WEBINAR

Implementing a Zero Trust Architecture for Tribes

PRESENTED BY
Bill Travitz, Arctic IT
Brent Nix, Microsoft

October 20, 2022

ARCTIC IT Tenacious Ingenuity

Microsoft

TRIBALWISE

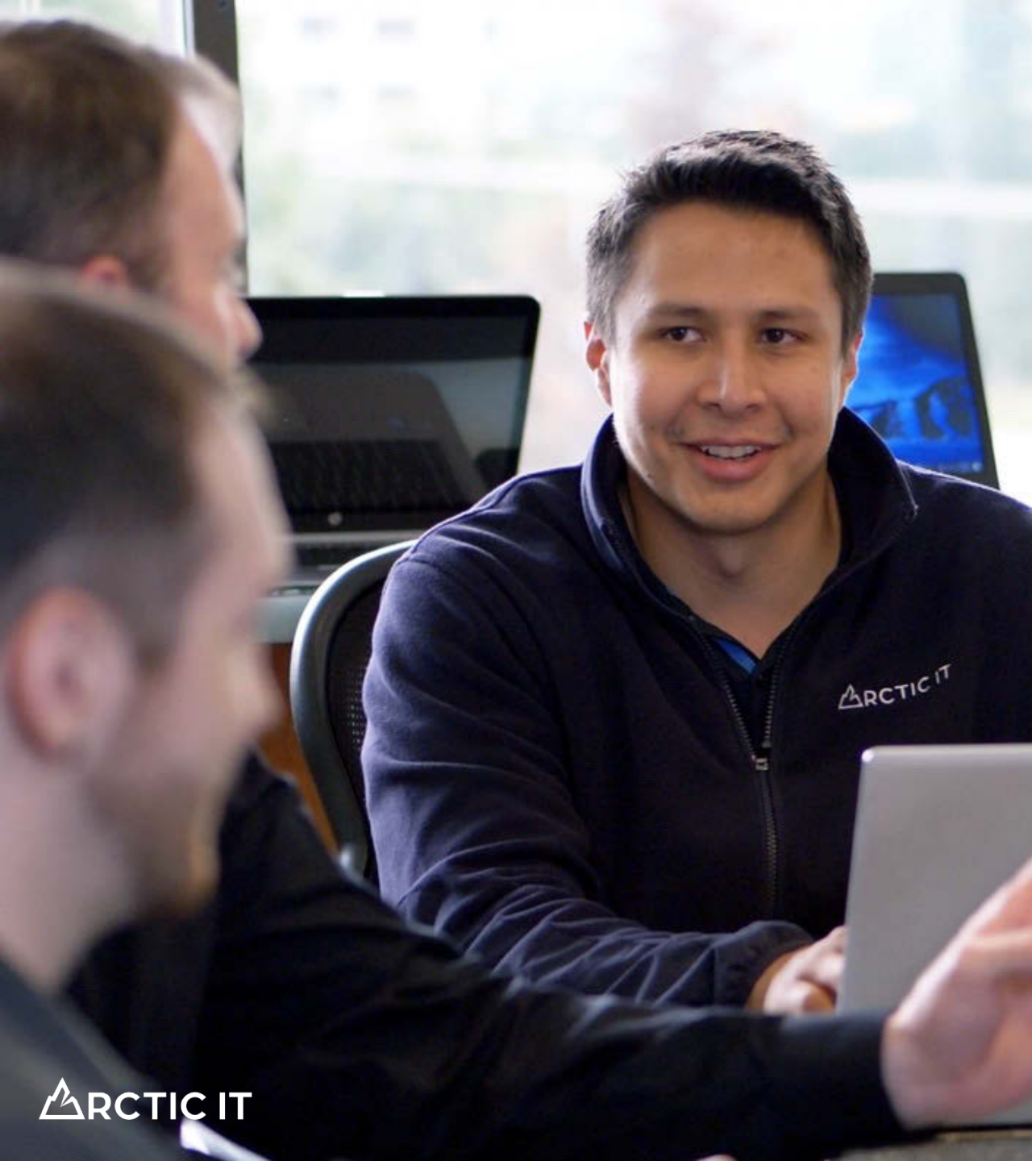
Today’s presentation

- Arctic IT Partnership
- Zero Trust Architecture (ZTA)
  - What is it
  - What does it look like
  - How to implement it
- Journey of the Eastern Band of Cherokee Indians
- Getting Started
- Q & A

ARCTIC IT Microsoft

A partnership that works for you

ARCTIC IT Microsoft



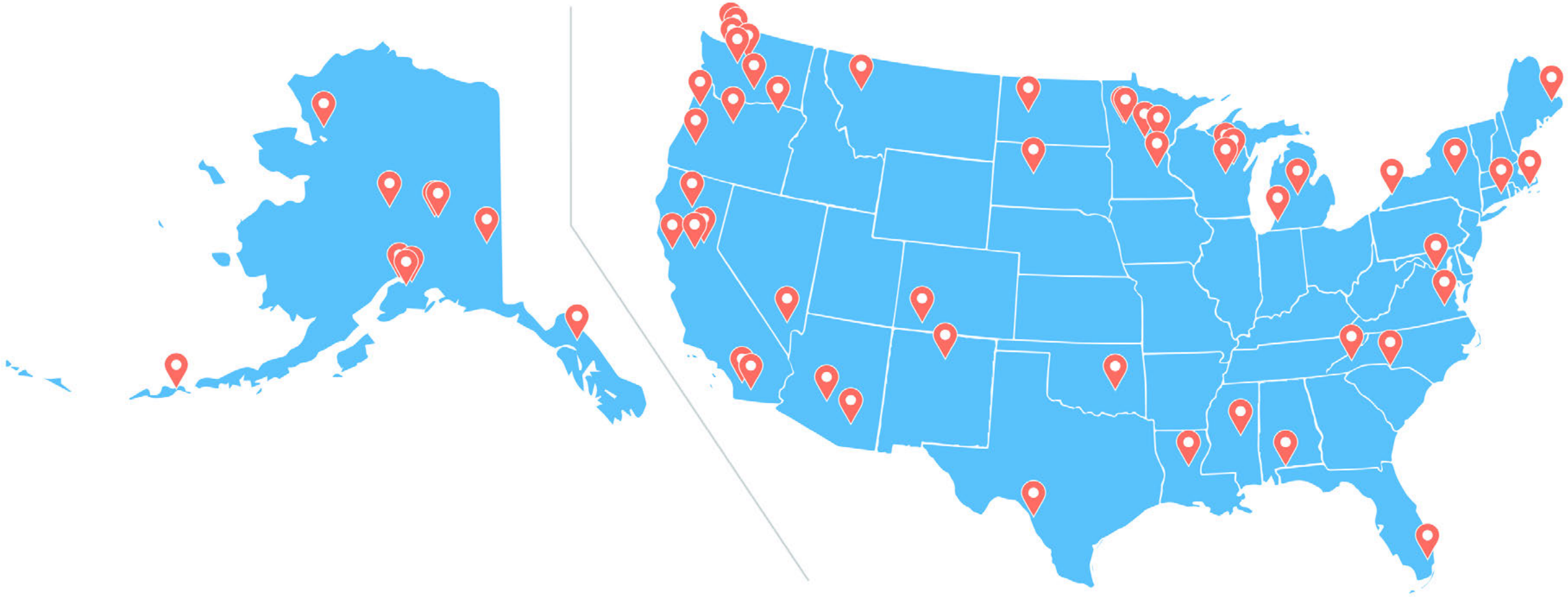
Arctic IT has deep roots with tribes

- More than 15 years of community engagement
- Client experience with 80 tribal entities across the U.S.
- Specialize in technology for tribal governments and casinos
- 100% native-owned

Gold
Microsoft Partner

Microsoft

Our experience spans tribal nations across the U.S.



Defining Zero Trust Architecture

Definition

Zero Trust Architecture is a security model designed to minimize lateral movement using the principles of **“never trust, always verify”, least privileged access, and assume breach**.

The guiding principals of Zero Trust

1

Verify Identity Explicitly

Always authenticate and authorize based on all available data points, including identity, location, device health, etc.

2

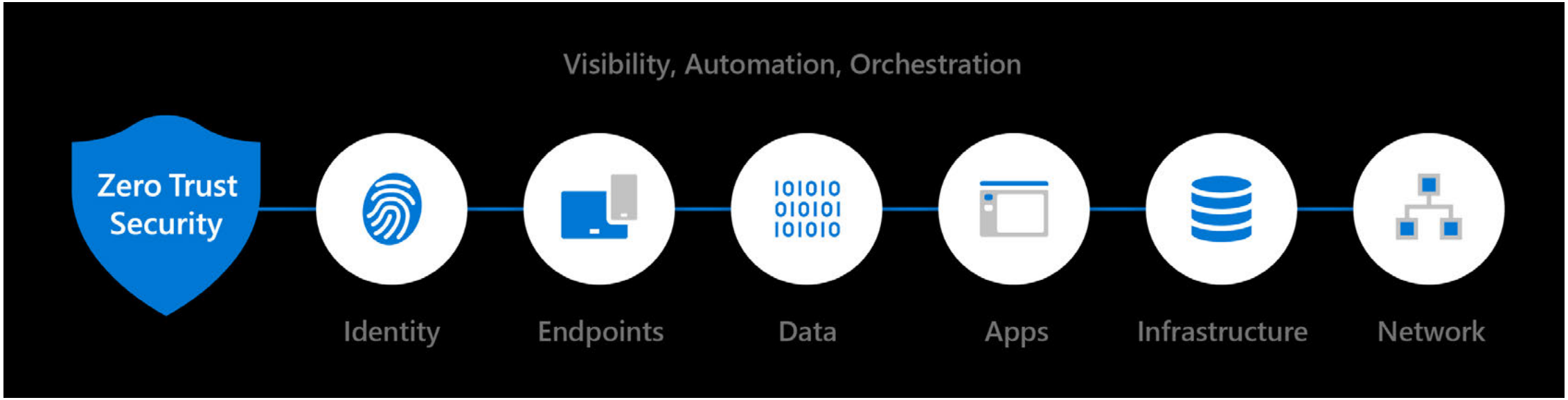
Use Least Privileged Access

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection to help secure data and productivity.

3

Assume Breach

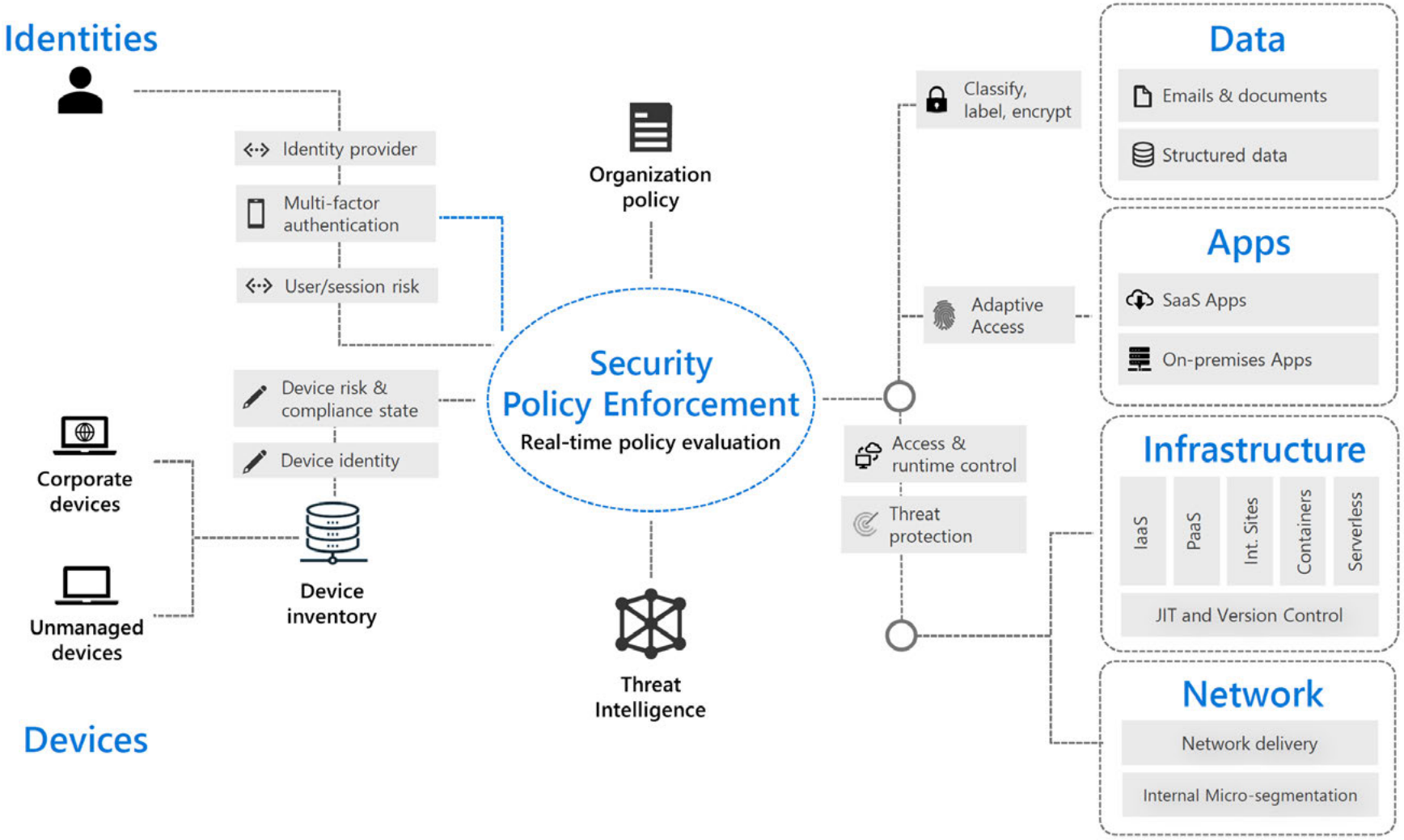
Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.



What a Zero Trust Architecture looks like

ARCTIC IT Microsoft

Zero Trust Model ➡ [M365 + Azure Security Center + Azure Sentinel]



Securing your identities with Zero Trust

Identities (representing people, services, or IoT devices) are the common dominator across today's many networks, endpoints, and applications. In the Zero Trust security model, they function as a powerful, flexible, and granular way to control access to data.

Before an identity attempts to access a resource, organizations must:

- **Verify the identity with strong authentication.**
- **Ensure access is compliant and typical for that identity.**
- **Follows least privilege access principles.**

Once the identity has been verified, we can control that identity's access to resources based on organization policies, on-going risk analysis, and other tools.

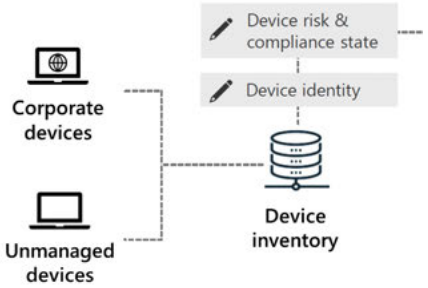
Azure Active Directory

Microsoft Entra Permissions Management

Securing your endpoints with Zero Trust

There are a few key rules for securing devices and endpoints in a Zero Trust model:

- **Zero Trust security policies are centrally enforced through the cloud and cover endpoint security, device configuration, app protection, device compliance, and risk posture.**
- **The platform as well as the apps that run on the devices are securely provisioned, properly configured, and kept up to date.**
- **There is automated and prompt response to contain access to corporate data within the apps in case of a security compromise.**
- **The access control system ensures that all policy controls are in effect before the data is accessed.**

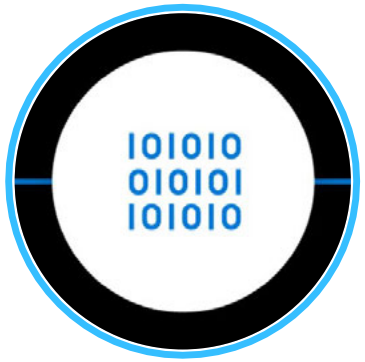


Devices

Microsoft Endpoint Manager

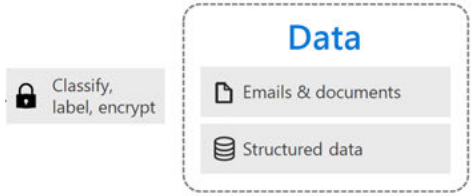
Microsoft Defender for Endpoint

Securing your data with Zero Trust



When data and sensitive content is understood, labeled, and classified, organizations can:

- **Inform and enforce policy decisions to block or remove emails, attachments, or documents.**
- **Encrypt files with sensitivity labels on device endpoints.**
- **Auto-classify content with sensitivity labels through policy and machine learning.**
- **Track and monitor sensitive content using policies as the content travels inside and outside your digital estate.**



Microsoft Defender for Office

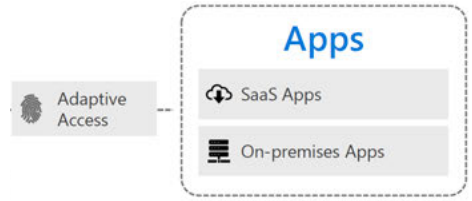
Microsoft Information Protection

Microsoft Purview

Securing your applications with Zero Trust

The Zero Trust model helps organizations ensure that apps, and the data they contain, are protected by:

- **Applying controls and technologies to discover Shadow IT.**
- **Ensuring appropriate in-app permissions.**
- **Limiting access based on real-time analytics.**
- **Monitoring for abnormal behavior.**
- **Controlling user actions.**
- **Validating secure configuration options.**



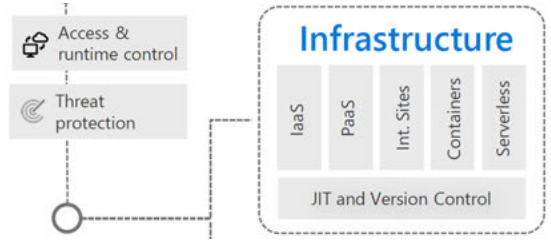
Azure Active Directory

Microsoft Defender for Cloud Apps

Securing your infrastructure with Zero Trust

Modern security with an end-to-end Zero Trust strategy makes it easier for you to:

- **Assess for version.**
- **Perform configuration management.**
- **Employ Just-In-Time and Just-Enough-Access (JIT/JEA) administrative privileges to harden defenses.**
- **Use telemetry to detect attacks and anomalies.**
- **Automatically block and flag risky behavior and take protective actions.**

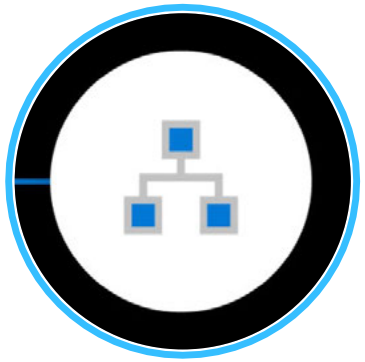


Microsoft Defender for Cloud

Just as importantly, Microsoft Azure Blueprints and related capabilities ensure that resources are designed, implemented, and sustained in ways that conform to an organization's policies, standards, and requirements.

Azure Blueprints, Azure Policies, Azure Security Center, Azure Sentinel, and Azure Sphere can greatly contribute to improving the security of your deployed infrastructure and enable a different approach to defining, designing, provisioning, deploying, and monitoring your infrastructure.

Securing your network with Zero Trust

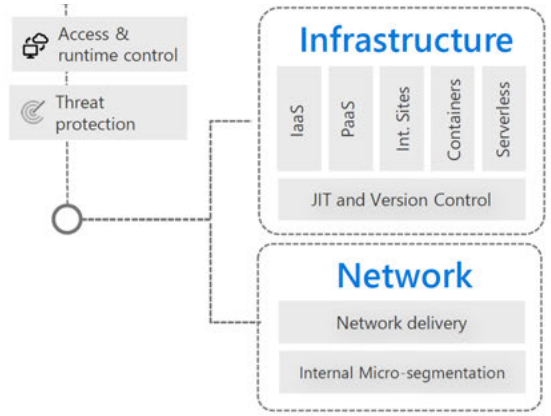


In the Zero Trust model, there are three key objectives when it comes to securing your networks:

- **Be ready to handle attacks before they happen.**
- **Minimize the extent of the damage and how fast it spreads.**
- **Increase the difficulty of compromising your cloud footprint.**

To make this happen, we follow the three Zero Trust principles:

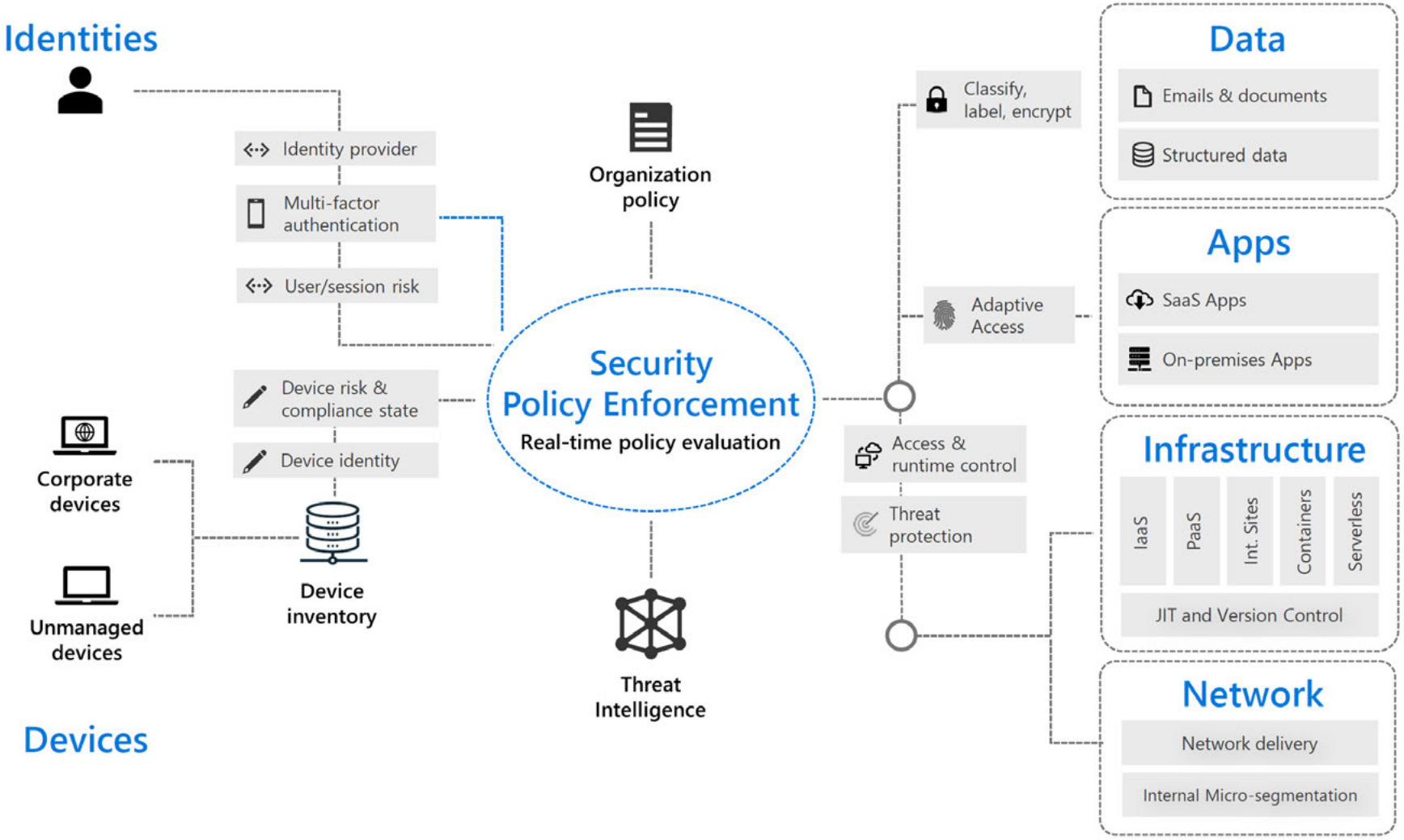
- **Verify identity explicitly.**
- **Use least-privileged access.**
- **Assume breach.**



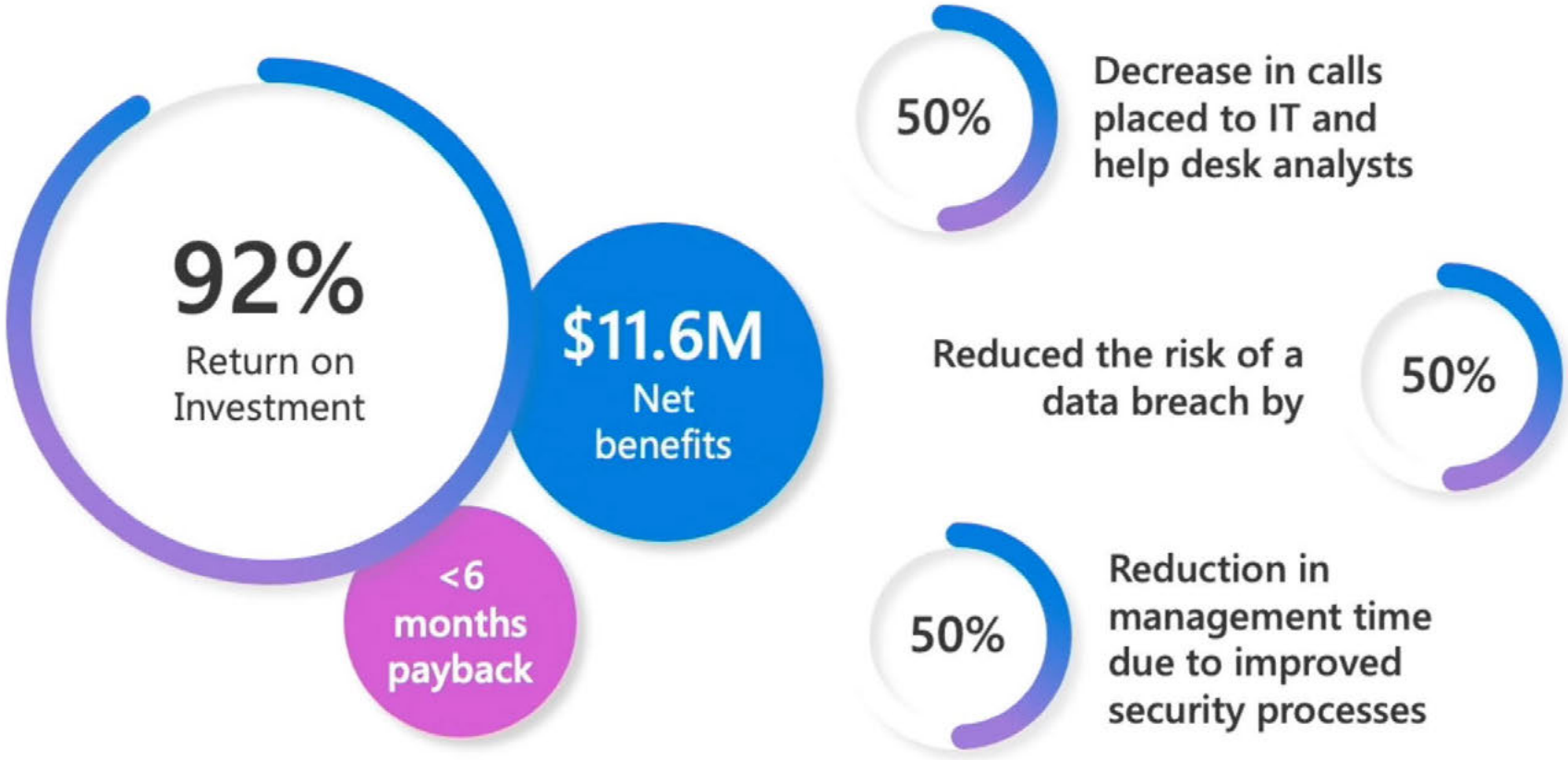
Azure AD Application Proxy

Azure Networking

Zero Trust Model ➡ [M365 + Azure Security Center + Azure Sentinel]



Total Economic Impact™ of Zero Trust solutions from Microsoft



The Total Economic Impact™ of Zero Trust solutions From Microsoft, December 2021. Study by Forrester Consulting, commissioned by Microsoft

Tribes are moving to the Microsoft Cloud

(Stats as of October 2022)

GREATER THAN

300

Tribal Tenants in the cloud

GREATER THAN

155k*

Tribal employees on Microsoft 365 E3/E5

GREATER THAN

60

Tribal organizations on Dynamics 365 SaaS Apps

*PLUS, another **65,000+ Tribal users** that are in the cloud at a mix level of suites and services

ARCTIC IT Microsoft

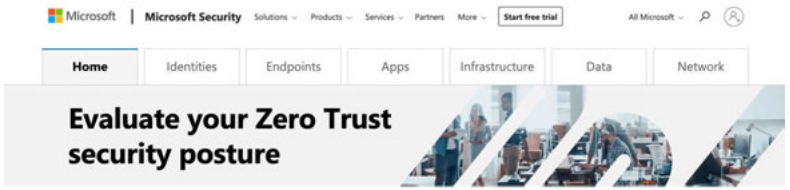
How to implement a Zero Trust Architecture

ARCTIC IT Microsoft

1

Assess your existing security posture

- Get into an identity-centric mindset
- Evaluate your current environment based on Zero Trust principals
- Take the quiz: https://bit.ly/3KSINEY

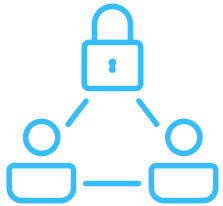


ARCTIC IT Microsoft

2

Build a security operations team

- Build internally or hire it out (or hybrid)
- Use a SIEM like Sentinel to capture log data
- Educate staff on Kusto (a query language) to build automated queries

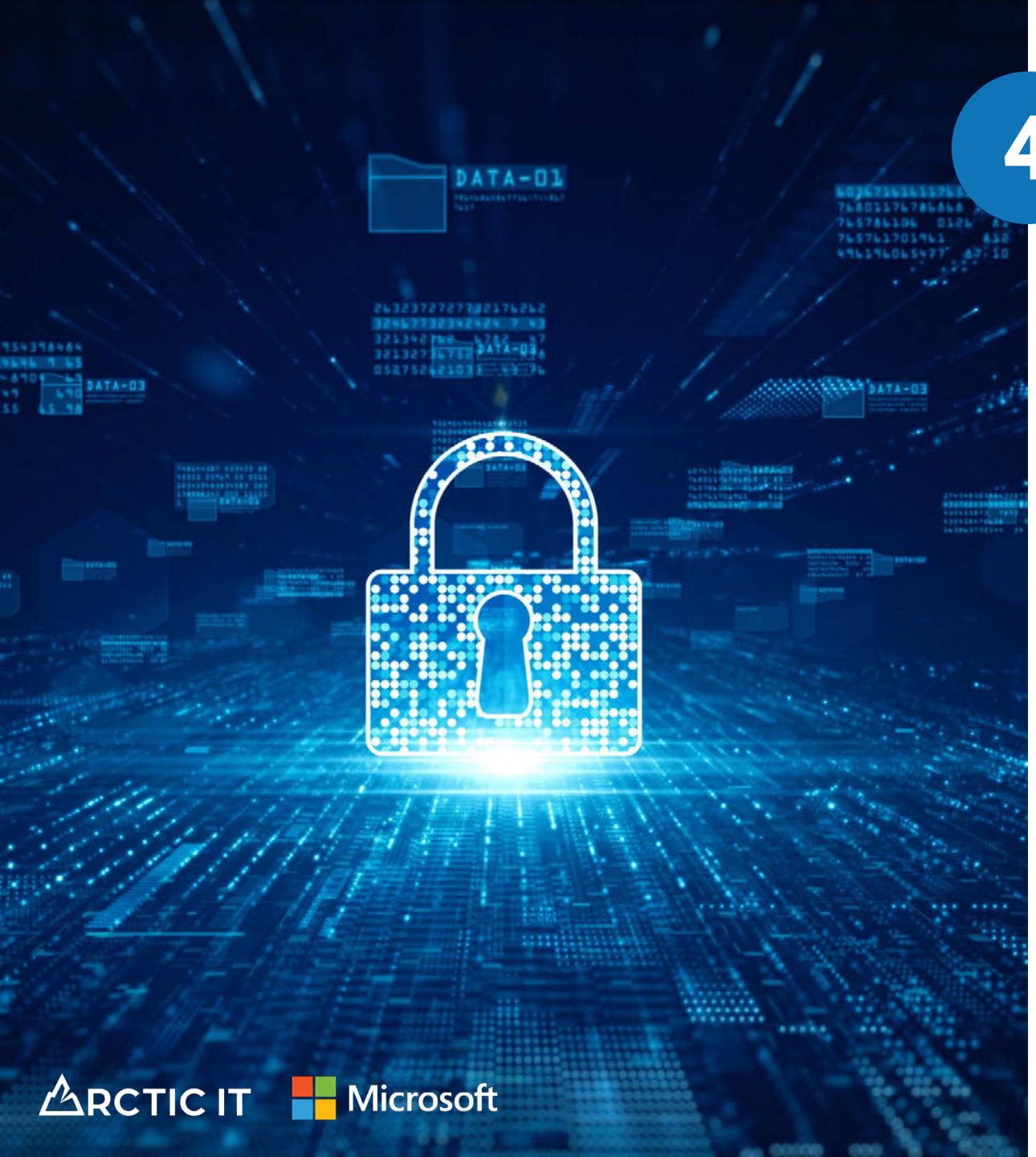


ARCTIC IT Microsoft

3

Prioritize the security of identities, devices & apps

- Switch to a North-South identity via Azure AD
- Turn on MFA
- Implement Microsoft Endpoint Manager
- Secure legacy apps with micro-segmentation in Azure



4

Establish data governance

This is the heavy lift to get right.

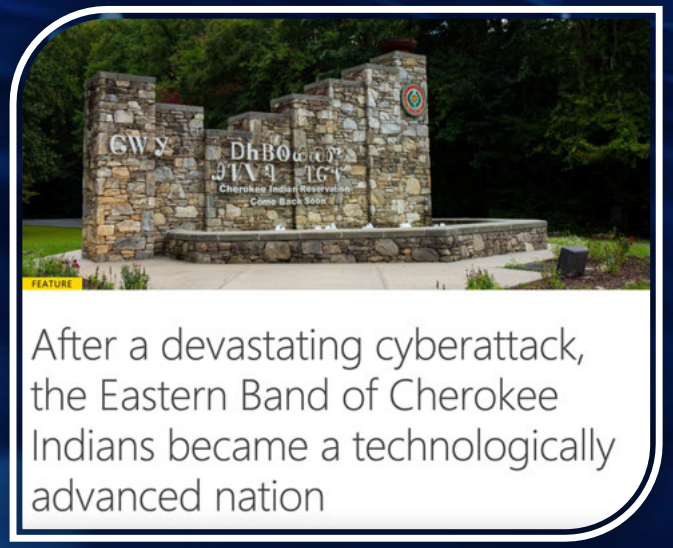
- Get key department stakeholders onboard
- Configure Data Loss Prevention
- Configure Information Protection
  - Provides information protection for hybrid cloud scenarios
- Set classification levels (goal of 2 or 3), do not over-complicate
- Use auto-classification tools to scan data

Feature	Microsoft 365 E3	Microsoft 365 E5
Data Loss Prevention	Add-on	Included
Information Protection	Included	Automated
Data Auto-Classification Tool	Add-on	Included

ARCTIC IT Microsoft

5 Continuously optimize

- Technology is changing rapidly day by day
- Routinely identify gaps in your security posture
  - Cross-functional within IT
- Make it your goal to be proactive, rather than reactive



READ THE FULL STORY!

Journey of the Eastern Band of Cherokee Indians

ARCTIC IT Microsoft

Getting started

Getting started on your journey to Zero Trust

- Partner with a trusted advisor.
- ZTA is an investment. Research and apply for the new IIJA Funding that launched in September 2022.
- Do not wait until you get breached.

Evaluate your Zero Trust security posture: https://bit.ly/3KSINEY


Questions?

Thank You!

Bill Travitz
Director Tribal Business

btravitz@arcticit.com

Brent Nix
Sr Technology Specialist, Cybersecurity

Microsoft

ARCTIC IT
Tenacious Ingenuity®