TODAY'S ATTACKS DESERVE BETTER

Stop using yesterday's strategies

May 2023

Den Jones
Chief Security Officer Banyan
Security

A Practitioners Journey…

Den Jones

Director of Enterprise Security

Project ZEN
(2018)

*7 months
40k+ users
50k+ devices
1300+ applications*

Sr. Director of Enterprise Security

Zero Trust Initiative
(2020)

*5 months
100k+ users
100k+ devices
100+ applications*

Chief Security Officer

Zero Trust Evangelists

*Helping you achieve
zero trust remote access*

BANYAN SECURITY

AGENDA

Threat landscape

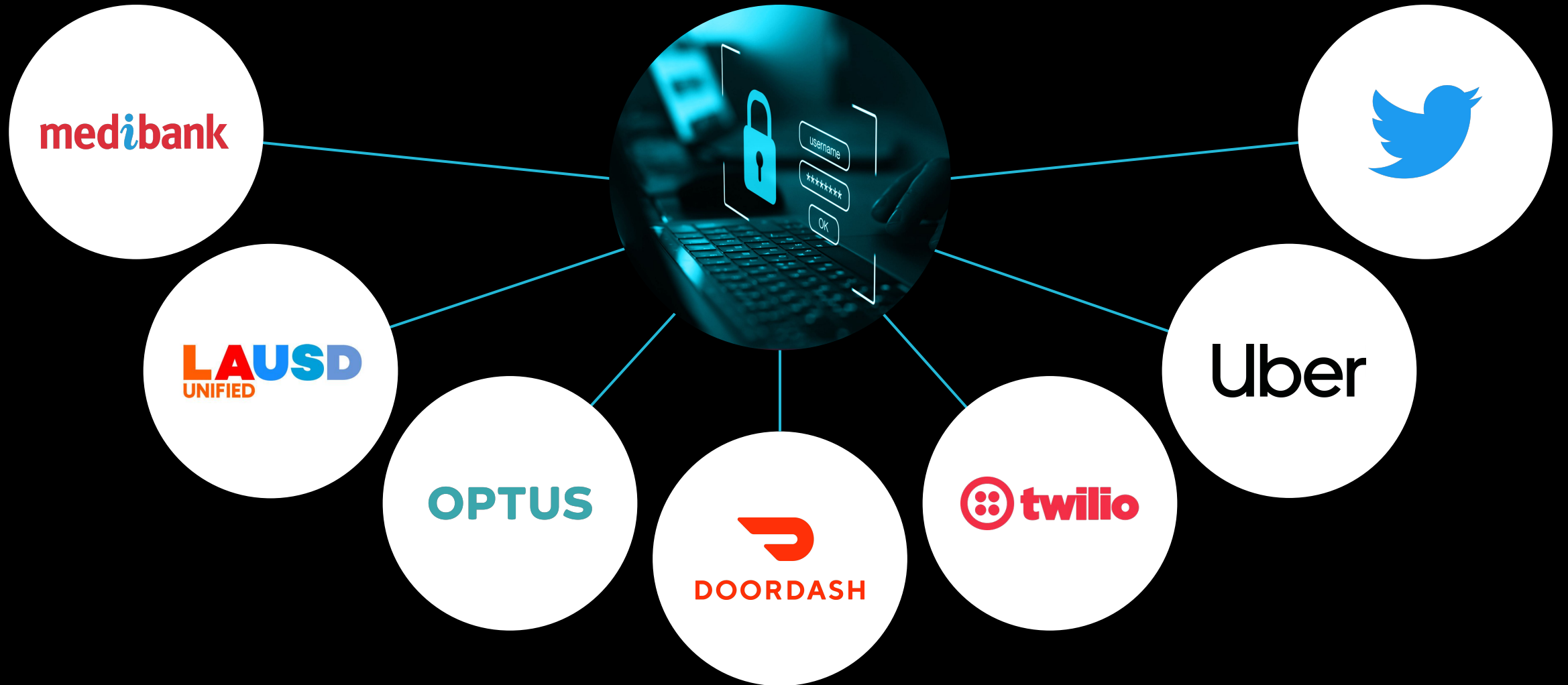Strategies that failed us

Strategies that work

Get IT Started & Get IT Done!

AGENDA

Threat landscape

We're all under attack!

BANYAN
SECURITY

Themes – Attack Vectors

Phishing, Smishing & Vishing

3rd Party (i.e., vendors & contractors)

Malicious Websites

Your Configurations

Product Vulnerabilities

BANYAN SECURITY

Themes – Outcomes

Credential Theft

Data Theft

Device Compromise

Privileged Access

Lateral Movement

Themes – Impact: CIA

Data Loss
(ransomware)

Company Brand
(reputation)

Data Leak

Service Outage
(customer impact)

System Outages
(company)
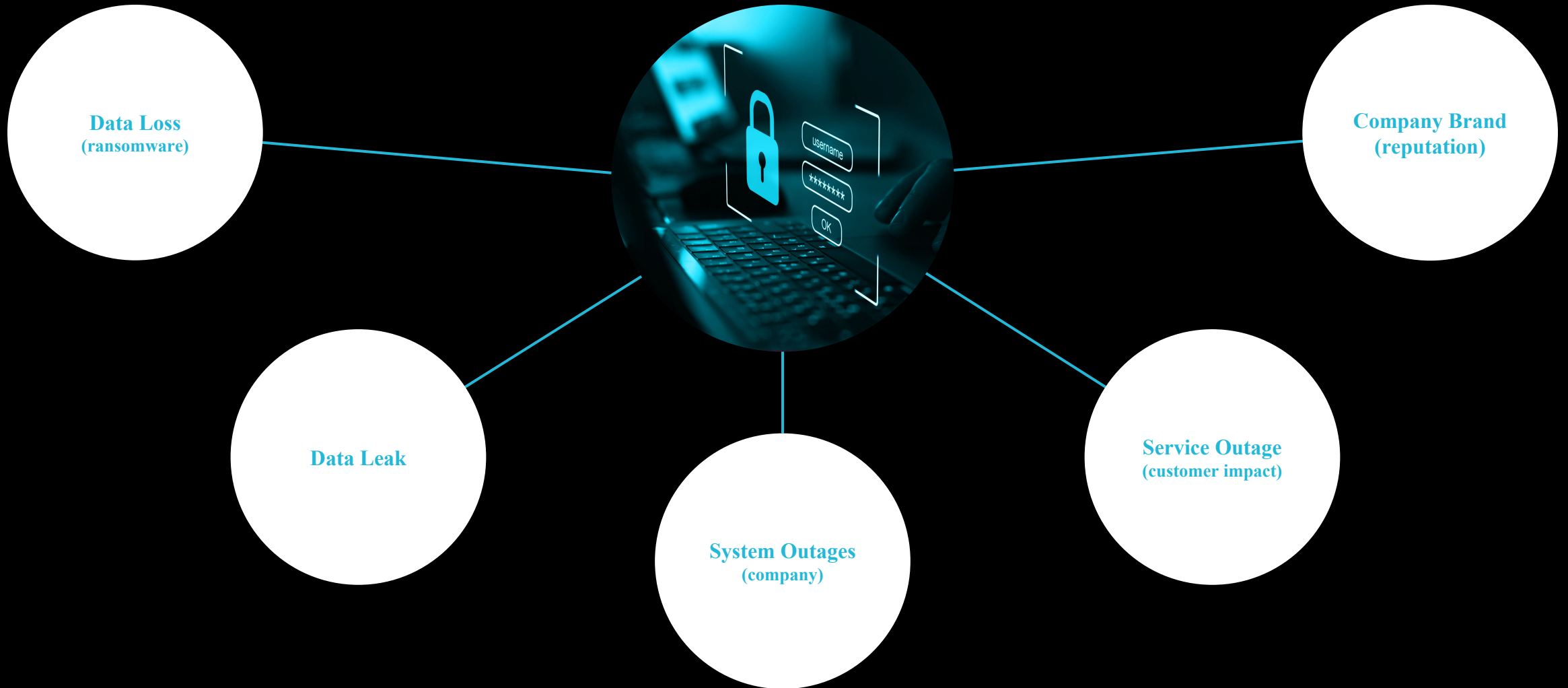
CIA: Confidentiality, Integrity & Availability

BANYAN
SECURITY

Themes – Impact: Cost

Data Loss
(ransomware)

Company Brand

The global average cost of a data breach in 2022 was $4.35 million according to IBM Security's "The Cost of a Data Breach Report"

Data Leak

Service Outage
(customer impact)

System Outages
(company)

BANYAN SECURITY

AGENDA

Strategies that failed us

Epic fail...or just too costly?

Security training

Social engineering is too good, employees are human

MFA

Passwords and MFA are no longer enough, fatigued yet?

Network Security

Costly and complex, users exist less on your network, choke points are flawed

Least Privileged?

So many of the attacks leverage access users needed to perform their role

AGENDA

Strategies that work

Defense in Depth

Still cover the basics: Least Privileged, Training, Network Security – but add some easy wizzbang!

That's what we did at Adobe and Cisco!

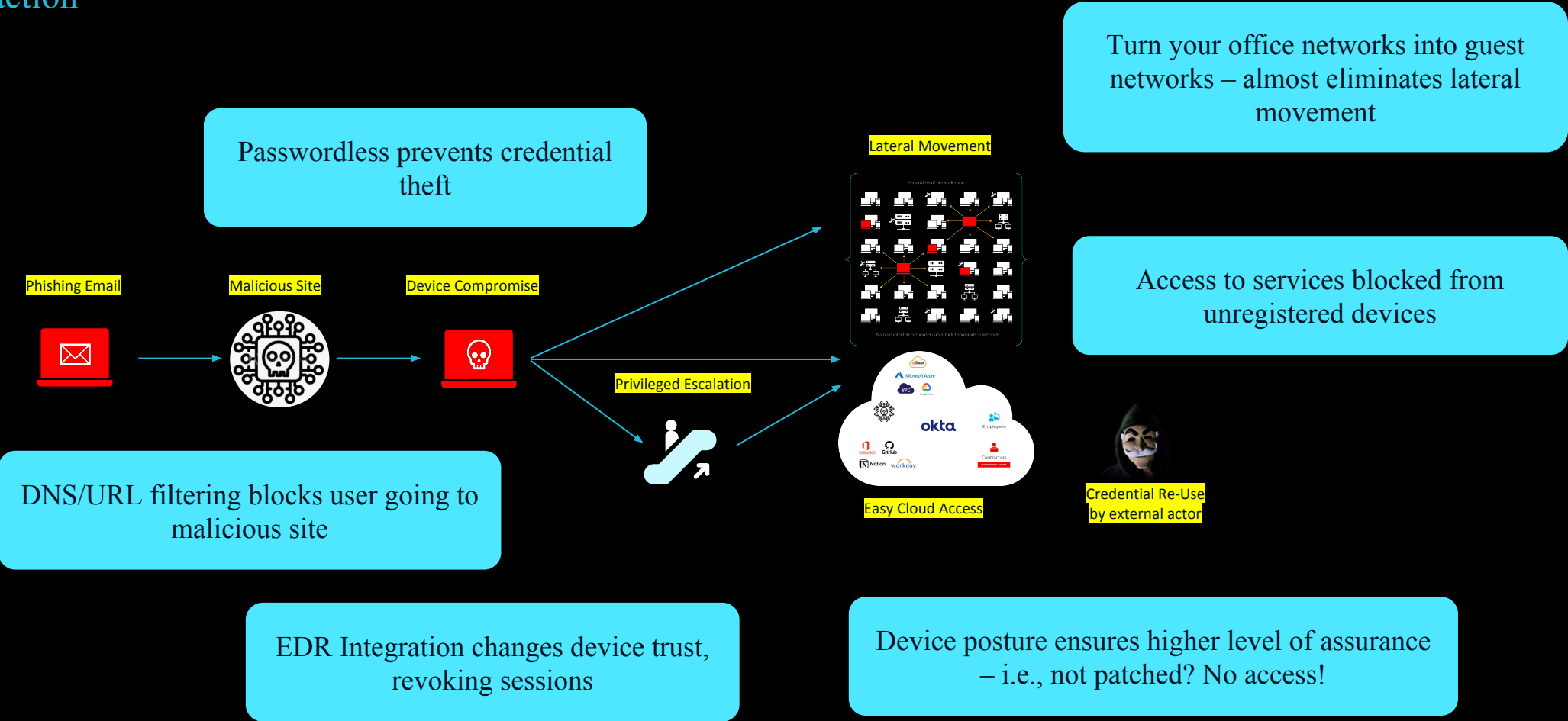|			
Replaced Passwords with Certificates		Established Security Intelligence	
Device Registration		Device Posture & Integrated Security	
No more VPN		Simplified User Experience	

BANYAN SECURITY

Defense in Depth

Example in action

Passwordless prevents credential theft

Turn your office networks into guest networks – almost eliminates lateral movement

Lateral Movement

Phishing Email

Malicious Site

Device Compromise

Privileged Escalation

Access to services blocked from unregistered devices

DNS/URL filtering blocks user going to malicious site

Easy Cloud Access

Credential Re-Use by external actor

EDR Integration changes device trust, revoking sessions

Device posture ensures higher level of assurance – i.e., not patched? No access!

BANYAN SECURITY

AGENDA

Get IT Started & Get IT Done!

Getting Started

Move to Passwordless

Devise your Strategy

Security Service Edge / ZTNA

**Move to Integrated Device Security**

**Gain Executive Support**

The People & Culture Journey

BANYAN SECURITY

Steps to Success

1   Sell the vision, people, process, and technology

2   Balance old strategies with new ones supporting a remote, modern workforce

3   Keep it simple, maximize your investments

4   Leverage existing investments

5   Start by integrating with your existing authentication platform

6   Short sprints and quick wins

BANYAN SECURITY
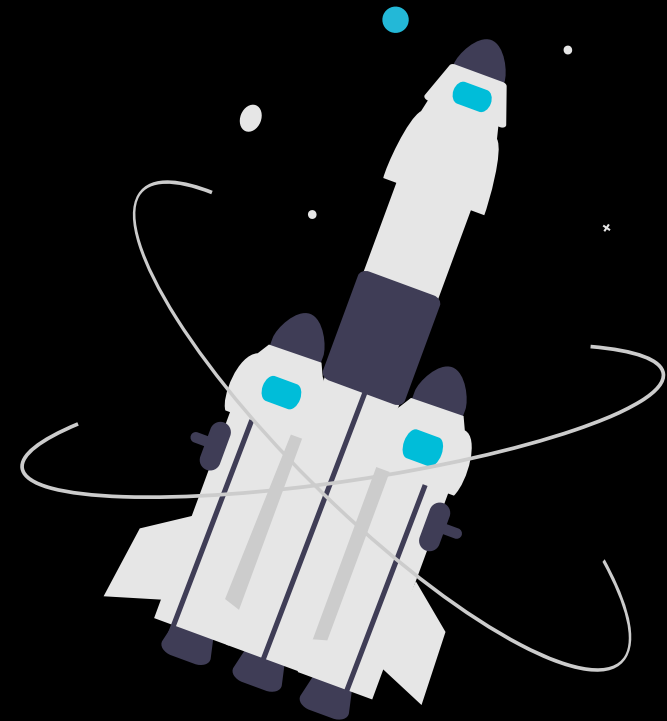
Things to Avoid

1 Confusing people with marketing terms

2 Thinking that a single vendor can do it all

3 Trying to sell a long-term program

4 Asking for trillions and billions

5 Forgetting the importance of education/communication

BANYAN SECURITY
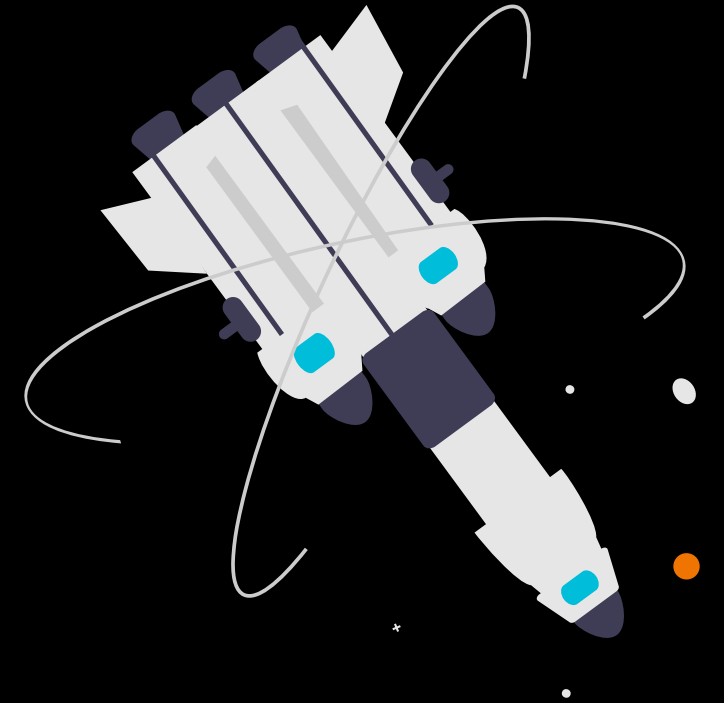
Lessons Learned

1 Your VPN team will not love your project

2 Network security purists will challenge you

3 MFA isn't enough, combine user and device identity

4 Complex network segmentation & VPN rules have failed us

5 It's easier than we thought to integrate device posture and security

BANYAN SECURITY

Shameless Commerce Slide

We work at Banyan Security

Banyan Security enables your Zero Trust and SSE journey

Want to get started today?

Visit the Banyan Website
www.banyansecurity.io

Request a Demo
www.banyansecurity.io/demo-request/

Get started with our free Team Edition
www.banyansecurity.io/team-edition-signup/

BANYAN SECURITY

World's **Easiest** Security Service Edge

Easiest to Deploy

- Cloud Command Center
- Guided Configurations
- Headless Connectors
- Discover and Publish
- Human-readable Policies
- Terraform Automation
- Seamless Integrations
- Incremental Deployments

Easiest to Use

- All-in-one SSE Client
- Zero-Touch Client Deployment
- Passwordless, One-click Access
- Service Catalog
- Automatic Service Tunnels
- IT-less Remediation
- Multi-organization Support
- Unmanaged Device Support

BANYAN SECURITY

Contact Me

@DenJonesCyber

/DenWJones

Den@BanyanSecurity.io

@DenJonesCyber@defcon.social

Book an Office Hour with Den

Get IT **Started.**
Get IT **Done.**

Hosted by

DEN **JONES**

Powered by

B **BANYAN**
SECURITY

Available on: amazon music | (Apple Podcasts) | (Google Podcasts) | RP | (Spotify) | | (RSS)

Thank you

Visit us at www.banyansecurity.io

BANYAN SECURITY

BANYAN SECURITY

Appendix

142 Minna Street, San Francisco, CA 94105
415-289-9414
info@banyansecurity.io

What did we deliver?

Improving security as we make it more of a background capability

- **Certificates replacing passwords**

- **No more broad internal network access from the internet**

- **Enforce device security posture & a path to SSE**

- **Ability to eliminate lateral movement**

BANYAN
SECURITY

What did we deliver?

Access internal applications and services without using legacy VPN

VPN

- **Publish applications and services to the internet**

- **Users don't connect to your network via VPN, exposing your internal network and thousands of devices**
- **Reducing cost of ownership, no IP tables to manage**

BANYAN
SECURITY

What did we deliver?

Improving Employee Experience: Happy employees are directly tied to profit
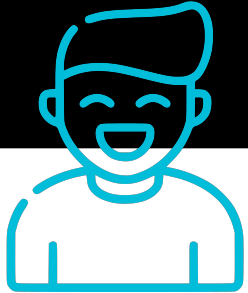
- **No more username and password during login**

- **No more 90-day password changes**

- **No logging into VPN or being confused when you need to**
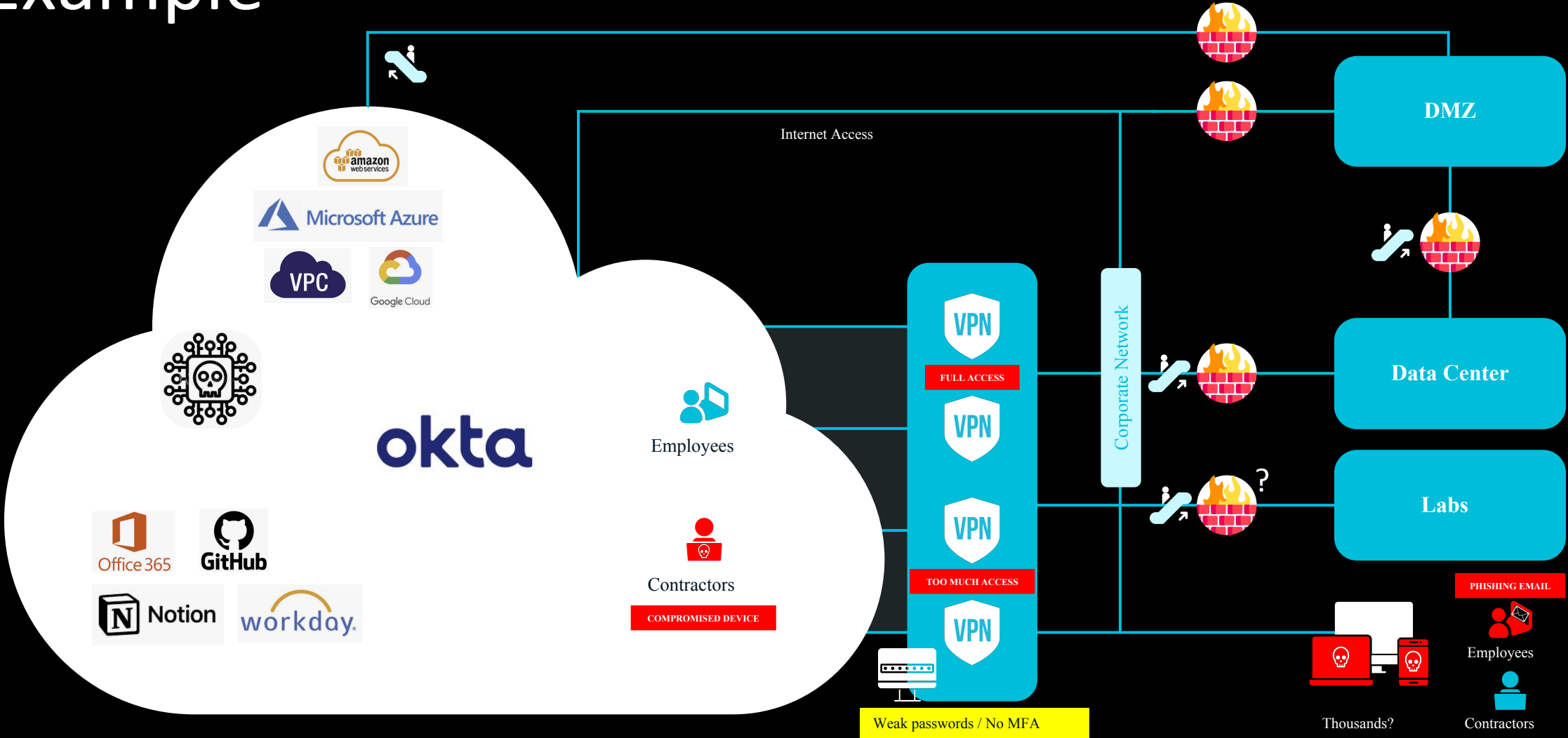
BANYAN
SECURITY

What did we deliver?

Enabling Business Strategies

- **Turn your office network into a guest network**

- **Seamless M&As**

- **Immediate modern remote workforce**

BANYAN SECURITY

Example

BANYAN SECURITY

Example

Regardless of network zone….

A single infected computer can attack thousands in seconds

DMZ

Data Center

Labs

Corporate Network

VPN — FULL ACCESS

VPN

VPN

VPN — TOO MUCH ACCESS

WHAT % ARE COMPROMISED?

PHISHING EMAIL

Thousands?

Employees

Contractors

BANYAN SECURITY