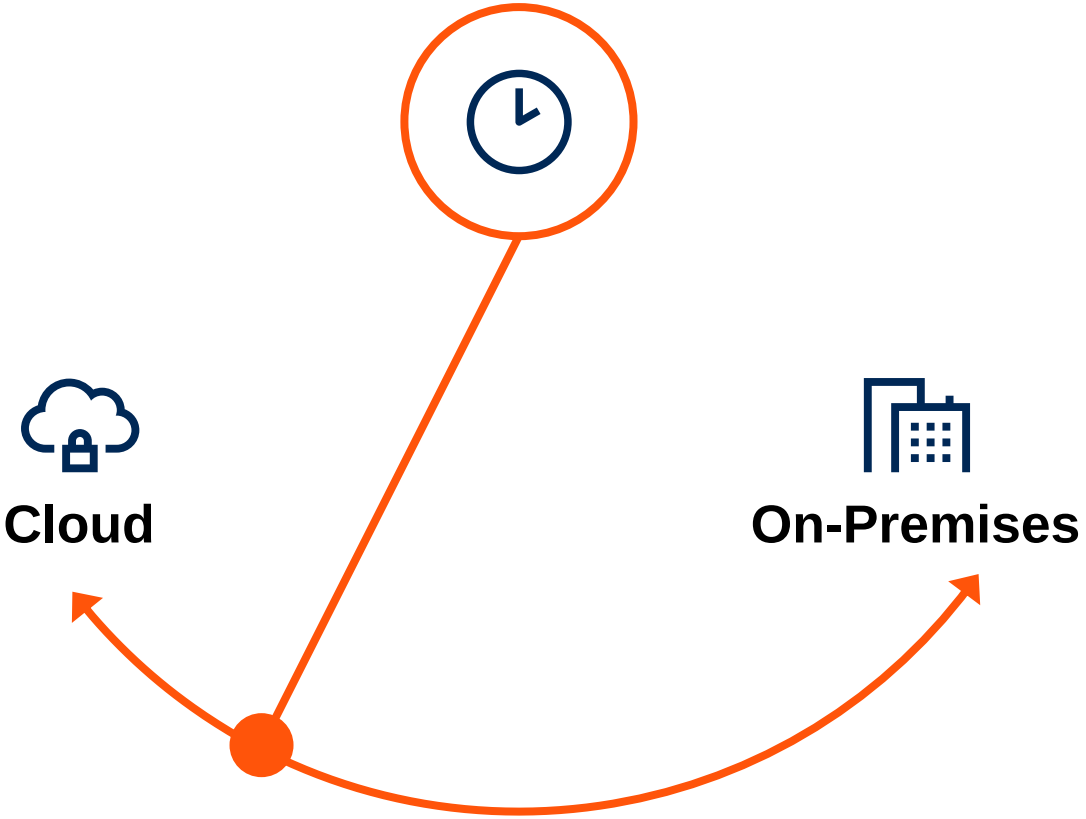
Tooling Source	Challenges	Risks Addressed	Tools
Import From On-Premises	Limited Protection Profile Cannot Protect Distributed Services Backhaul Costs Too High	Data Loss/Exfiltration **Some** Attack Surfaces	**EDR** **NGFW** **SIEM**
Cloud Provider	Focused on Their Own Cloud Limited Feature Set Potential Hidden Costs	+ Wider Attack Surface, Resource Theft, Regs, Compliance, & Sovereignty	**CNAPP** **VM** **TDR**
Third-Party Vendor	Complex and Changing Markets Very Large Number of Vendors Potentially Expensive	+ Complexity Path to Remediate Supply Chain Scale of Impact	**CNAPP** **SSPM** **SSE**

Gartner®

Learn what the service-provider tools do not provide before spending time and money on replacements. Move to third-party tooling where controls are missing, as complexity increases and for higher risks.

Gartner

Hybrid — Learning From Cloud to Secure the Enterprise



As more enterprise systems migrate to cloud:

- Assess cloud security successes
- Determine what can be brought back to on-premises/data center systems
- Look to control security from the cloud
- Seek to have as many common controls as possible

Gartner®

Key Issues

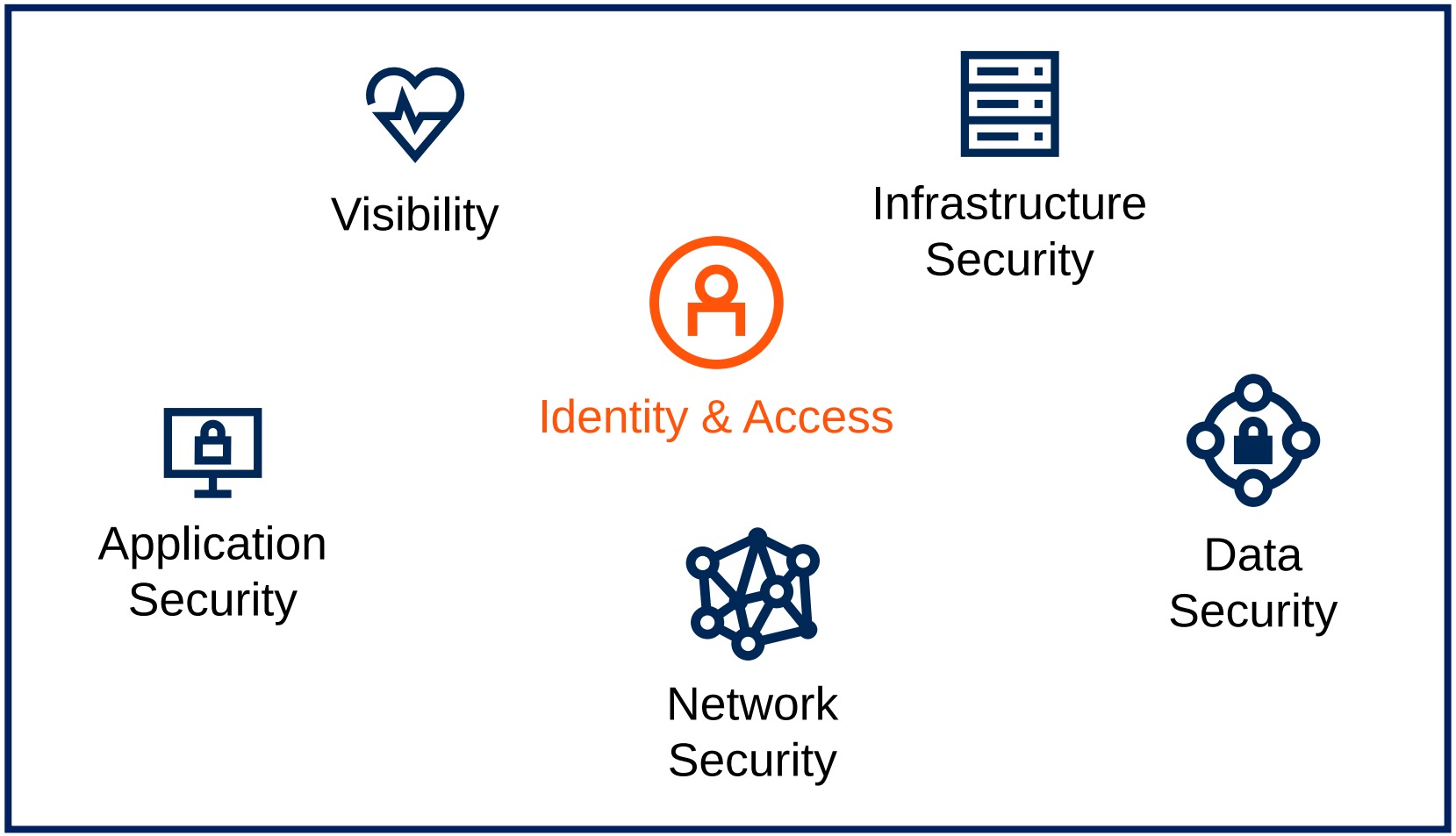
1. Cloud security challenges and risks today
2. Establishing effective cloud security
3. **New trends in cloud security**

Gartner

Emerging Trends

- Platform Engineering/CI/CD/ DevSecOps
- Security Data Analytics and AI/ML
- Zero Trust Architectures
- Risk Prioritization and Remediation Efficiencies
- Security Posture Management Extensions
- Continued Security Tool Convergence
- Confidential Computing
- Cloud Detection and Response
- Data and Cloud Sovereignty

Using Cloud Tooling to Enforce Zero-Trust Principles



Zero-Trust Security

Gartner®

Platform engineering, DevOps, AI/ML challenges and the speed of change in our clouds mean that we need continued stress on risk prioritization, security governance, asset and activity visibility, and cloud detection and response.

Gartner®

Recommendations

- Match your controls to your situation; SaaS, PaaS variants and IaaS.
- Automate configuration validation — across all clouds.
- Shift left and work **with** your developers and in **their** world.
- Own and tightly control identity and privilege — and monitor!
- Use the adoption of the cloud as a catalyst to adopt zero trust by default.

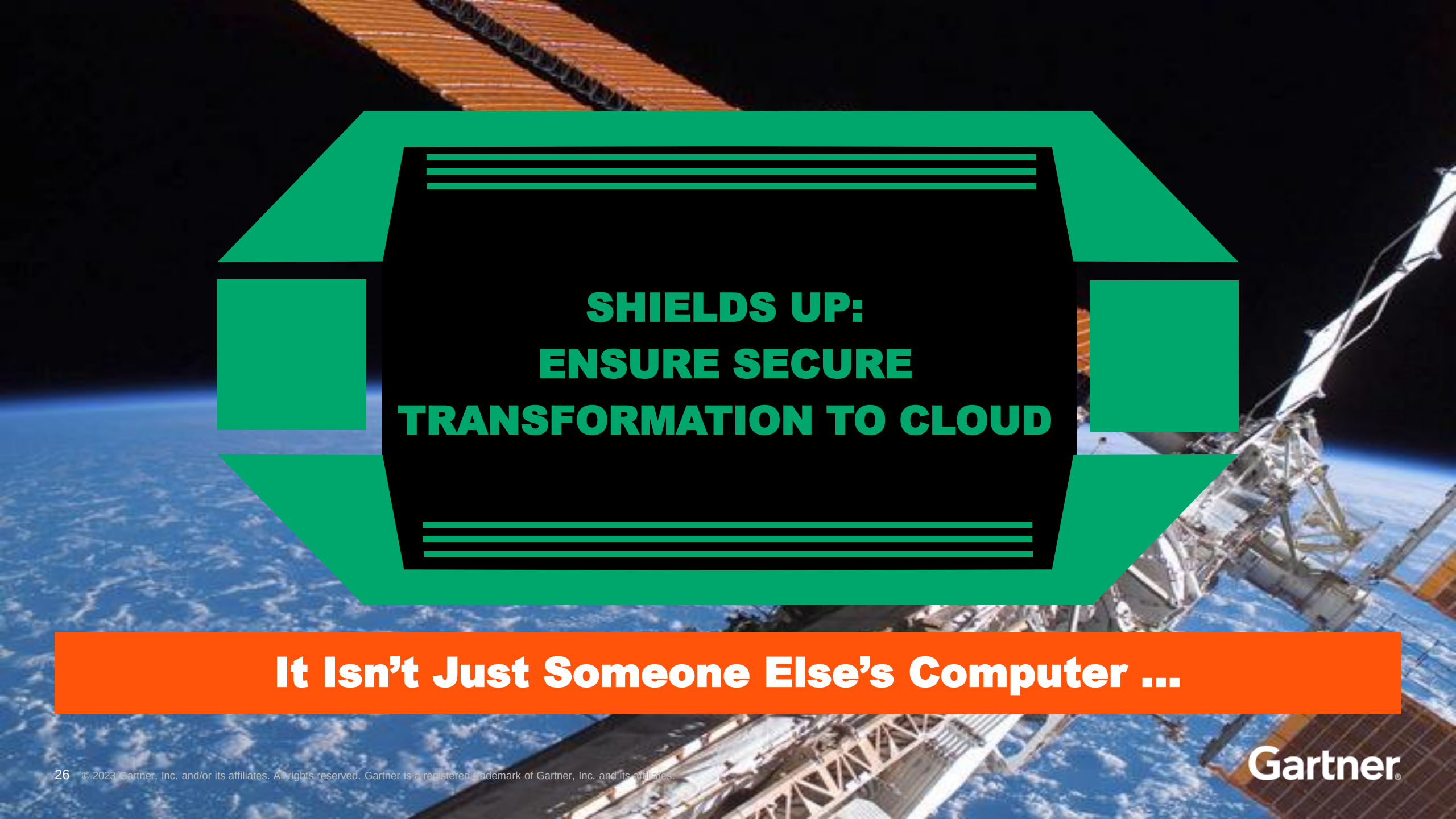
Recommended Gartner Research

- **Risk-Based Evaluations of Cloud Provider Security**
  Charlie Winckless and Jay Heiser
- **Adopt Security Service Edge (SSE) to Replace Stand-Alone SWG, CASB and ZTNA Products**
  Dennis Xu, Jon Amato and Patrick Hevesi
- **Essential Skills for Cloud Security Architects**
  Fred Sotolongo
- **Solution Path for Security in the Public Cloud**
  Richard Bartley

Gartner®

The Decision to Move to Cloud Has Already Been Made …

Gartner



SHIELDS UP: ENSURE SECURE TRANSFORMATION TO CLOUD

It Isn’t Just Someone Else’s Computer …

Gartner®

For most cloud users, the move increases security. Navigate the shared responsibility model to select what could be entirely different controls to handle your risks.

Gartner