Zero Trust Strategy Enabling the Hybrid Campus Experience

Steve Faehl Microsoft US Security CTO
COVID-19 brought unexpected IT challenges
How to rapidly enable remote and local faculty, staff, and students while protecting resources?

- Bad actors exploiting COVID-19 themes and VPN vulnerabilities
- VPN scalability constraints
- Sudden spike in the need for remote access to apps
- Challenges to onboarding and manage new and personal devices
- Network dependence of many security controls
- Remote support and student onboarding is difficult or impossible
Schools need the flexibility of a secure hybrid campus experience

- **Enable remote access to apps**
  
  Give students, faculty, and staff access to the apps they need while increasing security.

- **Manage devices and apps**
  
  Enable faculty and staff to use their own devices with unified management.

- **Protect sensitive resources**
  
  Built-in and frictionless security controls to protect data while maintaining productivity.
Security-enabled operational agility
The secure hybrid campus experience is independent of modality and increases flexibility

Working as a team amidst disruption at the University of South Florida

Christine Brown
Assistant VP of Digital Learning in Innovative Education at USF

“We support faculty in developing engaging, high-quality education regardless of the modality. When we design a course, we’re looking at the alignment between learning outcomes, content and assessment, and how it all works together in a student-centered learning environment.”
“Zero trust (ZT) is the term for an **evolving set of cybersecurity paradigms** that move network defenses from static, network-based perimeters to **focus on users, assets, and resources**.”

“Zero trust assumes there is **no implicit trust granted to assets or user accounts** based solely on their physical or network location.”

“Zero trust **focuses on protecting resources, not network segments**, as the network location is no longer seen as the prime component to the security posture of the resource.”

Source: SP 800-207 Draft, February 2020
Microsoft believes that Zero Trust is a strategy that should be woven throughout an organization’s architectures, technology selections, operational processes, and culture.
Moving from Implicit Trust to Zero Trust

**Implicit Trust**
- Request context:
  - Unauthenticated
  - Network Identifiers
- Static policy:
  - Allowed
- Level of access permitted:
  - Full Access
  - No Access

**Zero Trust**
- Request context:
  - Identity
  - Device
  - Application
  - Network
  - Infrastructure
  - Data
- Dynamic policy with continuous monitoring:
  - Known
  - Trusted
  - Allowed
- Level of access permitted:
  - No Access
  - Limited Access
  - Full Access
  - Increase Assurance
  - Remediate
Building Assurance

Choose attributes and assurances from across the six Zero Trust pillars to achieve necessary trust level per resource.
Building Assurance

Choose attributes and assurances from across the six Zero Trust pillars to achieve necessary trust level per resource:

- User: Was multi-factor used?
- Device: Is it a registered device?
- Apps: Is the application sanctioned?

- Network
- Infrastructure
- Data

- LMS (High Trust)
- Financial Aid (Medium Trust)
- Admin Access (Low Trust)
- Implicit Trust
Building Assurance

Choose attributes and assurances from across the six Zero Trust pillars to achieve necessary trust level per resource

- **User**
  - Was multi-factor used?
  - How risky is the user’s activity?
  - Is it a registered device?
  - Is it compliant with policy?
  - Is the session monitored?
  - How sensitive is the data?

- **Device**

- **Apps**

- **Network**

- **Infrastructure**

- **Data**

- **LMS**
  - High Trust

- **Financial Aid**
  - Medium Trust

- **Admin Access**
  - Low Trust

- **Implicit Trust**
**Building Assurance**

Choose attributes and assurances from across the six Zero Trust pillars to achieve necessary trust level per resource.

<table>
<thead>
<tr>
<th>User</th>
<th>Device</th>
<th>Apps</th>
<th>Network</th>
<th>Infrastructure</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Was multi-factor used?</td>
<td>Is it a registered device?</td>
<td>Is the application sanctioned?</td>
<td>Is the session monitored?</td>
<td>Is the resource privileged?</td>
<td>How sensitive is the data?</td>
</tr>
<tr>
<td>How risky is the user’s activity?</td>
<td>Is it compliant with policy?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Trust Levels**

- **High Trust**
- **Medium Trust**
- **Low Trust**
- **Implicit Trust**
Questions?
Scenario: Beyond VPN - Layer in Zero Trust with Secure Hybrid Access

- Central policy governs resource access (Identity Team and Security Team)
- Pre-Authentication
  - Known attributes
- Pre-Authorization
  - Trusted assurances
  - Allowed connectivity
  - Permitted access

- Zero Trust Policy Added

- Resource Policy Unchanged

- Resource policy (Resource Owner)
  - Authentication
    - Known credential
  - Authorization
    - Permitted access

- Anywhere User
- Azure AD
- Reverse Connect
- Internal User
- Resource
### Phased rollout plan to reduce complexity and friction

#### Phase 1: Identify and monitor
- Use a single user account with strong authentication
- Register personal and organizational devices
- Go hybrid by connecting your on-premises infrastructure to the cloud
- Enable access to on-premises web apps
- Discover and register applications in use

#### Phase 2: Reduce risk
- Add protection for identity-based attacks and monitor for signals of increased risk
- Enable secure methods for personal devices to access sensitive workloads
- Begin monitoring usage of sensitive data

#### Phase 3: Increase protection
- Manage and patch devices remotely
- Add application protection policies
- Begin policy enforcement
Phase 1: Identify and monitor

- Identify users and register devices
- Enable multi-factor authentication

Establish hybrid identity by connecting on-premises to cloud

Enable SSO access from anywhere to SaaS, cloud, and on-premises apps
Phase 2: Reduce risk

- Increase email protection
- Enable identity protection and risk-based conditional access
- Enable personal devices to reverse connect to secure virtual desktops
- Define sensitive data types and enable auto-labeling
Phase 3: Increase protection

- Enroll personal devices in MDM
- Enforce data and app policies
- Add app control session proxy

Enforce Information Protection
Secure hybrid work is enabled by Microsoft’s integrated end-to-end solutions:

**Architectural coherence enables end-to-end protection with reduced complexity**
Collaborate freely while also protecting sensitive information in Microsoft Teams

Identify and protect users

- Enforce risk-based sign-in policies backed by identity protection to secure access with less user friction.
- Use communications compliance to encourage positive student interactions

Manage and secure devices

- Deploy endpoints with zero touch using autopilot or register personal devices
- Enable unified endpoint management to keep devices healthy and unified endpoint security to protect them.

Identify and protect sensitive data

- Educate and guide end users with notifications and “policy tips.”
- Automatically block messages that contain highly sensitive information.
Protect organizational assets anywhere with Microsoft’s end-to-end solutions

Only trusted people

- Azure Active Directory SSO and MFA
- Microsoft Defender for Office
- Conditional Access
- Azure Identity Protection
- Azure B2B and B2C Collaboration
- Azure Privileged Identity Management

Using trustworthy resources

- Windows Virtual Desktop
- Microsoft Defender for Endpoint
- Microsoft Cloud App Security
- Azure Defender
- Microsoft Defender for Identity
- Intune MAM and MDM

Access systems, data, and apps

- Azure VPN
- Azure AD Secure Hybrid Access
- Microsoft Information Protection
- Cloud App Discovery
- Azure Sentinel
- Azure Policy
- Azure Bastion
EDUCAUSE Events

- **Education Transformation: From Recovery to Reimagine** – Anthony Salcito, Microsoft VP of Education Industry, and featuring University of South Florida (Tuesday, October 27, 12:15 p.m. – 1:00 p.m.)

- **Security Can’t Wait: Securing Your Virtual Campus** – Micah Linehan, Microsoft Principal Technical Specialist, and featuring Kent State University (Wednesday, October 28, 11:00 a.m. – 11:20 a.m.)

- **Reimagine Student Engagement** – Rob Curtin, Microsoft Director of Americas Higher Education, and featuring Florida State University (Thursday, October 29, 11:00 a.m. – 11:20 a.m.)

Online Resources

- **Microsoft Zero Trust Deployment Center**

- **Zero Trust Implementation Case Study**

- **Hybrid learning classroom**

Microsoft Team

- **Your Account Team**
- **Your Microsoft reseller or partner**

- **Education Help Center**

Find out more about Zero Trust and the Secure Hybrid Campus Experience
Thank you!

https://www.linkedin.com/in/steve-faehl