Gartner Webinars

Gartner delivers actionable, objective insight, guidance and tools to enable stronger performance on your organization’s most critical priorities

Gartner®

Enhance your webinar experience

Ask a Question

Download Attachments

Share This Webinar

Cut Through Zero Trust Hype and Get Real Security Strategy Advice

Connect with Gartner

Neil MacDonald

Distinguished VP Analyst

Gartner

Polling Question 1 of 3

Which of the following best describes your attitude about zero trust?

A. **It's the latest buzzword, nothing really new.**

B. **It's an interesting idea, but largely just an evolution of what we are already doing.**

C. **The concept is valuable, and we have plans to adopt zero trust principles in a few specific areas.**

D. **It's a significant mindset shift that we will fully embrace over the next several years.**

How to participate in our polling

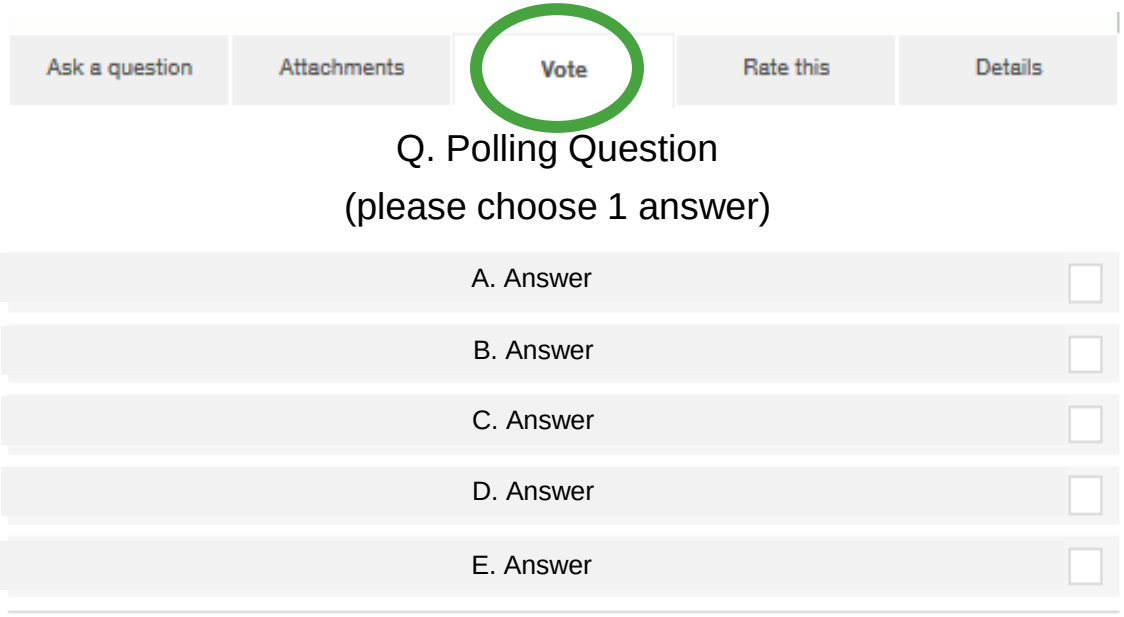
If you are in full screen mode – click Esc

The poll question is on the "Vote" tab.

Please click the box to make your selection.

Upon voting you will see the results.

Thank you!



Zero Trust Is Not “Zero Trust”

In order to get things accomplished, trust must ultimately be extended …

Zero Trust Is Not “Zero Trust”

In order to get things accomplished, trust must ultimately be extended …

… and continuously assessed for acceptable levels of risk/trust … and our security infrastructure should adapt accordingly.

Zero Trust Is Abused

It’s like the word “cloud” — overloaded, but useful.

Zero Trust Is Abused

It’s like the word “cloud” — overloaded, but useful.

There are things you can absolutely do in 2022 to move toward zero trust.

What Is Zero Trust and Why Is It Important?

We've used location, ownership and control of physical assets as an implicit proxy for trust.

This is a flawed security paradigm.

Gartner®

The Definition of Zero Trust by the National Institute of Standards and Technology (NIST)

Zero trust is a **cybersecurity paradigm** focused on resource protection and the premise that trust is **never granted implicitly** but must be **continually evaluated**.

Gartner®

Existing Security Patterns Leave Too Much Implicit Trust.

Pragmatic Explanation:

Zero Trust

Means

Zero Implicit Trust

Gartner®

Gartner Perspective:

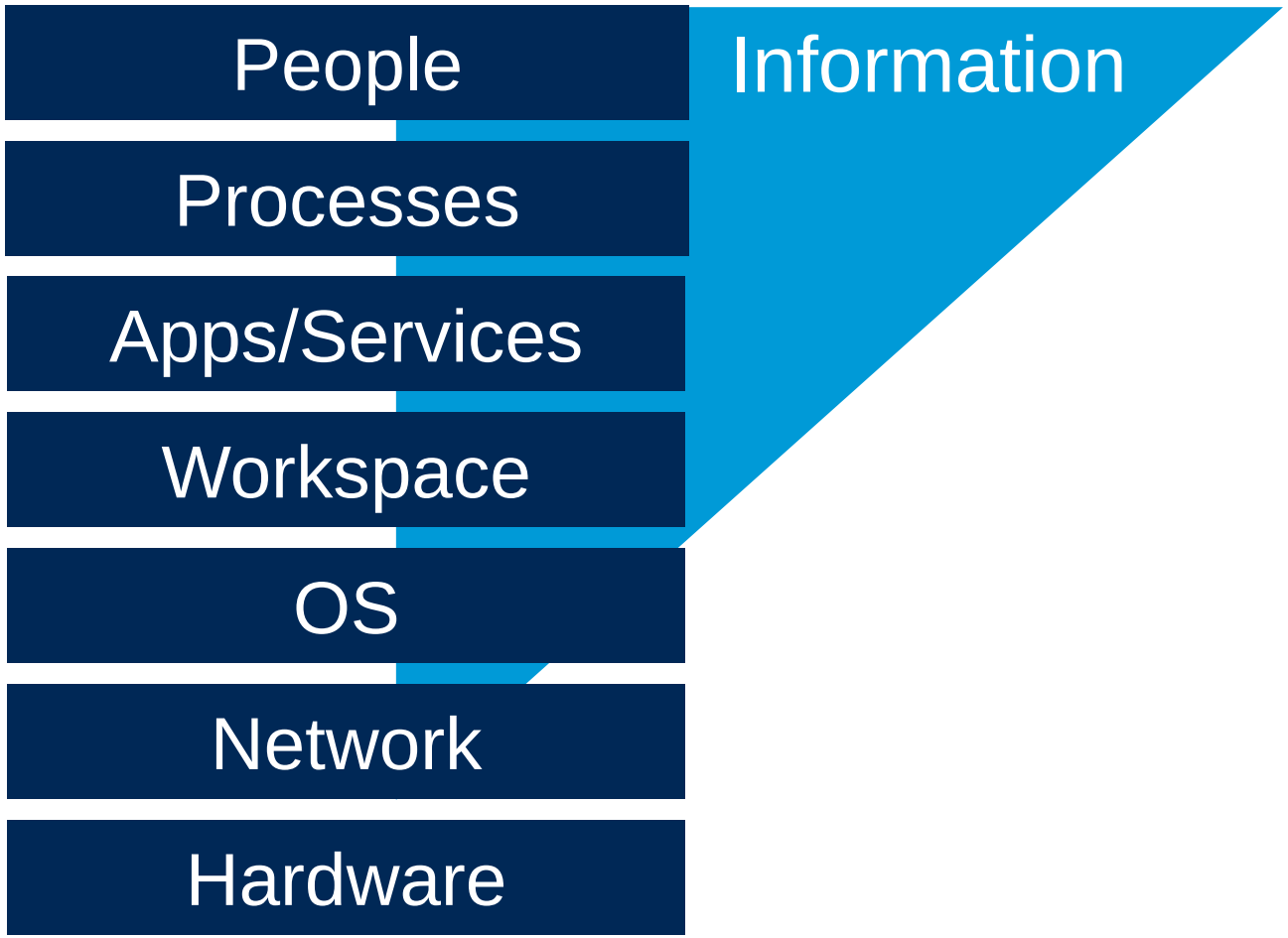
Zero trust is a security paradigm that replaces implicit trust with continuously assessed explicit risk/trust levels based on identity and context supported by security infrastructure that adapts to risk-optimize the organization's security posture.

Gartner®

Zero Trust (Security)	**Mindset/Paradigm**
Zero Trust Strategy	**Systematic Approach to Replace Implicit Trust With Adaptive Trust Across All of IT**
Zero Trust Initiatives **Conditional (Adaptive) Access** **Machine Identity management** **Zero Trust Network Access** **Identity-Based Segmentation**	**Specific Projects** **Specific Architectures**

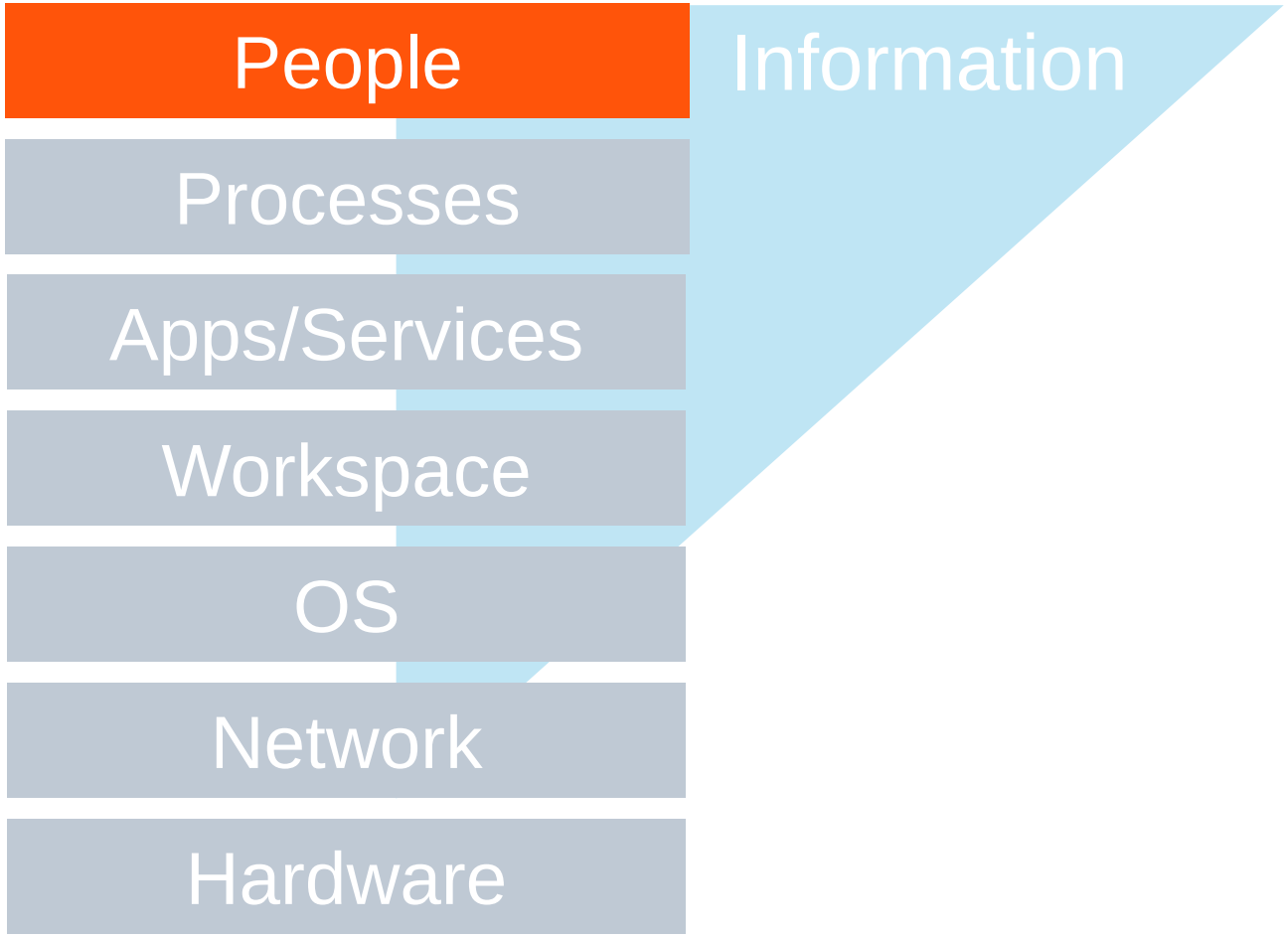
Gartner®

In a World of Cloud and Remote Work, What Do You Really Control?



Identity + Context Form the New Perimeter

Identity First!



Zero Trust Requires a Solid Identity Foundation

- Identify directories and trust relationships
- Implement SSO and activate MFA
- Standardize third party identity management
- Shift to cloud-based IdaaS
- Lockdown on-premises directory servers
- Activate directory behavioral monitoring
- Build a strategy for machine identities

Polling Question 2 of 3

Does your identity and access management team have a governance strategy for managing machine identities (devices, IoT/OT, virtual machines, containers and so on)?

A. **No. The machine identities are managed by the teams responsible for the devices/machines/containers. There is no central governance.**

B. **Partially. Some of this is decentralized while some is centrally managed such as PC identities.**

C. **Yes. The IAM team's framework for identity governance comprehensively covers human and machine identities.**

How to participate in our polling

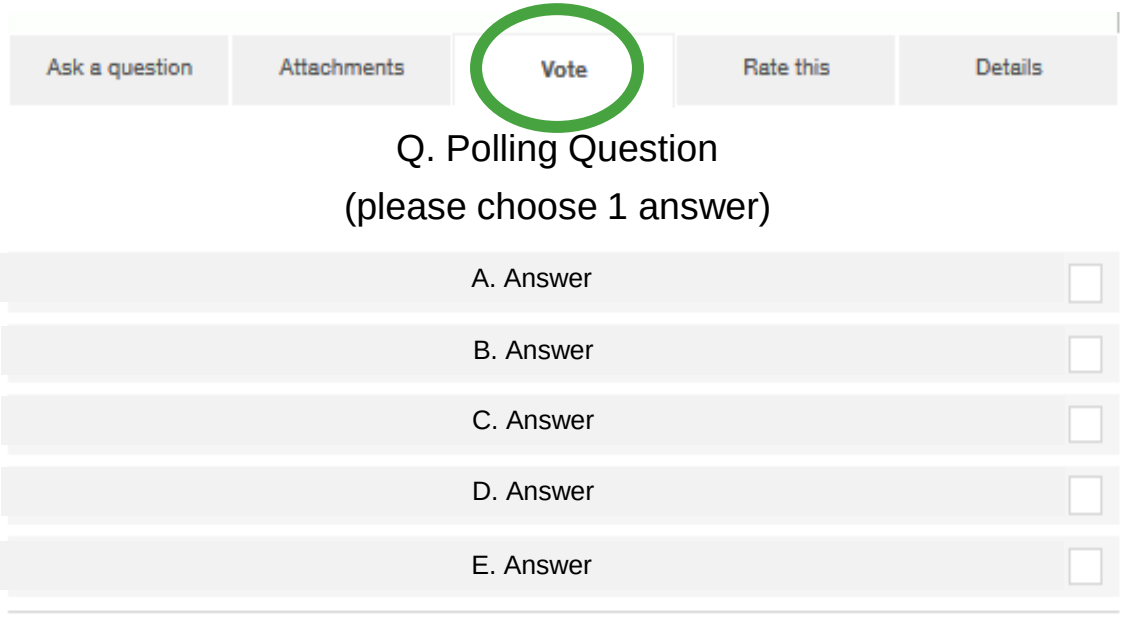
If you are in full screen mode – click Esc

The poll question is on the "Vote" tab.

Please click the box to make your selection.

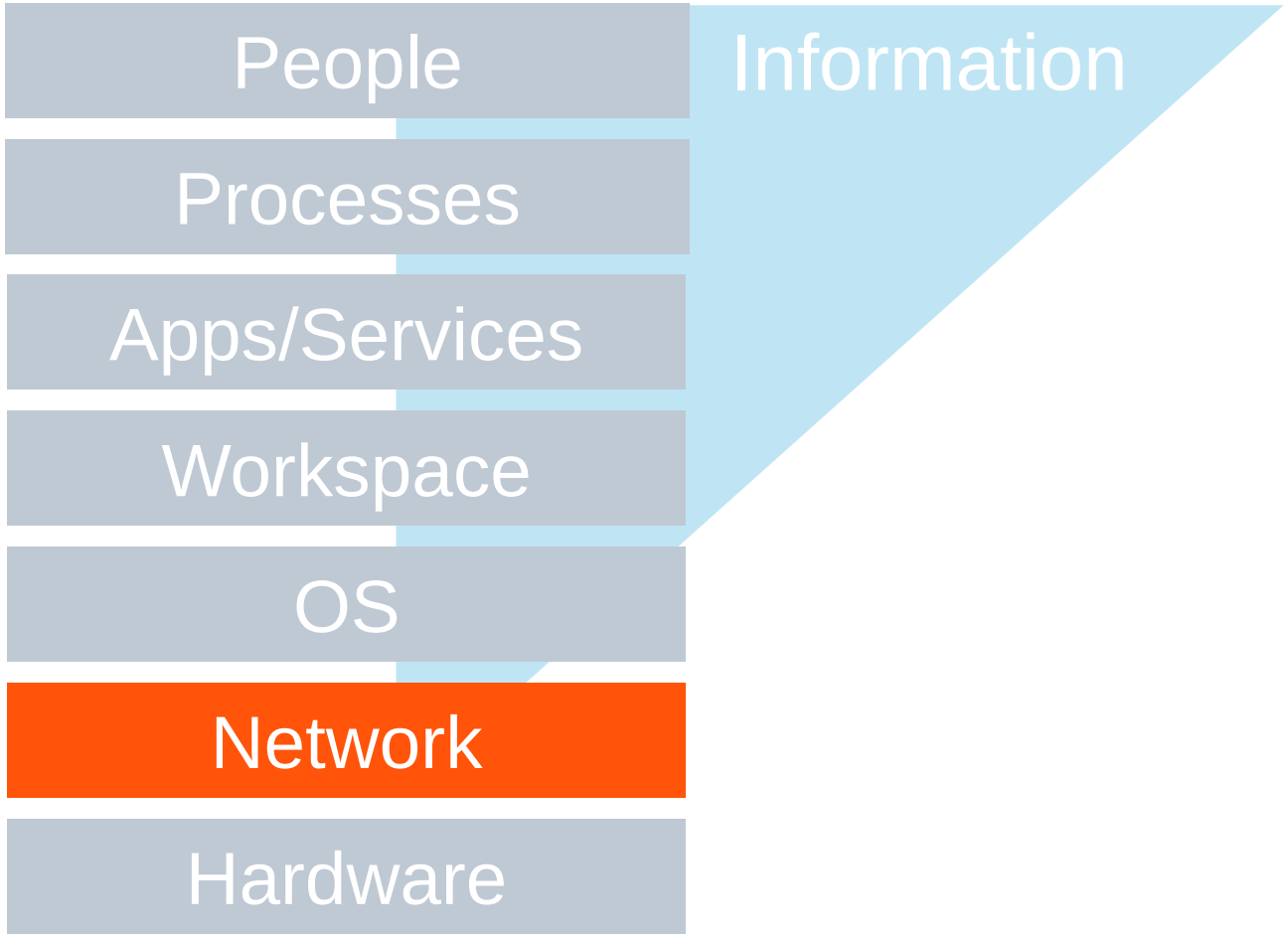
Upon voting you will see the results.

Thank you!



What Is Zero Trust Networking and Why Is It Important?

With the Identity Foundation in Place, Most Zero Trust Initiatives Start Next With Networking



Why Start With Zero Trust Networking?

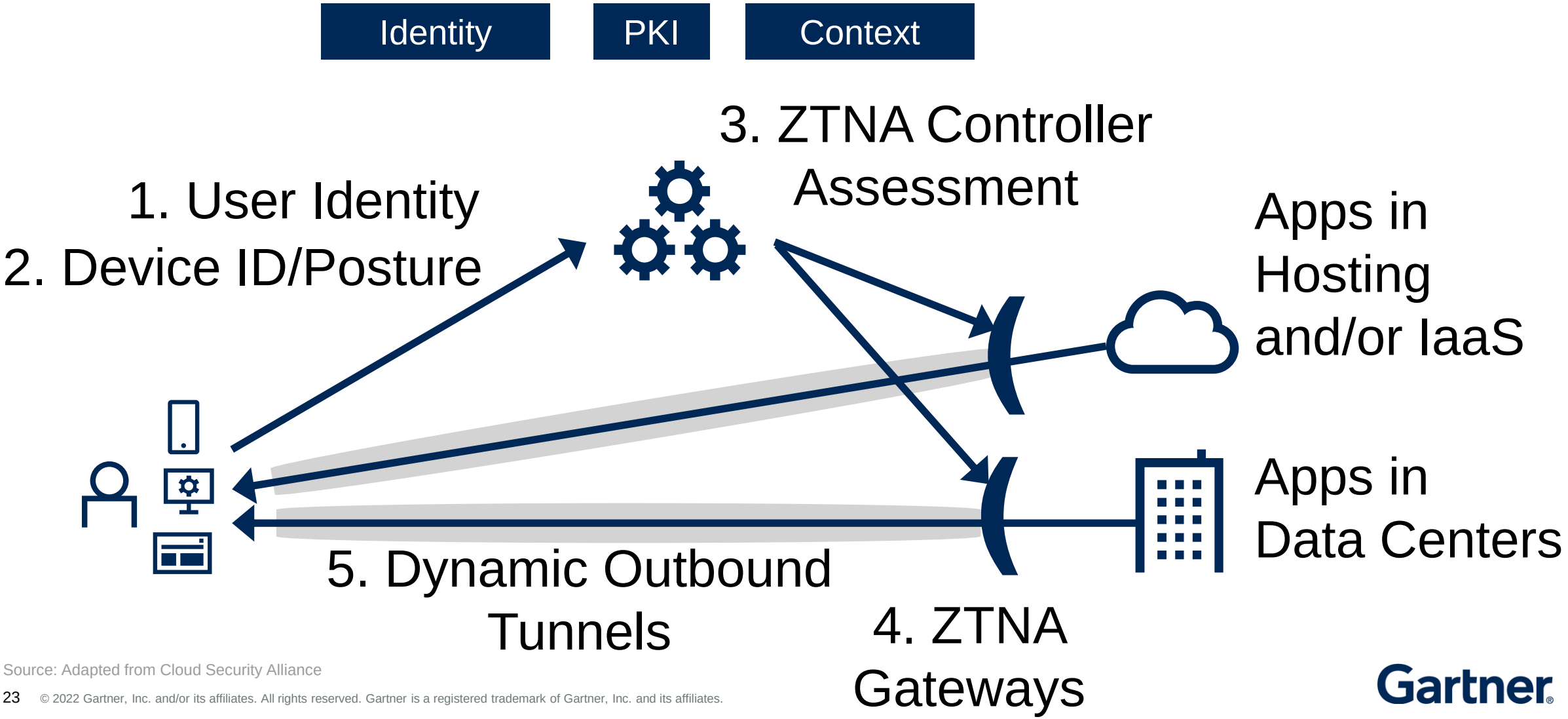
- TCP/IP design assumed trusted network connectivity.
- This excessive implicit trust leads to excessive latent risk.
- VPNs and DMZs are crude workarounds with excessive risk.
- IP addresses are weak identifiers.

Old model: Connect, then authenticate.
New model: Authenticate, then connect.

Key Tenets of Zero Trust Networking
“Never Trust, Always Verify”

- Assume compromise.
- The network is not trusted, even internally.
- Encrypt all communications.
- Your location inside/outside doesn’t matter.
- User/entity identity to establish trust.
- Use as much context at the point of access as possible.
- Extend risk-appropriate/least privileged access.
- Monitor everything, identify anomalies and excessive risk.

Zero Trust Network Access Project (Software-Defined Perimeter)



Source: Adapted from Cloud Security Alliance

Zero Trust Network Access Sample Vendors

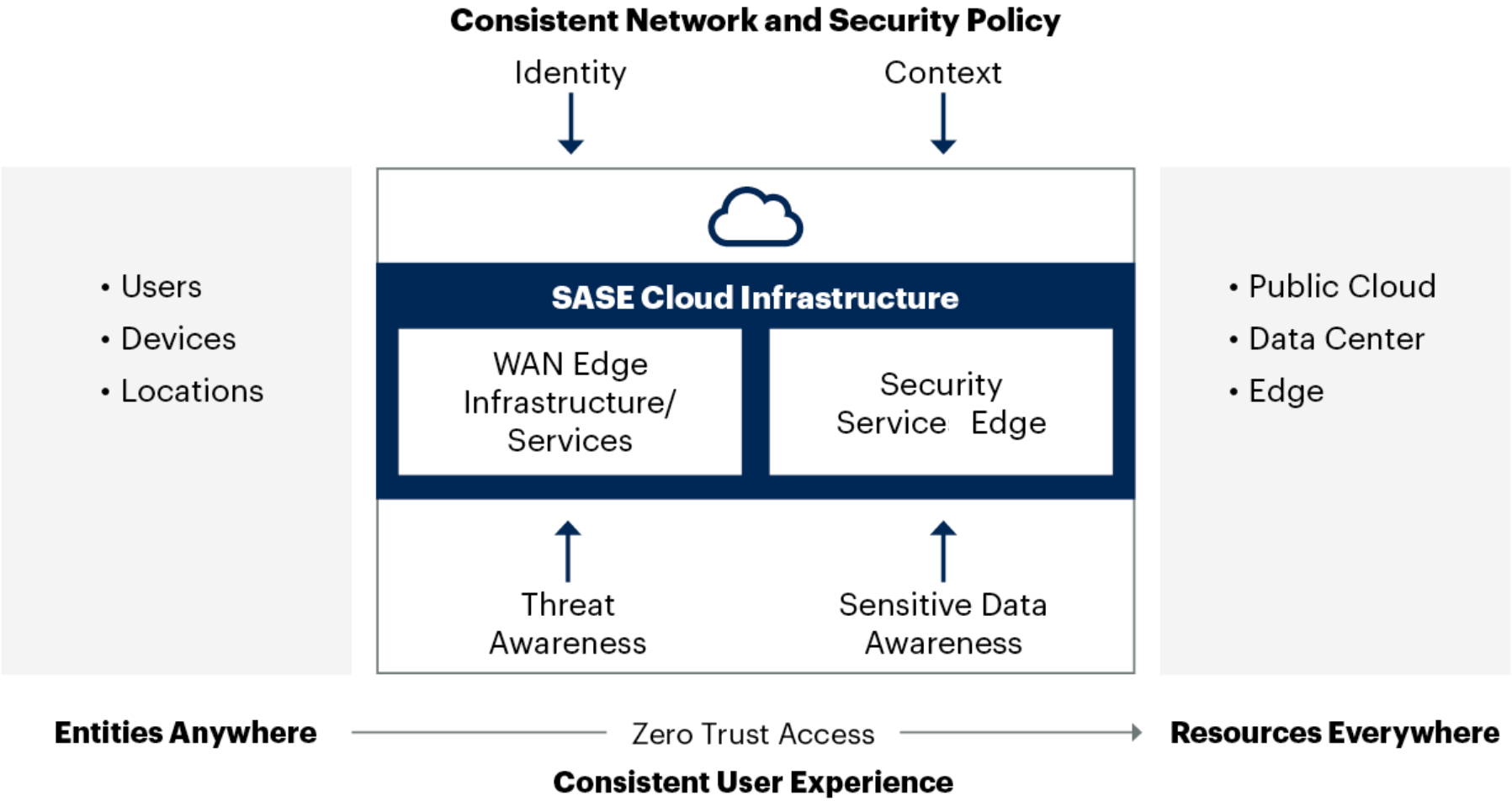
Cloud-based

- Akamai
- Broadcom (Symantec)
- Cato Networks
- Cisco (Duo Beyond)
- Fortinet (OPAQ)
- Google BeyondCorp
- McAfee
- NetMotion (VPN and SDP)
- Netskope
- Okta
- Palo Alto Networks
- Perimeter 81
- Proofpoint
- Zscaler

Customer Controlled

- Appgate
- Banyan Security
- BlackRidge
- Check Point Software Technologies (Odo Security)
- Forcepoint
- Google Cloud Platform
- Ivanti (Pulse SDP)
- Microsoft (Windows and Azure)
- Safe-T
- Unisys
- Waverley Labs
- Zentera Systems

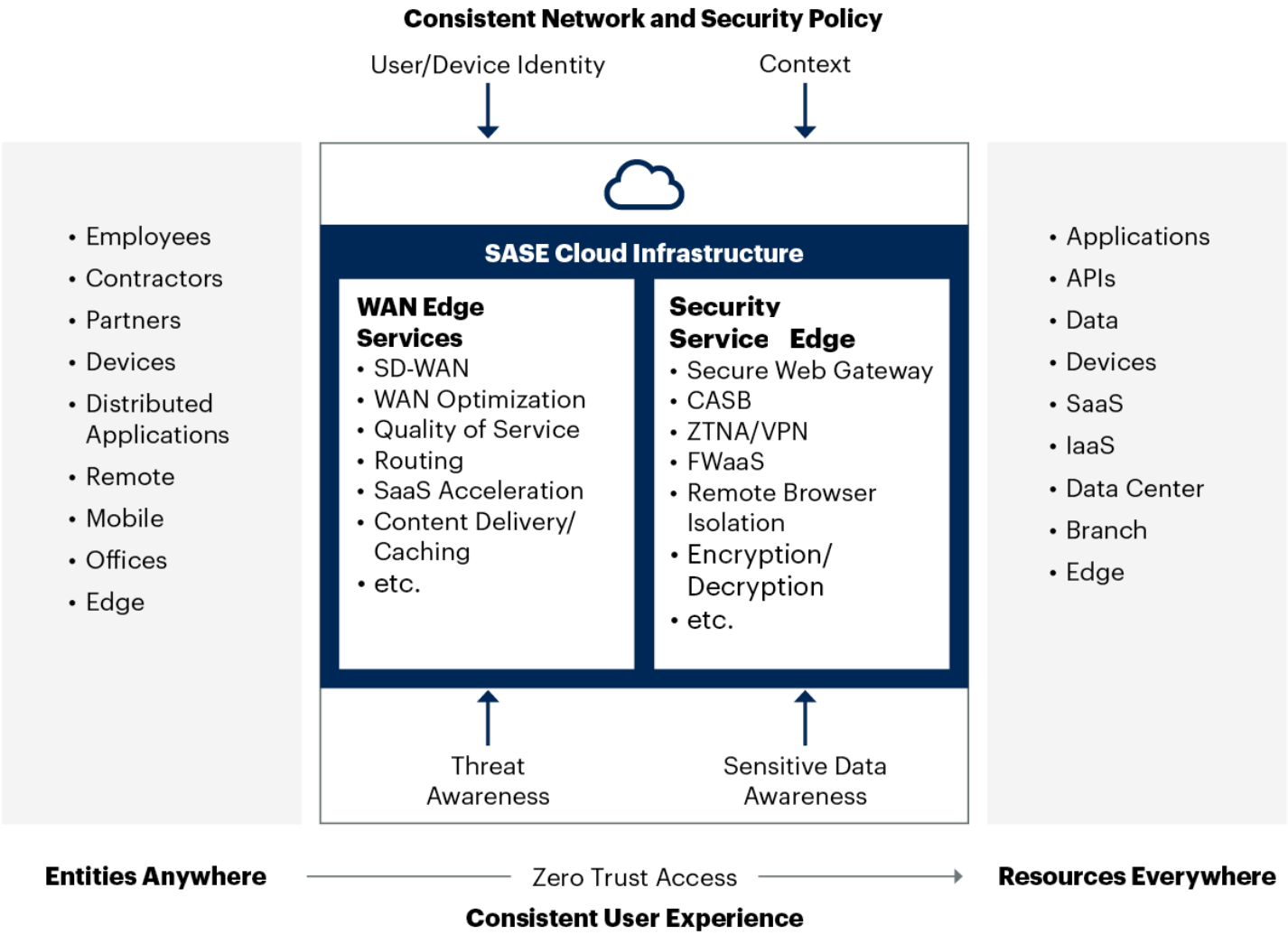
Secure Access Service Edge (SASE)



Source: Gartner

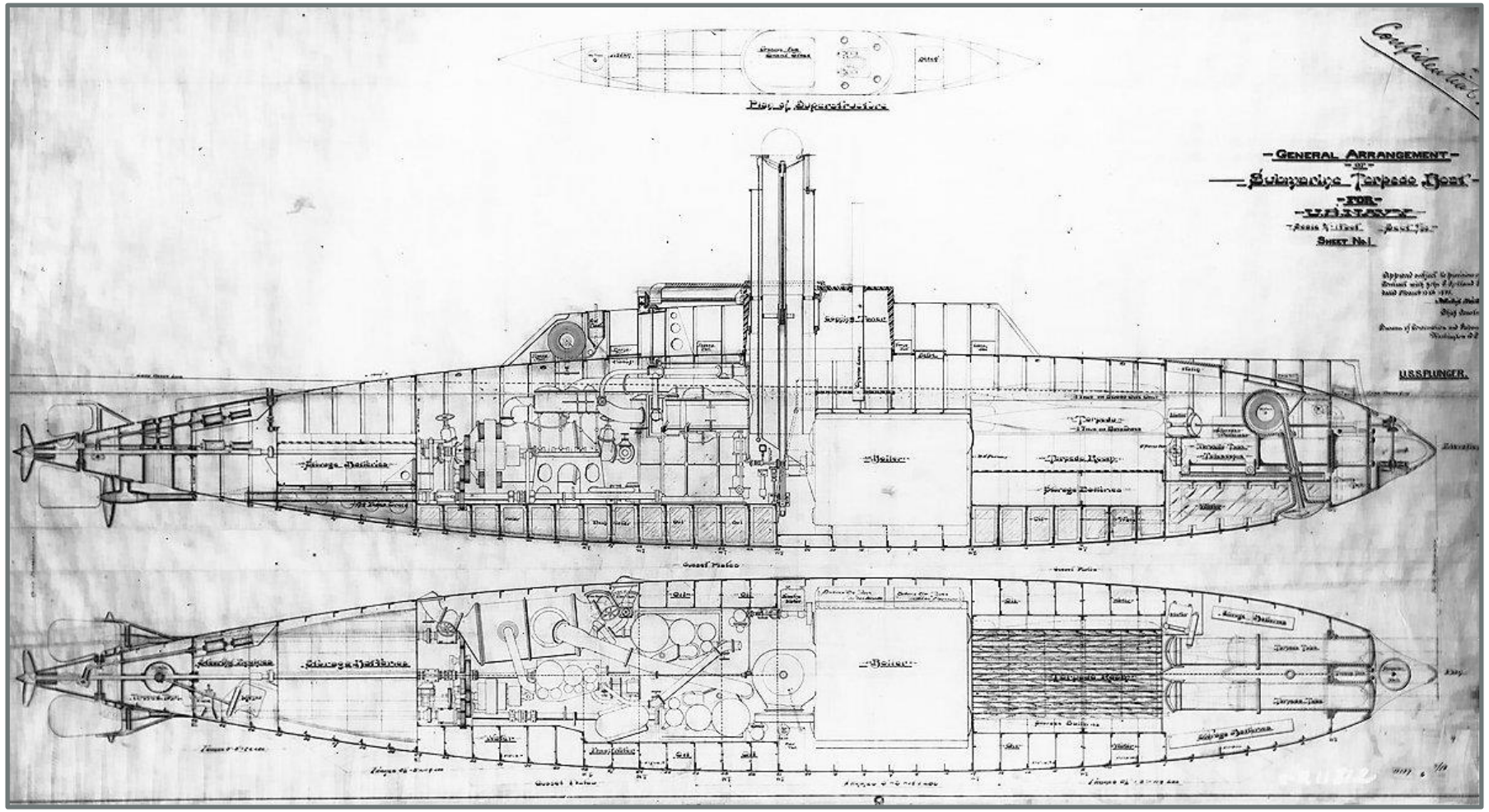
741491_C

Secure Access Service Edge (Detailed View)



Source: Gartner
741491_C

Submarines Assume Breaches, Why Not Data Centers? Zero Trust Network Segmentation/Identity-Based Segmentation



Gartner

Identity-Based Segmentation Sample Vendor List

Network Overlay

- AlgoSec, Tufin, FireMon (APIs)
- Cisco (ACI/ISE)
- Juniper
- ShieldX
- vArmour (APIs)
- VMware NSX

Built-in Segmentation

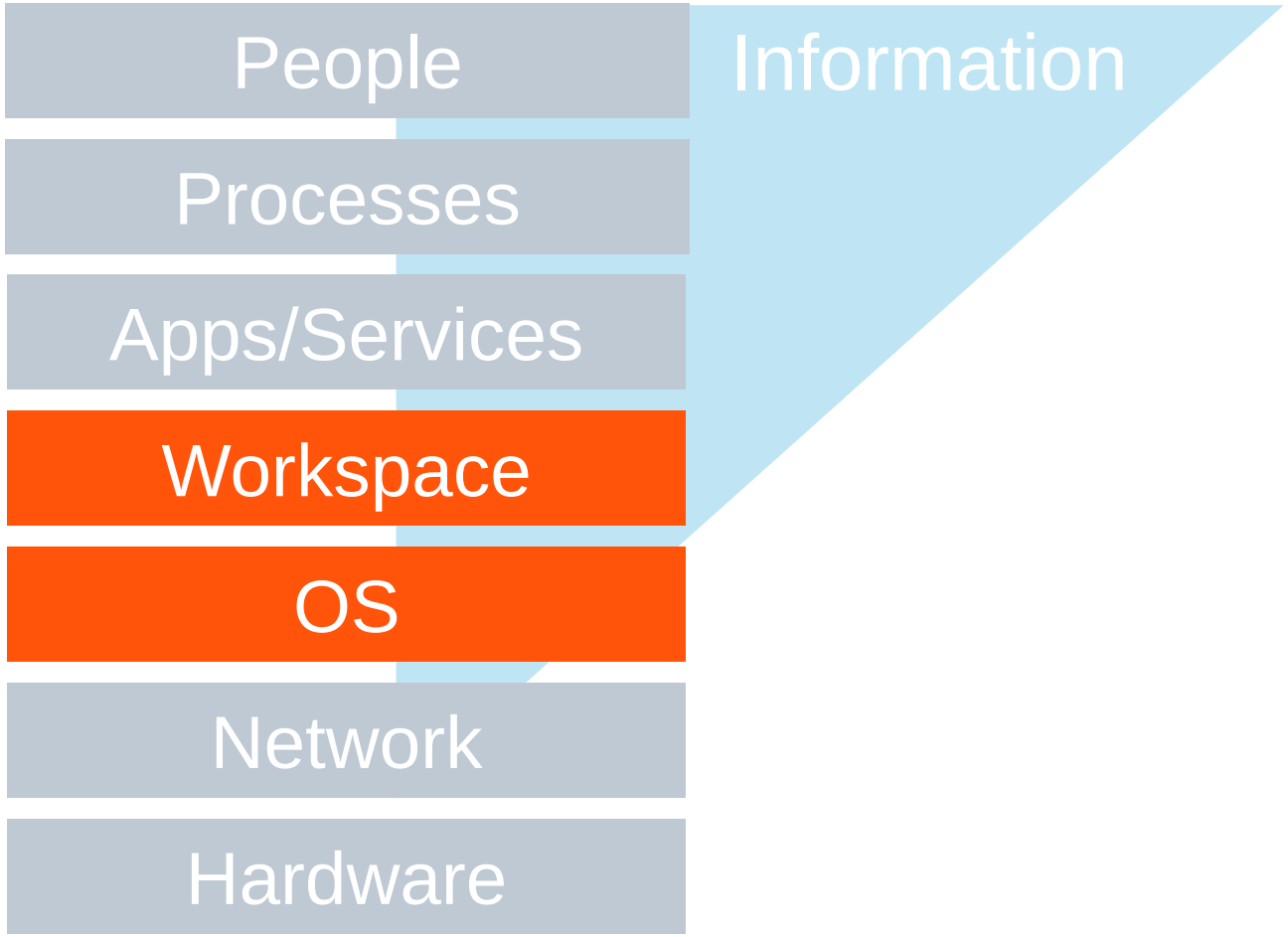
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Host/container

- Akamai (Guardicore)
- Aqua Security
- Cisco Secure Workload and Cisco (Portshift)
- Illumio
- NeuVector
- Palo Alto Networks (Prisma Cloud)
- Rapid7 (Alcide)
- Tigera (Calico Enterprise)
- TrueFort
- Zscaler Workload Segmentation

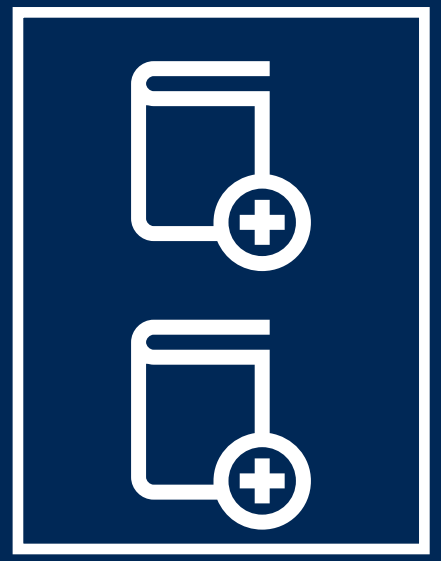
Beyond Networking, How Can Enterprises Pragmatically Start Evolving Their Overall Security Posture Toward Zero Trust?

What Can We Do at the Operating System and User Workplace Layer?



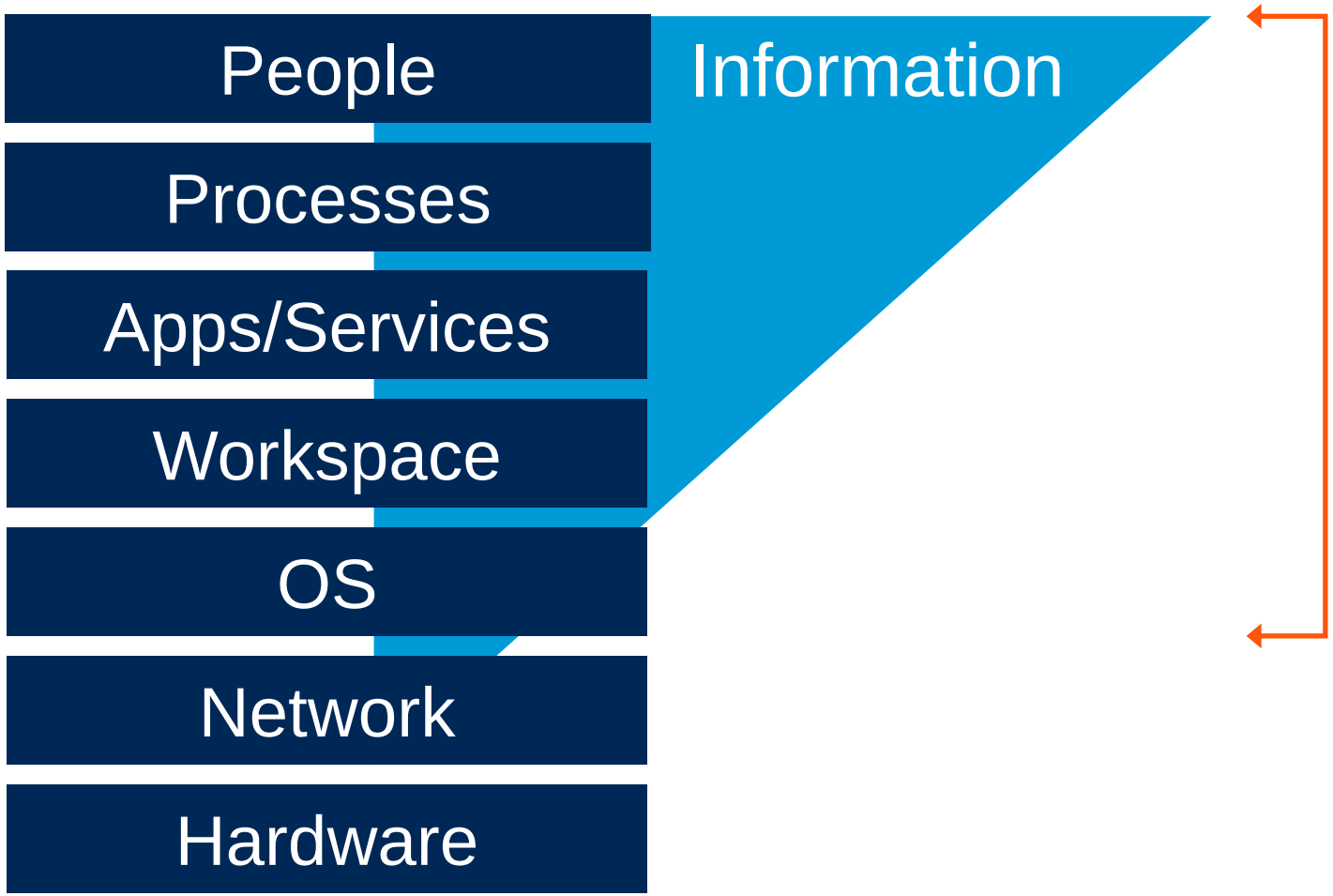
Remove Admin Rights From End-User Systems, Especially Windows

Implement Default Deny on Critical Servers/VMs



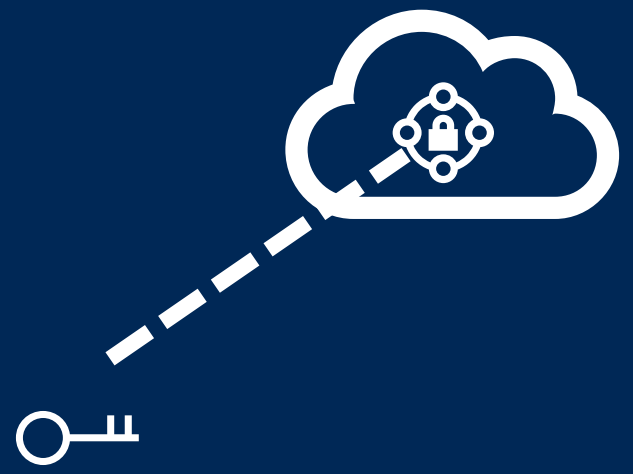
Pilot a Remote Browser Isolation Solution

What Can We Do With Information?



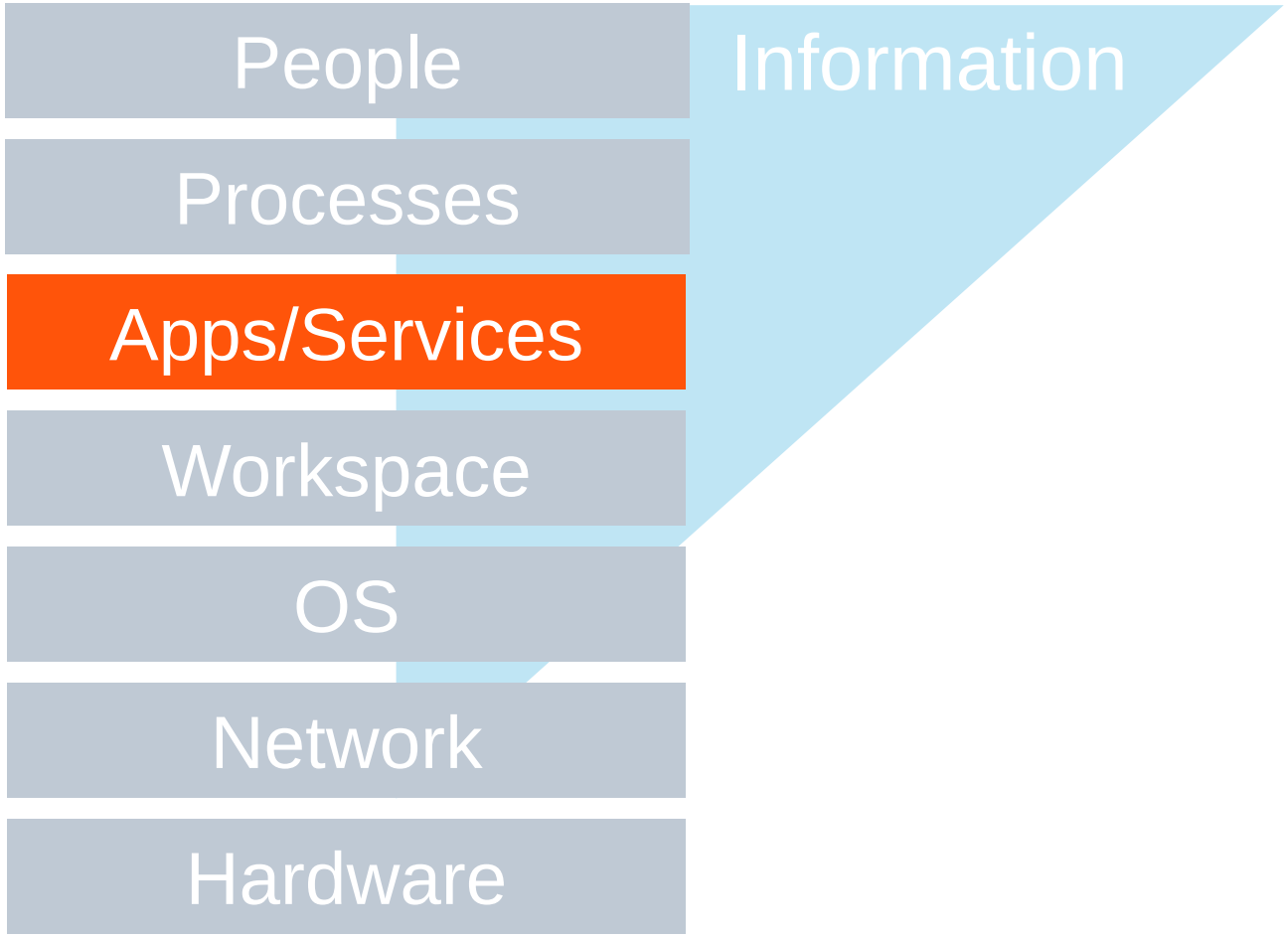
Encrypt All Data at Rest in Public Cloud.

Hold Your Own Key (HYOK)



Gartner®

What Can We Do at the Application Layer?



Start Scanning Containers in Development for Known Vulnerabilities/Software Composition Analysis

At Runtime for Containers — K8S Admission Control, Allow Listing and Network Communications Control.

Gartner®

Cloud as a Catalyst for Zero Trust Initiatives

- ZTNA for end-user access to apps (no VPN, no DMZ).
- Segmentation by default.
- PAM/MFA for all administrative access.
- Full monitoring/logging all activities, actions and events for analysis.
- Cloud native applications offer opportunities:
  - Scanning of all components in development.
  - Container admission control and process control.
  - Segmentation for service-to-service communications.

Recommendations:
Ten Zero Trust Initiatives You Can Start Now

- Get the identity foundation in place.
- Implement conditional access for all, MFA for remote access.
- Implement PAM (or at a minimum, MFA) for all admins.
- Zero trust network access (ZTNA [replaces legacy VPN]).
- Encrypt all data at rest in public clouds with customer controlled keys.
- Remove admin rights from most Windows users.

Recommendations:
Ten Zero Trust Initiatives You Can Start Now

- Segment end-users off of the data center network.
- Segment (ringfence) critical applications.
- Pilot RBI for uncategorized sites or external URLs in email.
- Implement lockdown/allow-listing on critical servers.
- Engage with dev to scan containers for new apps. For Kubernetes, link dev scanning to admission control.

Polling Question 3 of 3

What is your highest priority zero trust project that you have budgeted for in 2022?

A. **Conditional access, SSO and/or MFA**

B. **Zero Trust Network Access**

C. **SASE / Secure Service Edge (ZTNA, SWG, CASB convergence)**

D. **Zero Trust Network Segmentation**

E. **Other**

How to participate in our polling

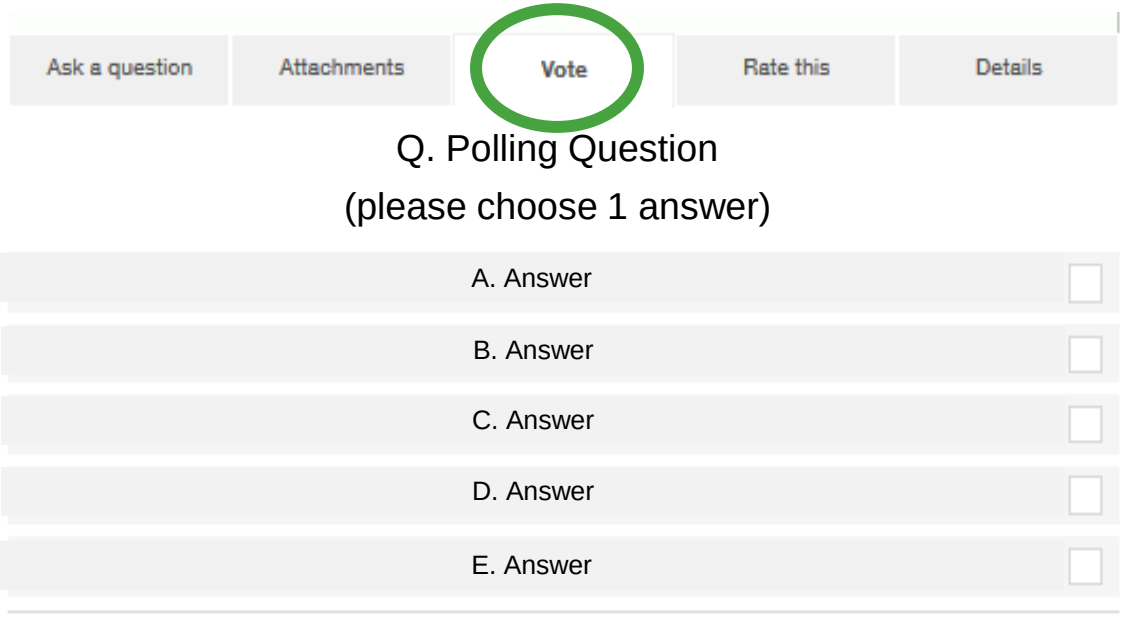
If you are in full screen mode – click Esc

The poll question is on the “Vote” tab.

Please click the box to make your selection.

Upon voting you will see the results.

Thank you!



Ask your questions

Gartner Security & Risk Management Summit

Gartner

14 – 15 February 2022 | Virtual (GST)
7 – 8 March 2022 | Virtual (IST)
7 – 9 June 2022 | National Harbor, MD
21 – 22 June 2022 | Sydney, Australia
25 – 27 July 2022 | Tokyo, Japan

Hear independent experts on what matters most now and how to prepare for what's ahead. You'll learn how to create the security and integrated risk management plans you need to give your organization the freedom to grow and innovate with confidence.

Learn more: gartner.com/conf/security

Register with code **WEBINAR** for an exclusive discount.

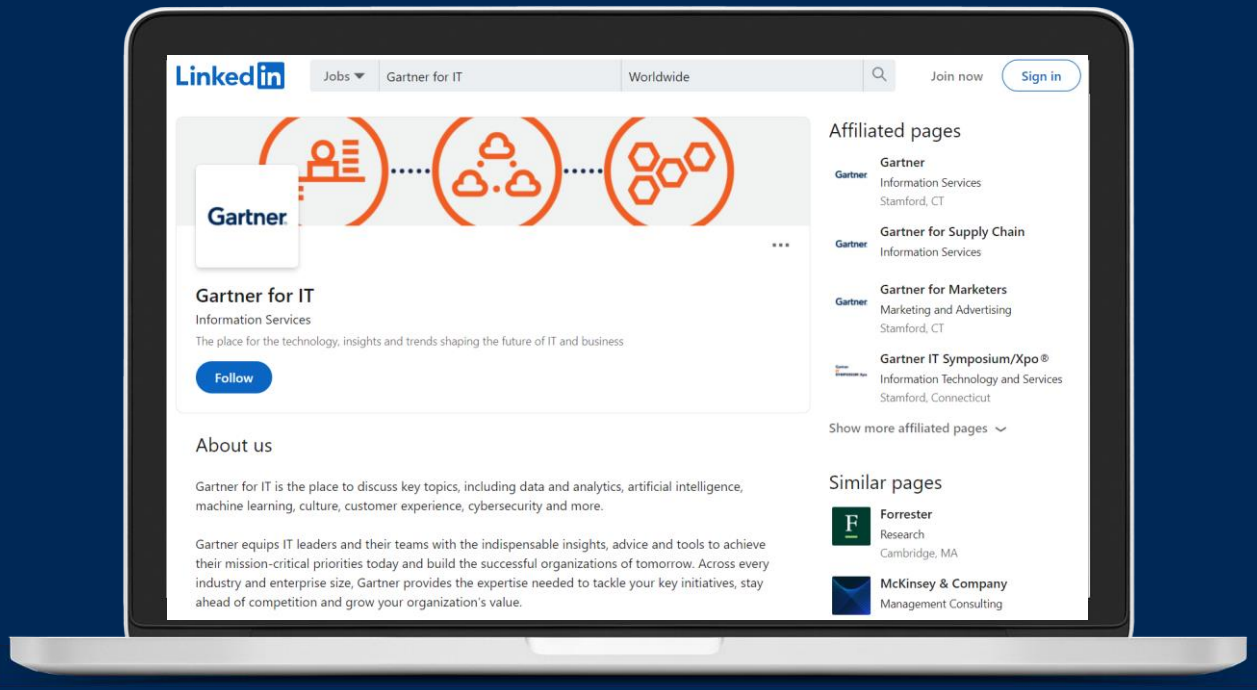
At this year's conference, you'll learn how to:

- **Design secure architectures** and technical solutions to support digital business objectives
- **Adapt your data privacy management program** to keep pace with rapidly developing regulations
- **Understand the latest trends** in cybersecurity, cloud security, application security, data security and related technologies

Gartner for IT on Social Media

Want to stay in-the-know? Connect with us on LinkedIn and Twitter to receive the latest Gartner IT insights and updates across research, events and more.

It's all curated specifically for IT leaders and decision-makers.



Follow us on

Gartner®

Gartner is a trusted advisor and an objective resource for more than 14,000 enterprises in 100+ countries.

Learn more about how we can help you achieve your most critical priorities.

Become a Client

U.S.: 1 800 213 4848
International: +44 (0) 3331 306 809

"The research is great, and the ability to interact with Executive Partners — and the symposiums and regional forums — are incredibly valuable."

Russell Morris
CIO, TransGrid

Gartner

Get more Gartner insights

Download the research slides

View upcoming and on-demand Gartner webinars at gartner.com/webinars

Rate this webinar