

Translating eBPF Into Business Value: Lessons From The Cilium Website



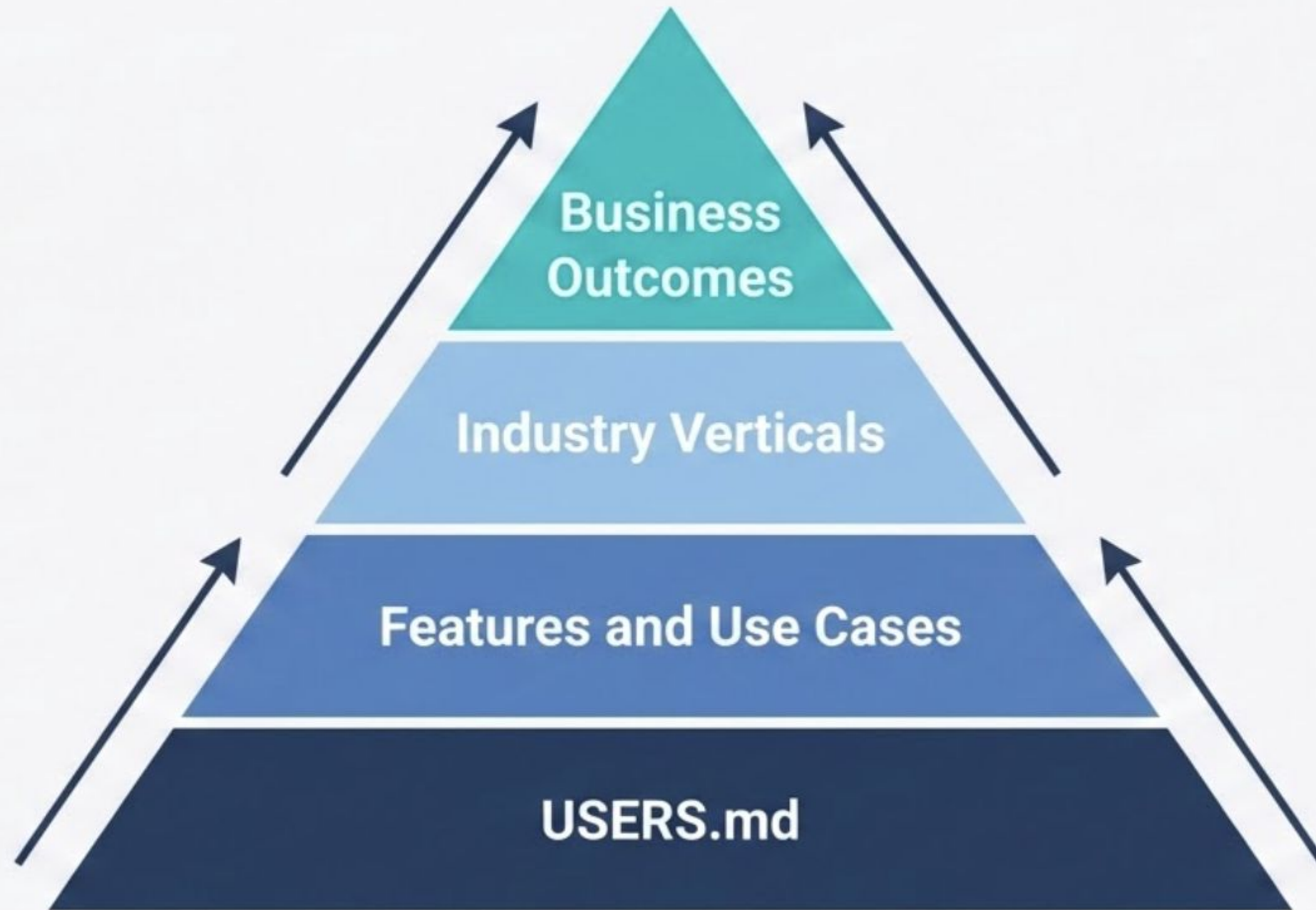
Bill Mulligan

KubeCon EU 2026

The Code vs Capital Disconnect



It All Starts with Users



Network Policy

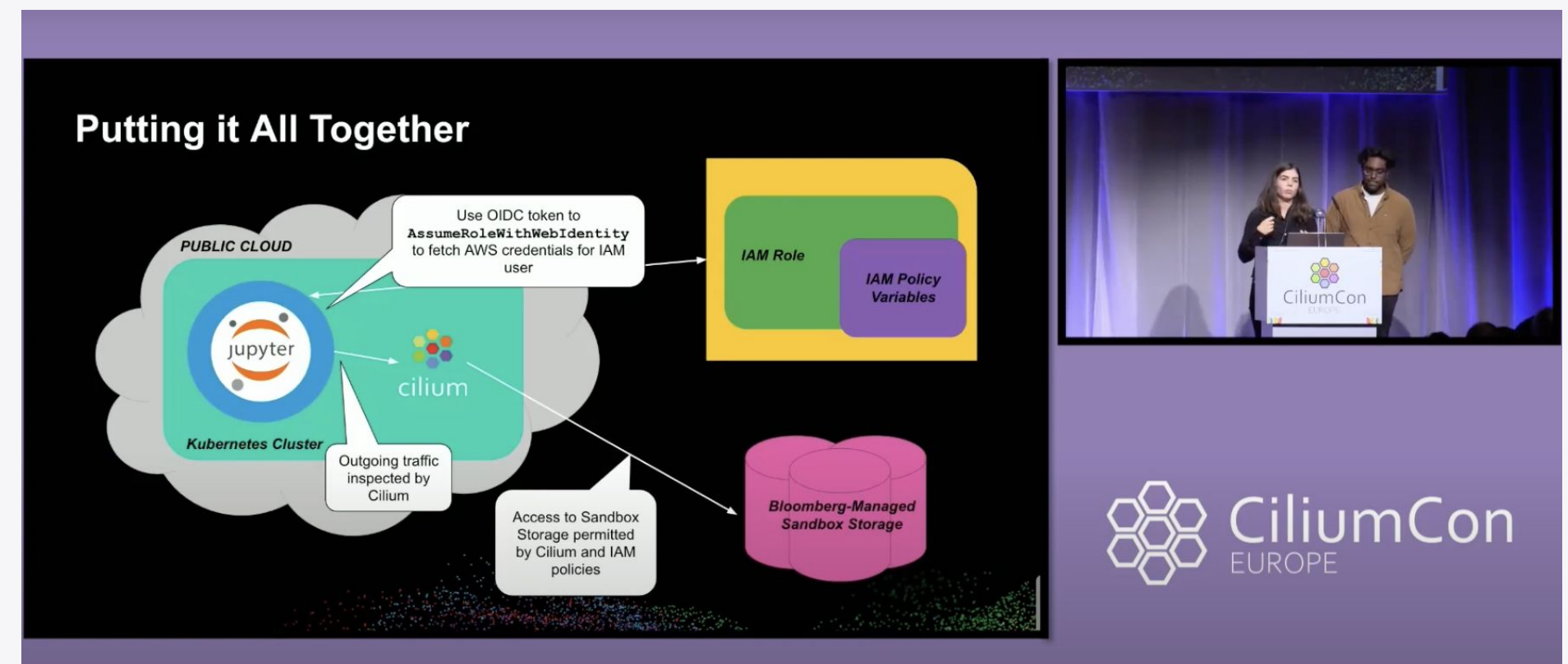
"We started by looking at some other tools, and we first used [the cloud provider CNI]. But we found that Cilium, **with its host-based policies** and its ability to replace what we had out of the box, **was really valuable.**"

Anne Zepecki

Team Lead for the BQuant Enterprise

Identity Management Team

Bloomberg



Financial Services

Bloomberg

Cilium's Solutions for Financial Services



Transparent Encryption

Elevate compliance and lower risk with Cilium transparent encryption. With just one switch, no application changes, service meshes or additional proxies

[LEARN MORE →](#)



Network Policy

Maintain identity based policies effectively at scale with Cilium's advanced network policies

[LEARN MORE →](#)



Egress Gateway

Present a group of cloud native workloads from a stable IP address to integrate with traditional firewalls

[LEARN MORE →](#)

S&P Global

PostFinance

Robinhood

Bloomberg

FORM3

证达通
ZENITERA

Qwist

Rabobank

Sicredi

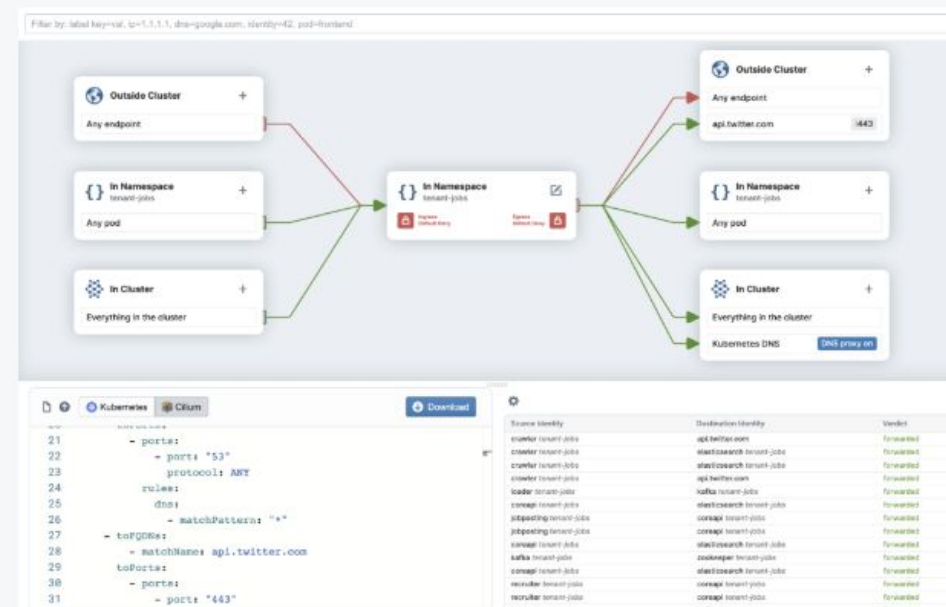
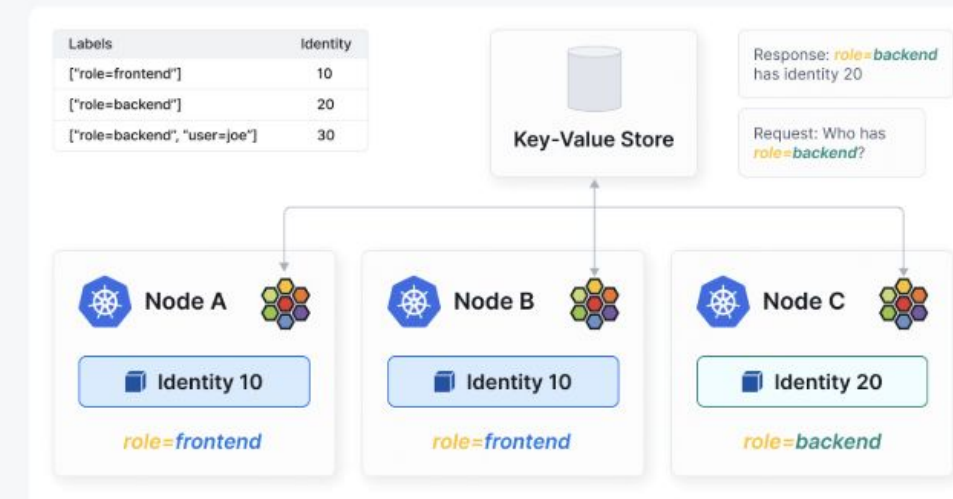
ISOVALENT
now part of CISCO

How Cilium scales Zero Trust Networking

Enforcing identity driven policies instead of IP-based rules

As workloads scale, restart, or move across nodes and clusters, IP addresses change constantly, creating gaps or needing constant rule updates.

Cilium solves this by applying security policies tied to Kubernetes-native identities like service accounts, pod labels, and namespaces. These identities stay consistent even as workloads shift or restart, so policies automatically follow the correct services wherever they run, removing the need to manage static network rules and ensuring reliable Zero Trust Networking enforcement at scale.



Implement policies in the kernel

Typically, enforcing Zero Trust Networking relies on proxies, sidecars, or userspace components to inspect and control traffic. These methods can make things more complicated to run, especially as systems scale.

Cilium takes a different approach by using eBPF to apply security policies directly in the Linux kernel. This allows high-performance enforcement at the source of the traffic without extra components in the data path. The result is fast, low-latency security that scales cleanly with your infrastructure.

Business Outcomes

"When it was time for us to build a more explicit data sandbox and storage solution, we found it was a lot easier to do because we already had Cilium running as our CNI. It worked out super nicely and also **unlocked the ability to offer additional features to our customers**, like data replication."

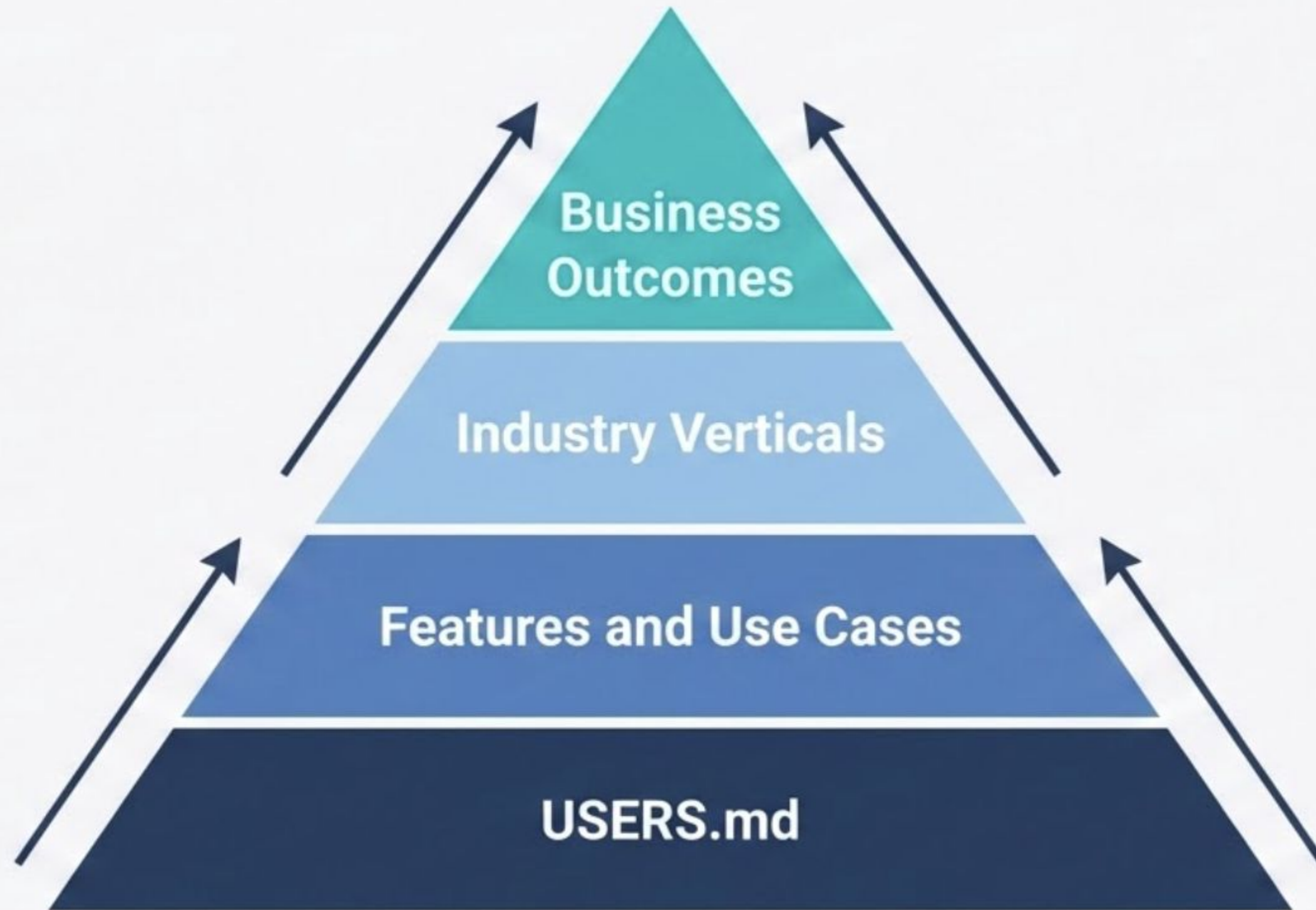
Anne Zepecki

Team Lead for the BQuant Enterprise

Identity Management Team

Bloomberg

It All Starts with Users



ISOVALENT
now part of cisco

Thank
you!

