Connect It, Protect It
in Remote Working and Learning Environments

Wendy Nather
Head, Advisory CISOs
Duo Security

Peter Romness
Cybersecurity Principal
US Public Sector CTO Office

8 October 2020
Agenda

1. Educational trends & challenges
2. Zero Trust primer
3. Connect it, protect it with Zero Trust principles
4. Resources
No one expected this to happen now

A brand new, highly-contagious virus causes a global pandemic

- Campuses forced to close practically overnight
- All students, faculty, staff and administrators sent home
- Added effects on international students and faculty
- Remote learning has highlighted connectivity gaps
- Not just academics effected – all campus facilities
- Some campuses re-open in Fall, many to close within days
- A mix of on-campus and remote learning, with no end in sight
Remote users can **increase** cyber risks

- Loss of Network controls and restrictions on outside networks
- Use of more SaaS-based and unsanctioned apps
- Bypassing the VPN to gain network access
- More unpredictable BYOD
- Connecting to unsecured Wi-Fi without concern for cybersecurity
- Low awareness of how behavior exposes institutions to risk
Agenda

1. Educational trends & challenges
2. Zero Trust primer
3. Connect it, protect it with Zero Trust principles
4. Resources
The perimeter is no longer where it used to be: at the edge of your network

The perimeter is NOW any place you make an access control decision...

and it can be anywhere.
The Zero Trust Paradigm

Treat every access attempt as if it’s originating from an untrusted network
Zero Trust ≠ Lack of Trust
Zero Trust

Workforce
Ensure only the right users and secure devices can access applications.

Workloads
Secure all connections within your apps, across multi-cloud.

Workplace
Secure all user and device connections across your network, including IoT.
Deploying Zero Trust Access

- Inventory of Users
- Inventory of Devices
- Inventory of Applications
- Access Proxy for Secure Conn.
- Way to Gauge Trustworthiness
- Single Sign-On (SSO) Workflow
- Robust Policy Engine
Zero Trust Access: Where to Start?

1. Deploy secure access control (MFA) for all users & apps
2. Inventory all devices; Check security posture; Enable secure BYOD
3. Inventory all apps, dependencies, flows; Define tiers & adaptive, risk-based policies
4. Deploy access proxies, map expected flows and implement segmentation
5. Deploy analytics & anomaly detection capabilities
Zero Trust Critical Capabilities

• Trusted Access
• Micro-segmentation
• Continuous visibility & enforcement
• Threat intelligence
• Automation
Agenda

1. Educational trends & challenges
2. Zero Trust primer
3. Connect it, protect it with Zero Trust principles
4. Resources
Building Zero Trust Policies

Have we verified the user and device?

Do we have secure communications?

Is the device or app connecting to an unsafe entity?

Are our devices compromised now?

Secure cloud apps & collaboration tools

School Network
Use **Zero Trust** principles as you continue to adapt

Zero Trust is not a technology, it’s a way of thinking

- Call it what you like, you may already be doing some Zero Trust
- Think Workforce, Workload and Workplace
- Make incremental improvements
- Maintain flexibility
- Think long term
Agenda

1. Educational trends & challenges
2. Zero Trust primer
3. Connect it, protect it with Zero Trust principles
4. Resources
Free trials for securing your remote learners

- Duo MFA
- Umbrella DNS Security
- AMP for Endpoints
- AnyConnect VPN+

And many more!!
Links for more information:

- [Secure Remote Learning One-Pager](#)
- [SecureX Integrated Security Platform](#)
- [Learn more about Cisco Security in our Education space](#)
- [Video Explainer](#)
- [Free Trials](#)

Contact info: promness@cisco.com