FORTINET

# Zero Trust Network Access (ZTNA) Securely Connecting Users to Applications

Paulo Pinto
ppinto@fortinet.com

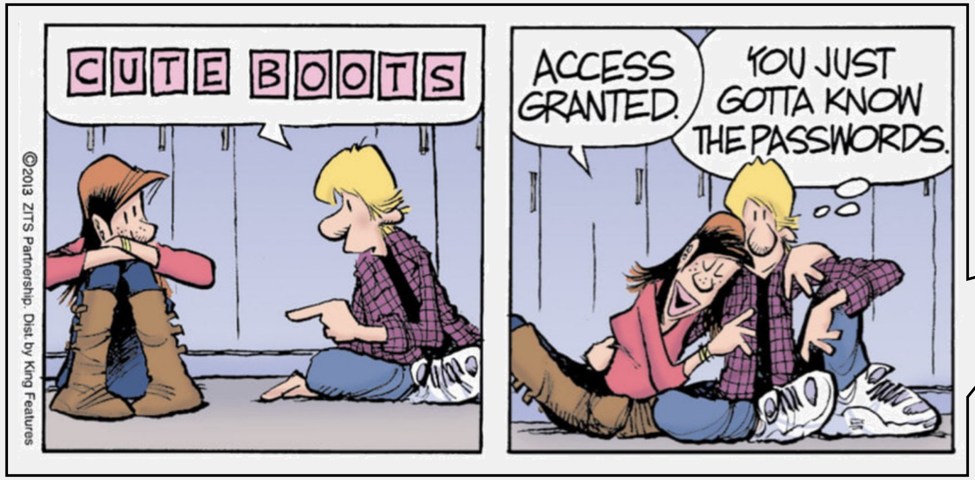
# It seems a little harder to get around in cyberspace

enter passcode
●●●●
CANCEL
SCOTT and BORGMAN

More six-digit authorization codes texted to your phone.

More requests to confirm the name of your first pet.

rockgod99
5/5


CUTE BOOTS
ACCESS GRANTED.
YOU JUST GOTTA KNOW THE PASSWORDS.
©2013 ZITS Partnership. Dist. by King Features

Overall, having to prove more often that you are you.

# It’s “ZERO TRUST” and it’s transforming networks globally

It’s a set of design principles and a cybersecurity strategy.

01

**Never trust, always verify**

Treat every user, device, application/workload, and data flow as untrusted.

Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.

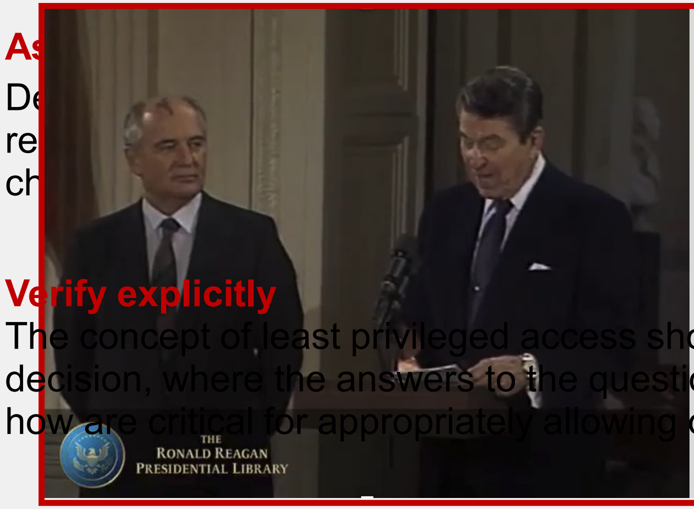
02

**As**

De

re tion

ch



**“TRUST but VERIFY”**

It was first used in the text of nuclear disarmament during the Cold War era by **Ronald Reagan** when talking with **Mikhail Gorbatchov** in **1987**.

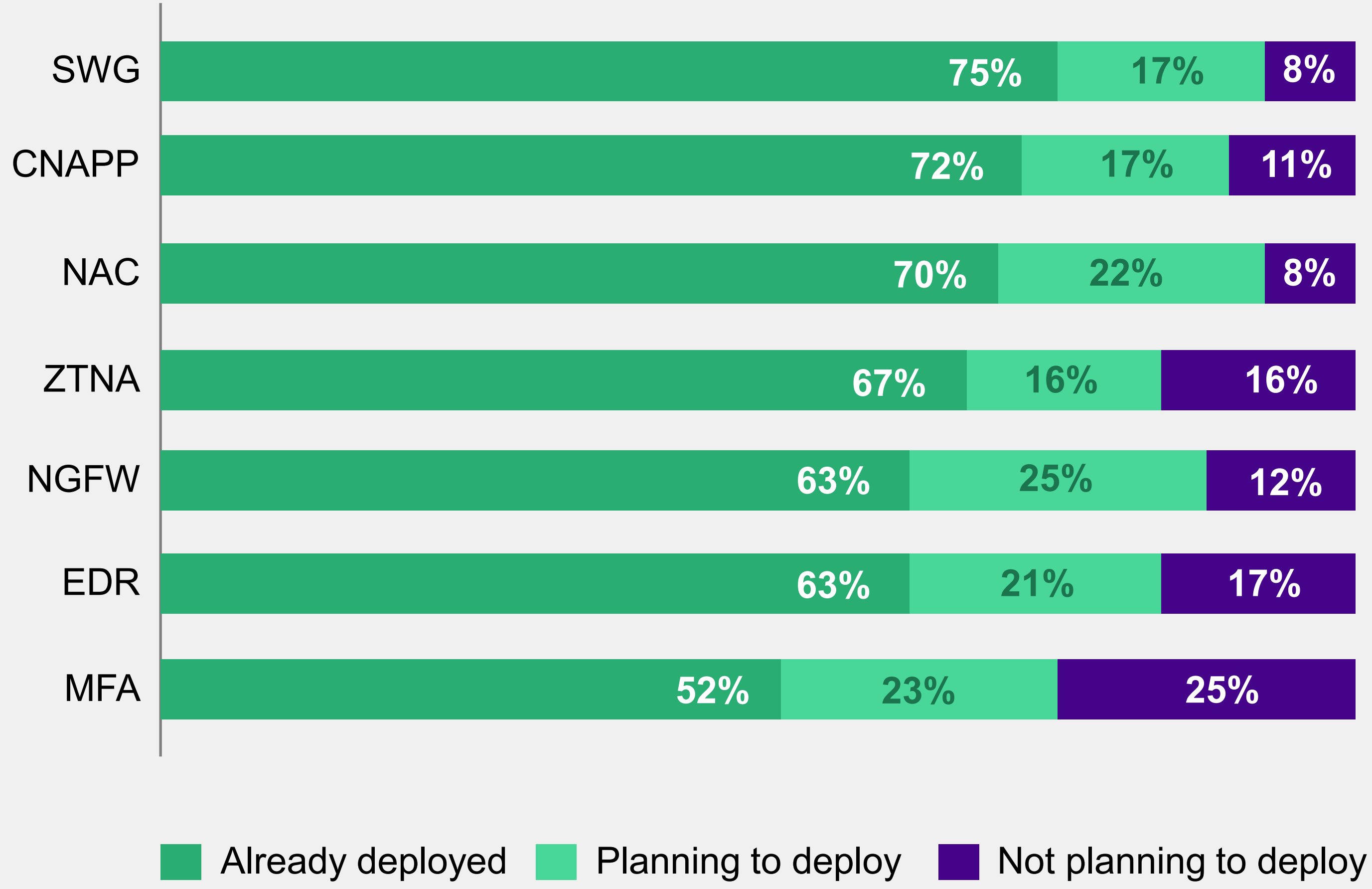
03

**Verify explicitly**

The concept of least privileged access should be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources.

# Technologies as part of zero-trust strategy

2023, “Report: The State of Zero Trust”, Fortinet

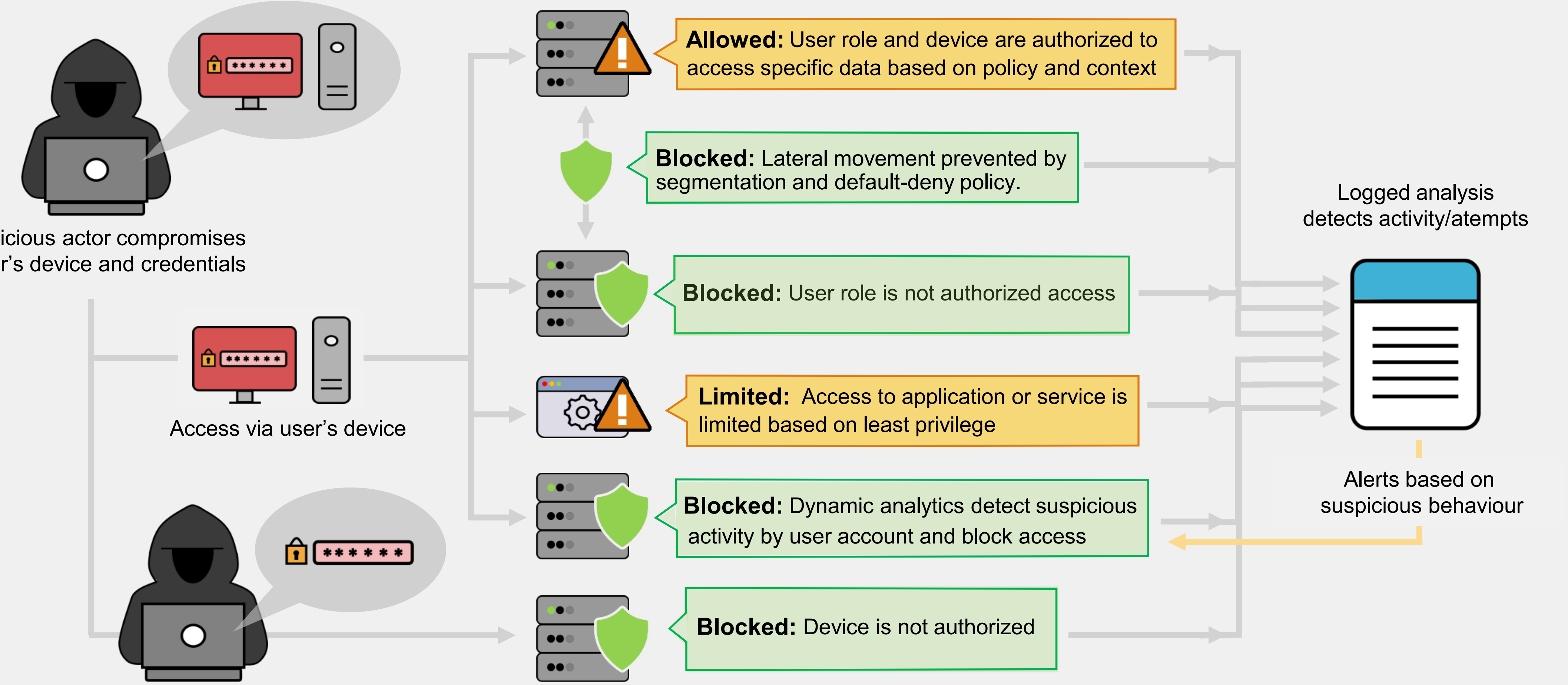


# How far can a malicious actor go?

ACCESS METHOD

ACCESS ATTEMPTS

ACCESS VISIBILITY



Malicious actor compromises user’s device and credentials

Access via user’s device

Access via malicious actor’s device using user’s stolen credentials

**Allowed:** User role and device are authorized to access specific data based on policy and context

**Blocked:** Lateral movement prevented by segmentation and default-deny policy.

**Blocked:** User role is not authorized access

**Limited:** Access to application or service is limited based on least privilege

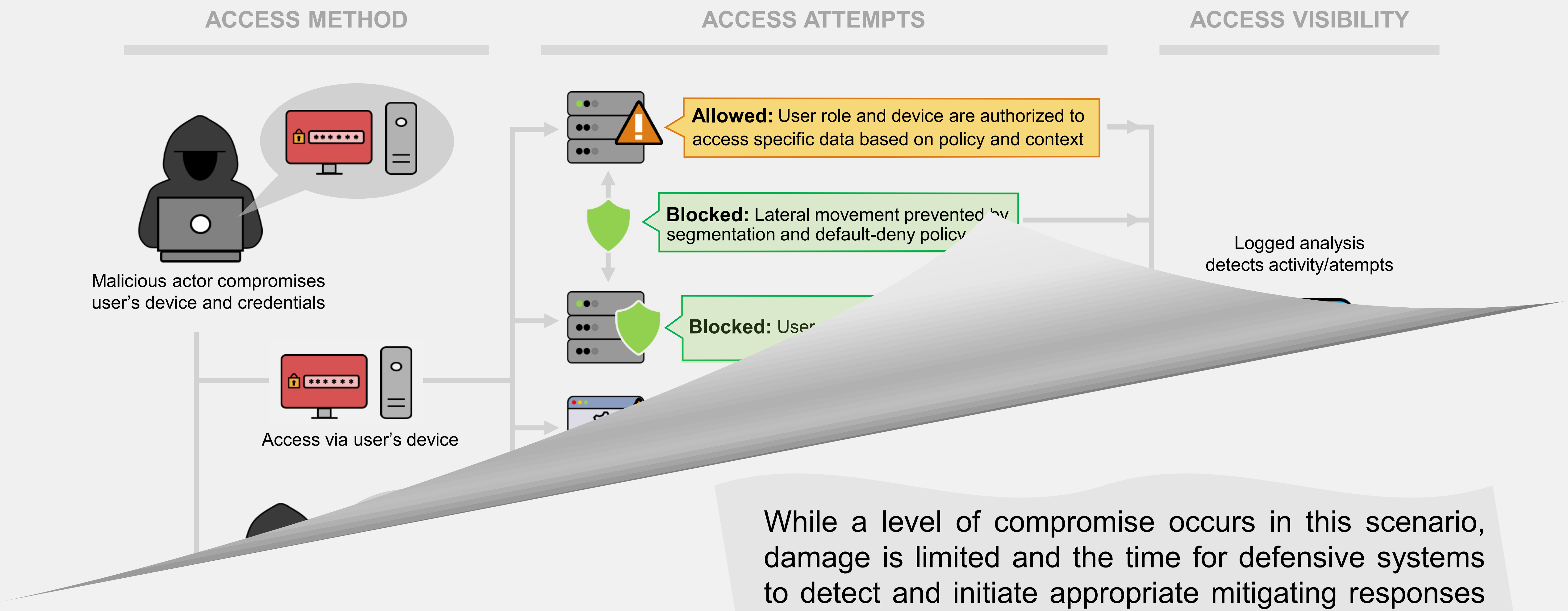
**Blocked:** Dynamic analytics detect suspicious activity by user account and block access

**Blocked:** Device is not authorized

Logged analysis detects activity/atempts

Alerts based on suspicious behaviour

# How far can a malicious actor go?



ACCESS METHOD

ACCESS ATTEMPTS

ACCESS VISIBILITY

Malicious actor compromises user’s device and credentials

Access via user’s device

**Allowed:** User role and device are authorized to access specific data based on policy and context

**Blocked:** Lateral movement prevented by segmentation and default-deny policy

**Blocked:** User

Logged analysis detects activity/atempts

While a level of compromise occurs in this scenario, damage is limited and the time for defensive systems to detect and initiate appropriate mitigating responses is greatly reduced.

# How to implement a zero-trust strategy

## Define the Attack Surface

Defining your attack surface should be the first item on your zero trust checklist.

[application access?; remote access?]

## Create a Zero-Trust Policy

This involves asking who, what, when, where, why, and how for every user, device, and network that wants to gain access.

## Architect a Zero-Trust Network

A zero trust network is designed around your specific protect surface—there is never a one-size-fits-all solution. Decide which network controls to implement and where to position them.

## Monitor your Network

Monitoring activity on your network can alert you to potential issues sooner and provide valuable insights for respond and optimizing security.

# Key takeaways

The shift to cloud computing and decentralized work immediately led to an uptick in cybercrime. Security methods have had to move quickly to modernize.

The zero-trust cybersecurity strategy is transforming global networks. These networks, sites, or applications won't allow you in (or let you stay) without proof you belong there, and they monitor for unexpected behavior. Your organization shall do it also.

More than three-quarters of global organizations are now taking a more aggressive approach to cybersecurity. About 40% have adopted a zero-trust model, moving security focus to the internet access.

FORTINET®