How to Apply Zero Trust to Strengthen Endpoint Security

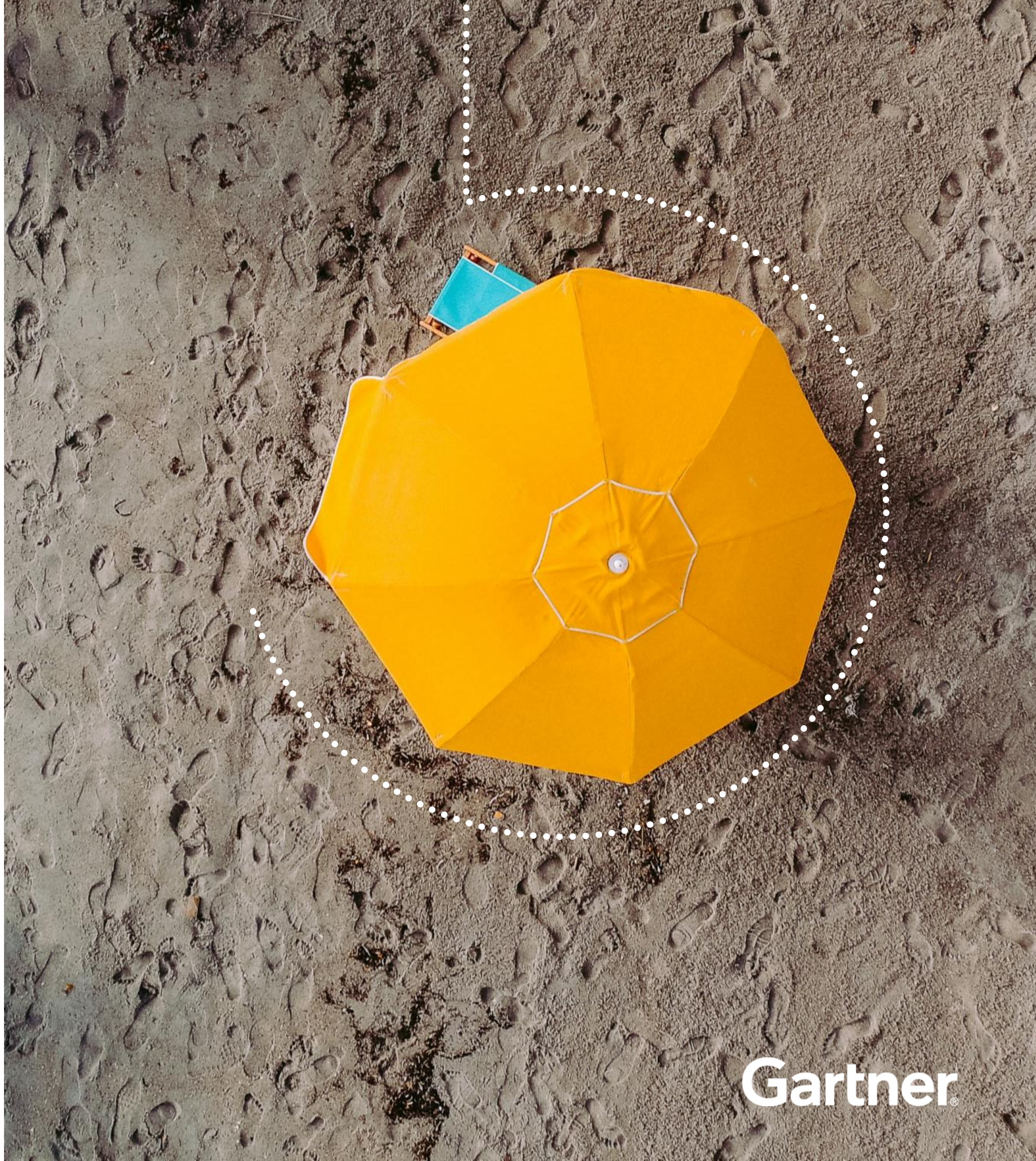
Chris Silva

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."

By 2026, the number of large enterprises will have matured and measurable zero trust program will grow 10X.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Currently, less than 1% large organizations have a mature zero trust strategy.



© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

“Zero Trust” Is Often Used to Describe:

- **Security paradigm,** which leads to a …
- **Strategy,** which defines an …
- **Architecture** that defines a set of …
- **Technical implementations**

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Zero Trust Is Not …

A magic technology that prevents all attacks

A single product

A comprehensive approach to cybersecurity

Then, what is it and why should we care about zero trust?

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

What Outcomes Can You Expect From a Zero Trust Strategy?

Replace implicit trust with dynamic access

Replaces implicit trust with explicit trust.

Support modern working environments

Flexibility to apply access rights tied to users and devices rather than network location.

Better protect data

Control unauthorized access of sensitive data and adjust controls to user and device context.

Zero trust can reduce exposure by optimizing an organization’s risk posture

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner’s definition of “zero trust”

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.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Integrating Endpoints to a Zero Trust Strategy

- A secure endpoint is the “key” to the integration.
- Actively securing endpoints is possible.
- Building active endpoint security will require multiple tools.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

How Do We Get There?

1. Attack surface reduction
2. Resilience against credential threats
3. Protecting the dynamic work environment

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

How Do We Get There?

1. Attack surface reduction
2. Resilience against credential threats
3. Protecting the dynamic work environment

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Attack Surface

Endpoints are more vulnerable in remote working environments and become a larger attack surface.

Through 2028, more than 60% of security incidents will be traced to misconfigured security controls.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Technology & Tools to Reduce Attack Surface

- Harden the endpoint using built-in security capabilities of the operating system.
- Implement host-based firewalls and strong device controls along with a UEM tool.

Use a balanced approach

Example:

Protection: AV/NGAV for known and behavior-based attacks

Prevention: app control to lock down system to protect against zero-day malware and untrusted applications

Perform continuous monitoring using endpoint detection & response (EDR)

Deploying technology in silos doesn't implement Zero Trust

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

One Size Does Not Fit All

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Steps to Reduce Your Attack Surface

- **Assess current state,** prepare inventory list of applications, users and their access on the endpoints.
- Allow **only approved applications** and limit execution of known good behaviour of approved applications on the endpoints.
- **Implement device control,** host-based firewall and utilize built-in OS hardening features.
- **Reduce legacy systems,** and identify misconfiguration of security tool and correct it.
- Perform **continuous monitoring** of the endpoints.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

How Do We Get There?

1. Attack surface reduction
2. Resilience against credential threats
3. Protecting the dynamic work environment

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Credential Threat

Credential misuse is now one of the primary attack vectors.

Over 50% of all breaches use stolen credentials.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Technology and Tools for Resilience Against Credential Threat

Multifactor authentication

Identity threat detection & response (ITDR)

Correlate adaptive signals

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Steps to Creating Resilience Against Credential Threat

- **Remove local admin access** on endpoints.
- **Apply least-privilege access** on the endpoints.
- Implement **MFA** and Identity Threat Detection & Response (ITDR).
- Integrate the MFA, and **ITDR** tools with your **EDR** tool.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

How Do We Get There?

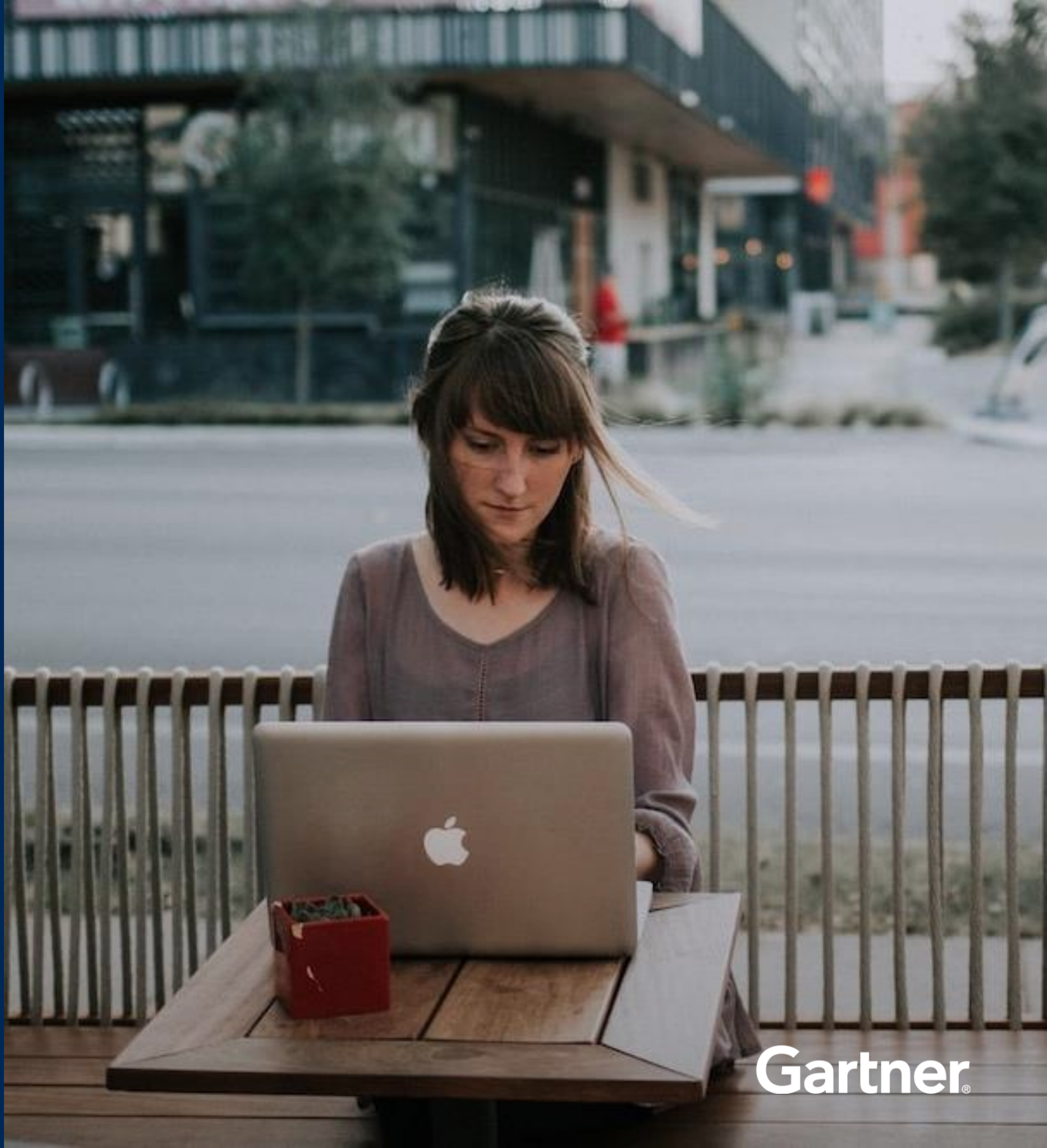
1. Attack surface reduction
2. Resilience against credential threats
3. Protecting the dynamic work environment

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Dynamic Work Environments

Can increase risk for an organization.

74% of all breaches include the human element.



© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Technology and Tools to Protect Dynamic Work Environments

SaaS-based UEM, identity and endpoint protection platforms

VDI, DaaS or an enterprise browser

Conditional access of resources on endpoints based on risk assessment

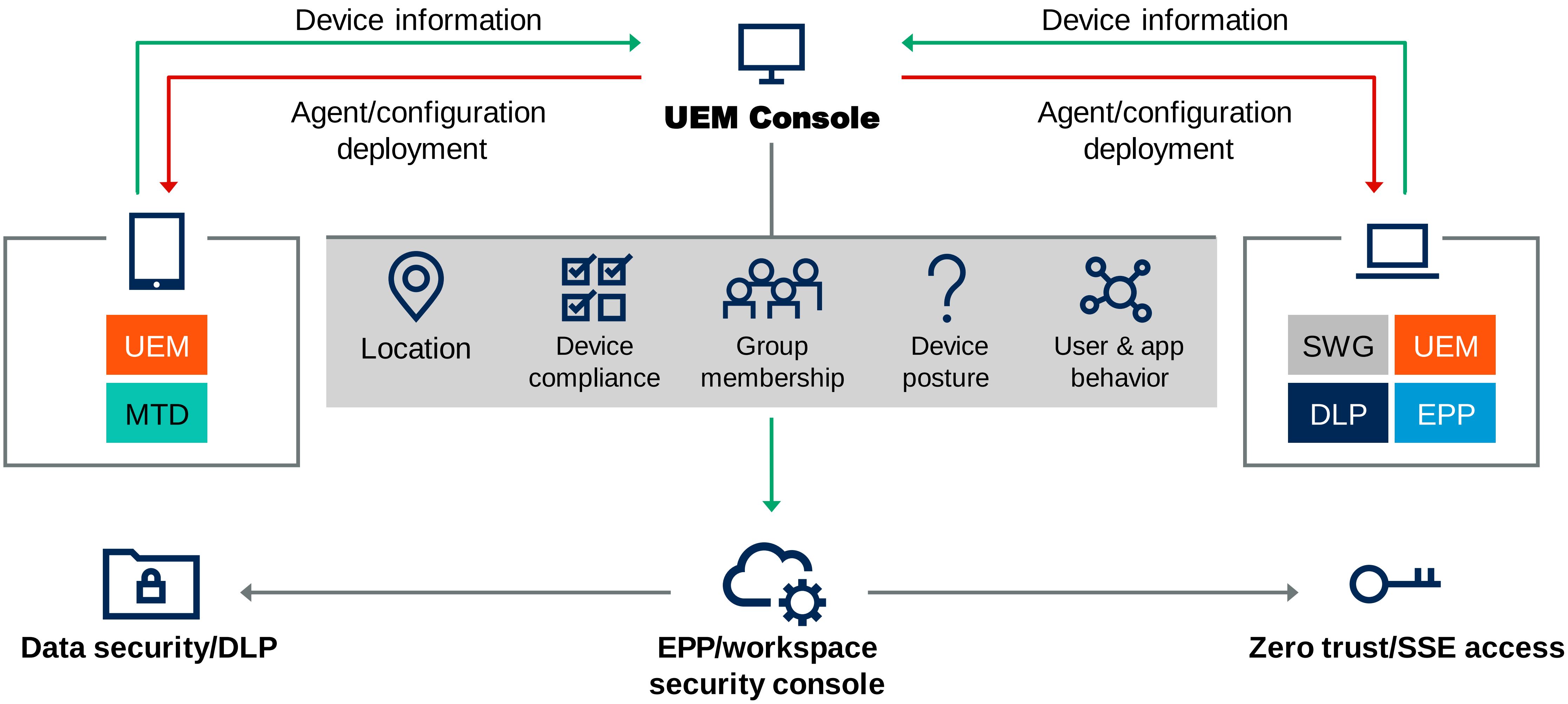
© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Steps to Protect Dynamic Work Environments

- Remove dependencies for devices having to be on the corporate network and **manage your endpoints, identities and endpoint security tools** via cloud platforms whenever possible.
- Utilize **conditional access policies** whenever possible.
- Restrict **access to resources** on unmanaged devices.

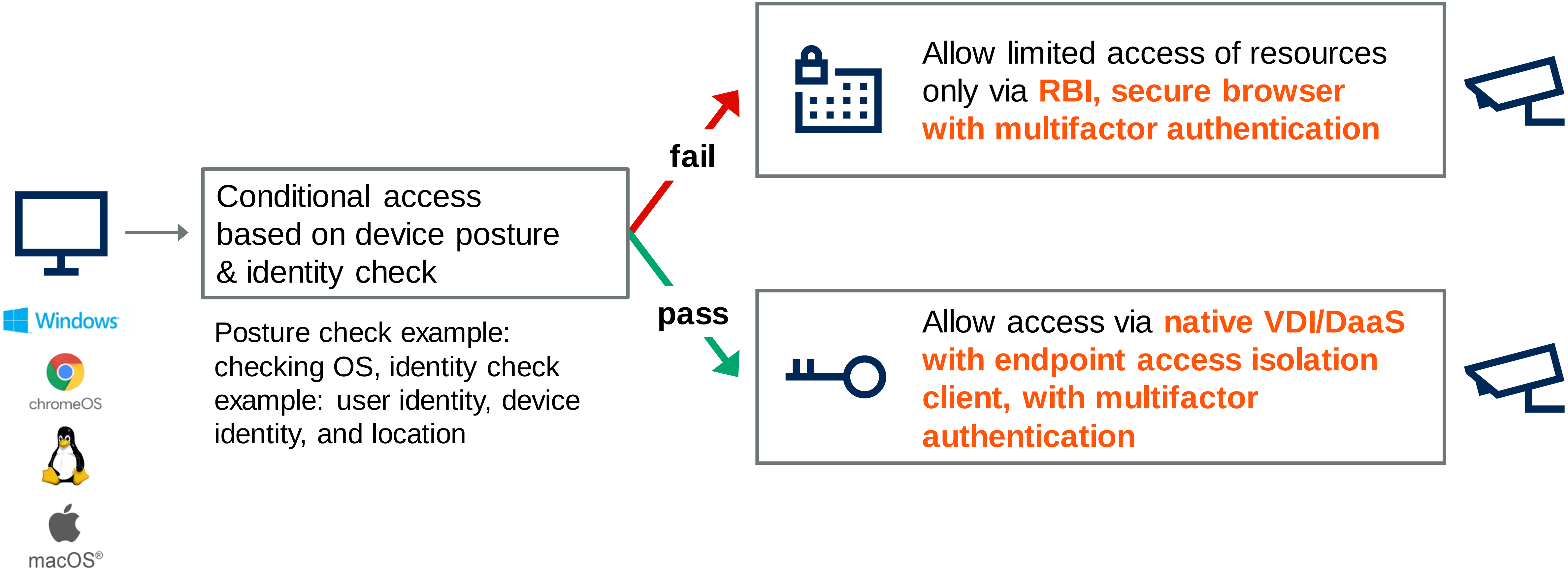
© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Workspace Security Integrates EPP/UEM/MTD



© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Zero Trust: Unmanaged Devices



Conditional access based on device posture & identity check

Posture check example: checking OS, identity check example: user identity, device identity, and location

fail

Allow limited access of resources only via **RBI, secure browser with multifactor authentication**

pass

Allow access via **native VDI/DaaS with endpoint access isolation client, with multifactor authentication**

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Zero Trust Is

A strategy founded on endpoint diversity

Dynamic endpoint policy that adapts

An iterative process

Many foundational investments exist but remain underutilized.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Recommendations

- ✓ Zero Trust strategies on endpoints **must include** both managed devices and unmanaged devices.
- ✓ Take advantage of your **existing endpoint security tools** fully **before** buying new tools for your zero trust implementation.
- ✓ **Integrate** endpoint security tools with identity, and network through SIEM or XDR to correlate the events to get **single source of truth** for proactive threat hunting.
- ✓ **Reduce legacy** infrastructure and combine zero trust with detection and response strategies to **reduce overall risk.**

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **How to Build a Zero-Trust Architecture**
  Thomas Lintemuth
- **Understanding the Capabilities of Modern Endpoint Protection Platforms**
  Eric Grenier
- **Emerging Tech: Security — The Future of Enterprise Browsers**
  Dan Ayoub, Evgeny Mirolyubov and Others
- **How to Improve Endpoint Security to Protect Organizations Against Advanced Cyberattacks**
  Satarupa Patnaik and Peter Firstbrook

Access to Gartner research is subject to individual subscription type and product entitlements.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.