# Trust No One

## Pipelines as Critical Infrastructure in Zero Trust Architectures

# Agenda

1. Introduction
2. Overview of Zero Trust
3. Why Any of This Matters
4. CI/CD Implied Trust
5. Thank you + Q&A

# Introduction


Mike Lanciano

CTO, Systems and Data

- Software Engineer turned Platform Engineer
- Data Scientist on Weekends
- Start-Up to 50,000 person companies including Fortune 100/500
- Banking/Finance, Energy, Higher Education, Healthcare, Defense/Intelligence

# Core Concepts vs. Dogma

Much like DevOps, there are foundational tenets to  Zero Trust Architecture. Implementations may vary, but it’s important we don’t gatekeep especially given the prevalence of threats the current cyber era.

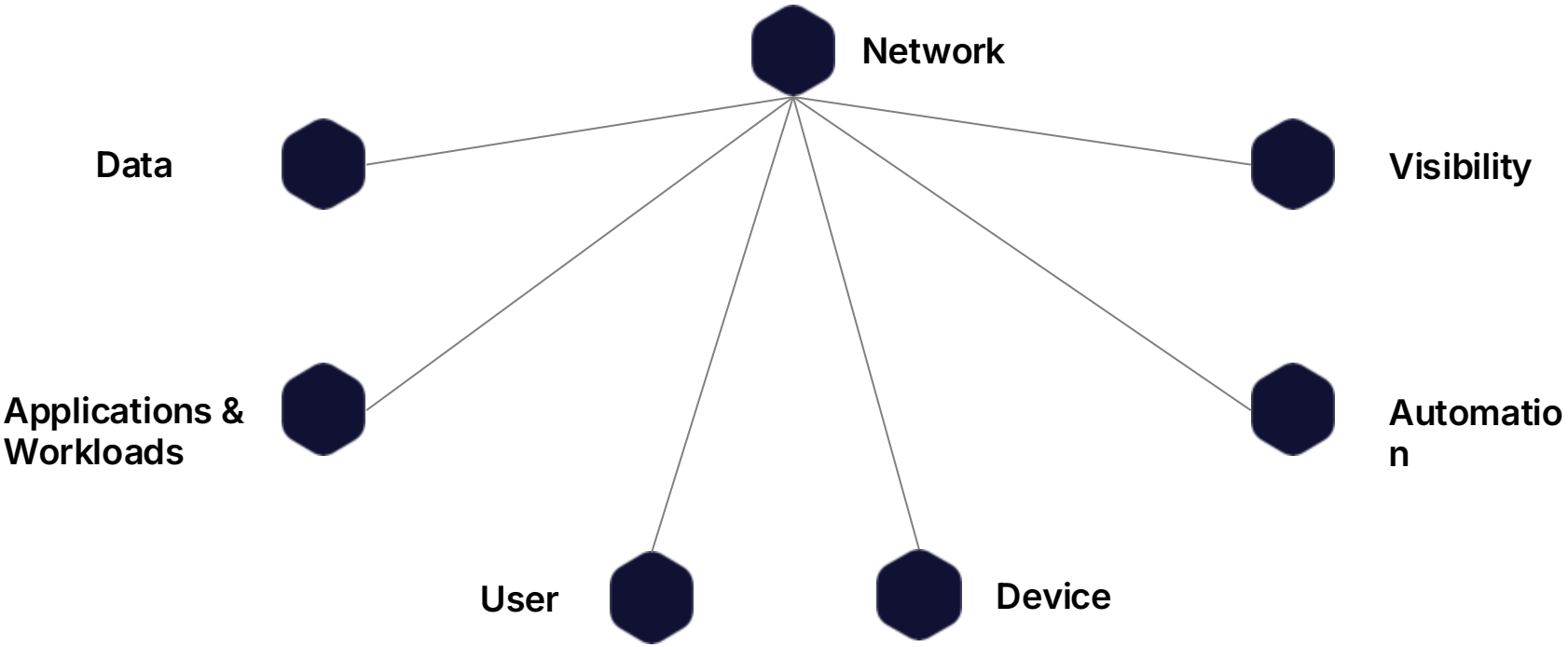

The core concept is there is no **implicit** trust based on a boundary. To take your organization on a zero trust journey means every component of your architecture becomes a contextual part of access and the organization continually works to remove implied trust.

# A Parallel to DevOps


**If at its core, DevOps is the full contextualization of development and operations as a cohesive organizational backdrop....**


**...Zero Trust is similarly the full contextualization of identity and access as a cohesive organizational strategy to remove implicit trust**

# Standard Implied Trust



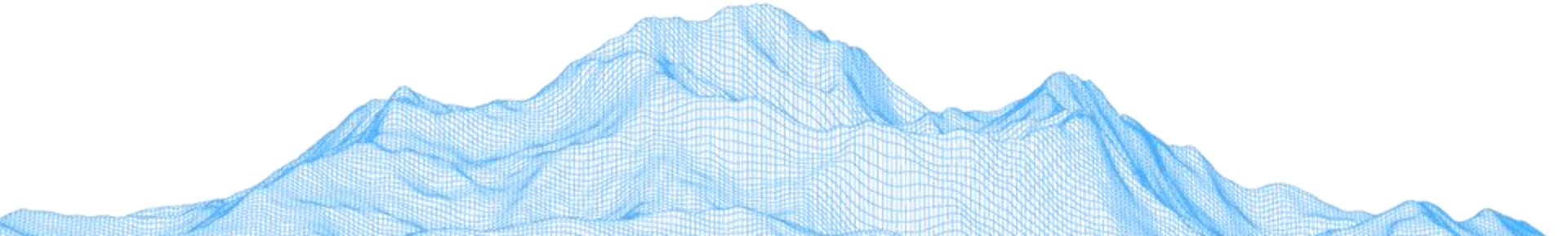
# Individualized Context

**Network Engineers** consider trust in terms of **segmentation and policy enforcement points**

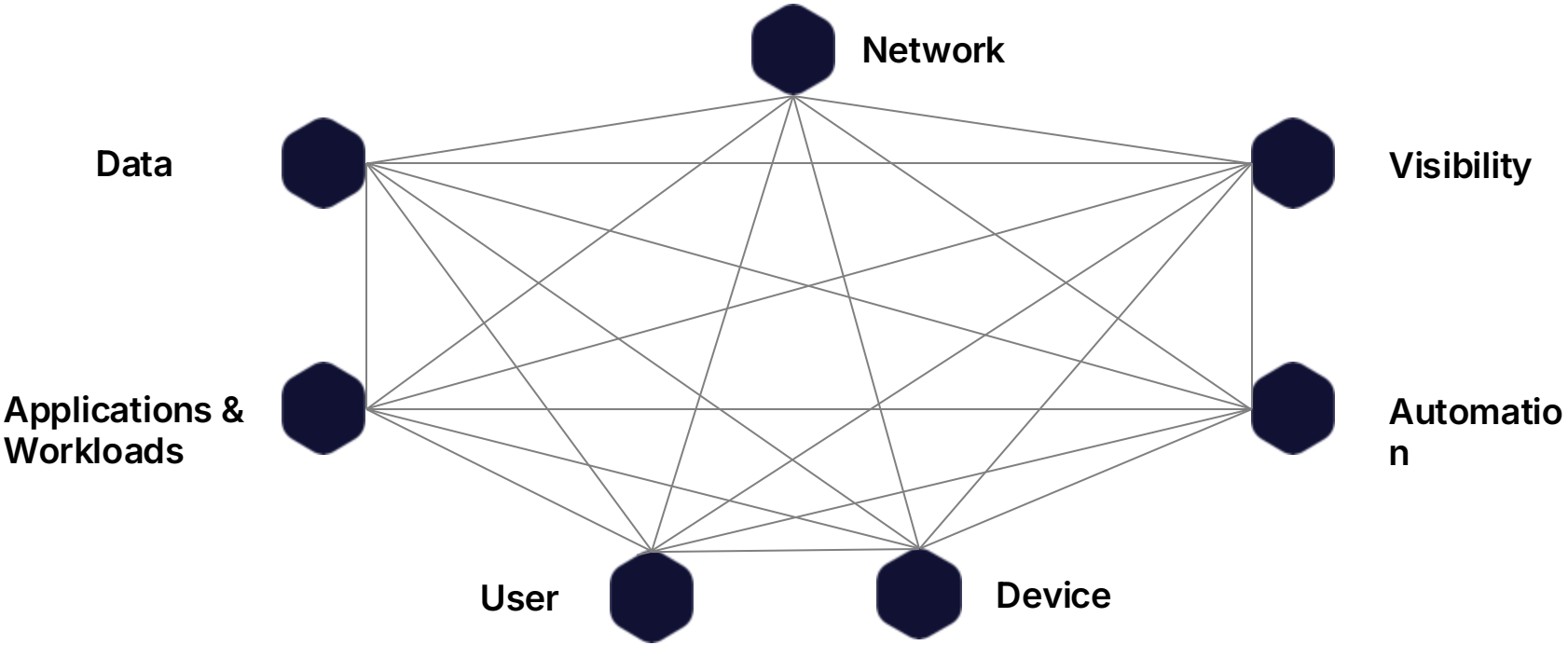
**Device Managers** consider trust in terms of **endpoint management**

**Software Developers** consider trust in terms of **ABAC and RBAC**

**Data Engineers** consider trust in terms of **meta tagging**



# Fully Contextualized Zero Trust Strategy

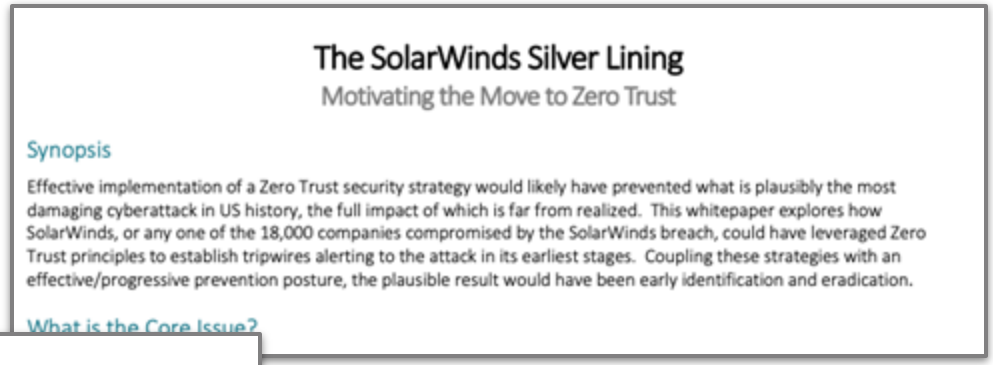


# So why does this even matter?

The changing landscape of mobility is driving considerable challenges in this boundary. Implied trust based on **location**, **network**, and **device** are all challenged in the multi-domain operations leading to bigger problems for the cybersecurity.

# Still not hearing the “So What” for DevOps?

Pipelines are continually targeted….



The SolarWinds Silver Lining

Motivating the Move to Zero Trust

Synopsis

Effective implementation of a Zero Trust security strategy would likely have prevented what is plausibly the most damaging cyberattack in US history, the full impact of which is far from realized. This whitepaper explores how SolarWinds, or any one of the 18,000 companies compromised by the SolarWinds breach, could have leveraged Zero Trust principles to establish tripwires alerting to the attack in its earliest stages. Coupling these strategies with an effective/progressive prevention posture, the plausible result would have been early identification and eradication.

What is the Core Issue?

malicious

/məˈlɪʃəs/

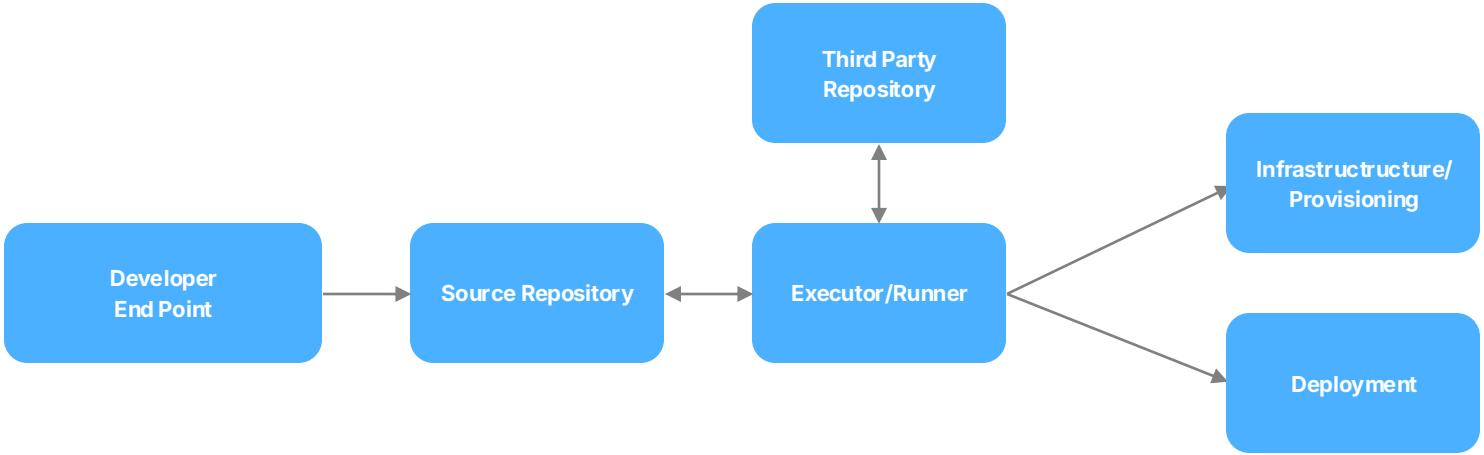
adjective

Malicious Software Supply Chain Attacks Increase Another 633% YoY

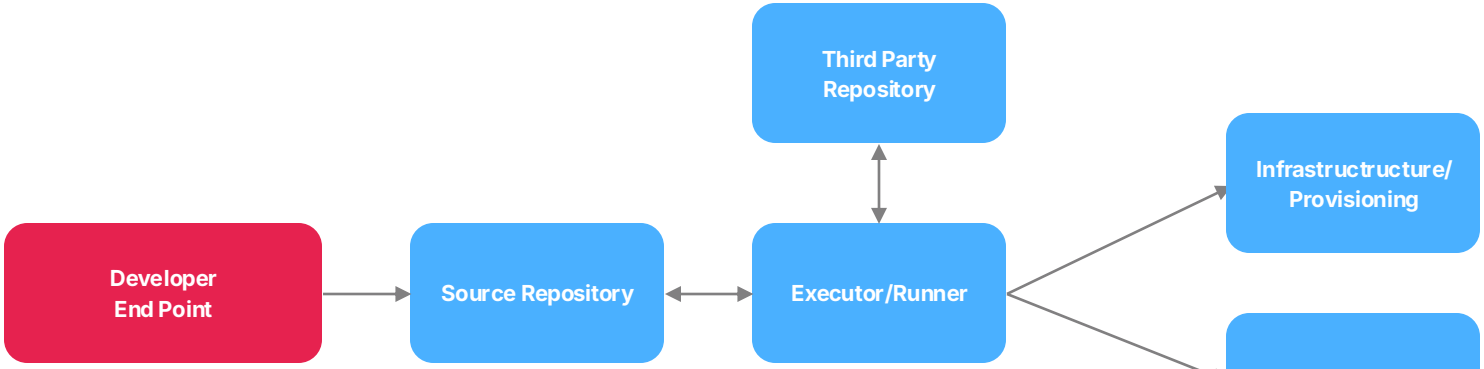
It's not just the new security vulnerabilities that companies must contend with day-to-day. The world's software development community must also deal with the ever-increasing threat from packages that are specifically designed to be malicious and present serious security threats from the onset.

…yet remain the most trusted parts of our infrastructure.

# A CI/CD Improvement Journey

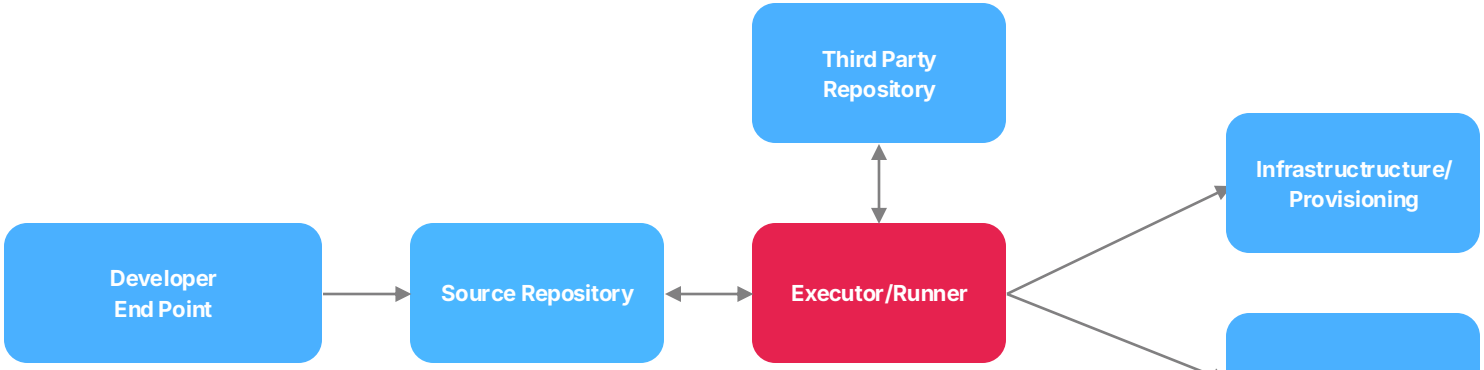


# A CI/CD Improvement Journey




- Username & Password
- Network

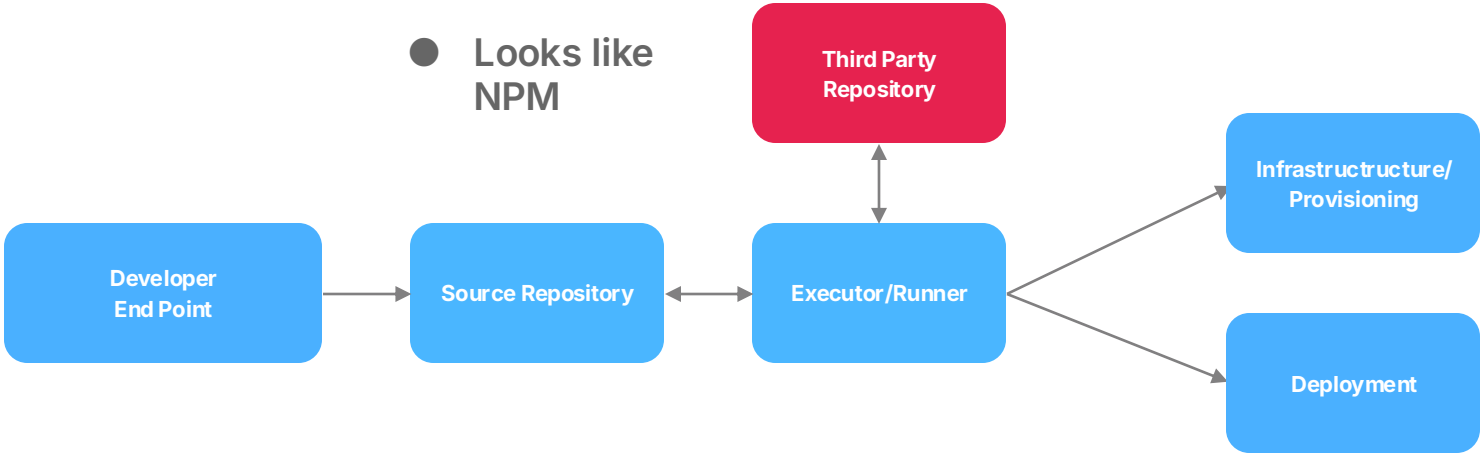
# A CI/CD Improvement Journey



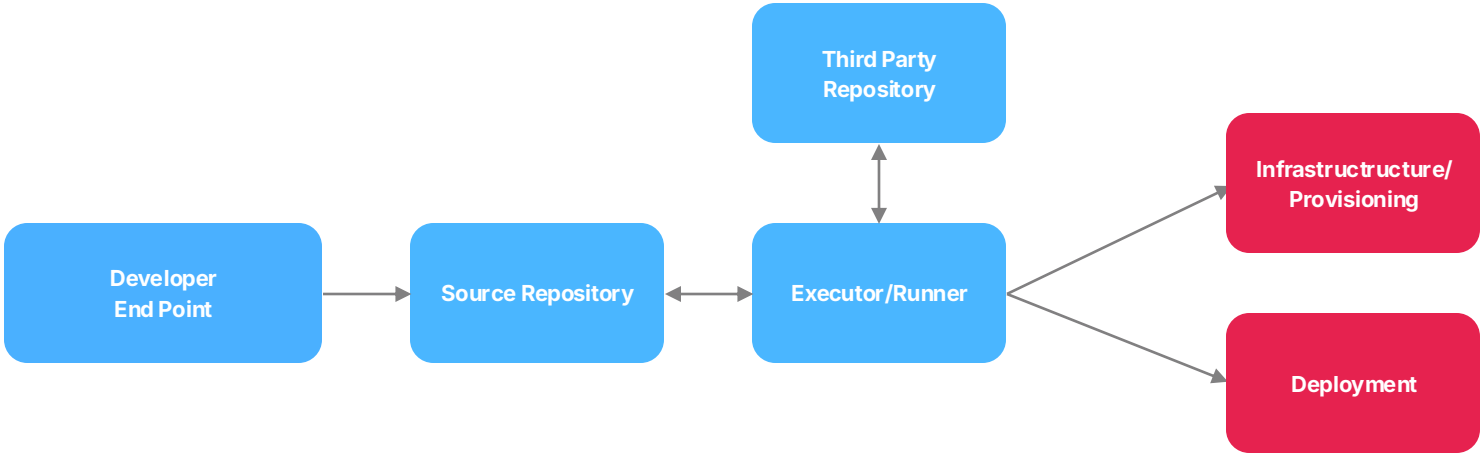

- Token Based Registration
- Executor Privilege

# A CI/CD Improvement Journey

- Looks like NPM



# A CI/CD Improvement Journey




- Access Keys

# Key Takeaways

- In the current cyber climate, Zero-Trust is critical for enabling us to work securely from anywhere.
- Zero-Trust is not a product solution.
- The ability to contextualize access and identity is complex and starts with strong ICAM infrastructure and policy.
- Our DevOps Infrastructure has a critical role in achieving true zero trust architectures.

# Thank you!

Questions

?