Defending Our Schools and Students: A Look into Attack Trends and How to Stop Them with Zero Trust

October 20, 2022

Presenter

Adam Roeckl

Product Marketing Manager

Cyber attacks on schools ramping up

Recent cyberattacks highlight the vulnerability of California schools

Hackers infiltrate second-largest US school district in growing trend

US government warns ransomware attacks on schools may increase

Potential Fraud Schemes Targeting Individuals Seeking Federal Student Loan Forgiveness

Criminal hackers targeting K-12 schools, U.S. government warns

Cybersecurity: how safe is your school?

A growing and persistent problem for K12 schools

Encrypted attacks

315%
rise in encrypted attacks

207M
attacks targeted at EDU

Ransomware

80%
rise in ransomware

225%
rise in double extortion targeted at EDU

9th
EDU rank in most targeted with ransomware

Phishing

47.4M
phishing attacks targeted at EDU

436%
rise in phishing targeted towards retail

Case study: Los Angeles Unified ransomware attack

Hackers infiltrate second-largest US school district in growing trend

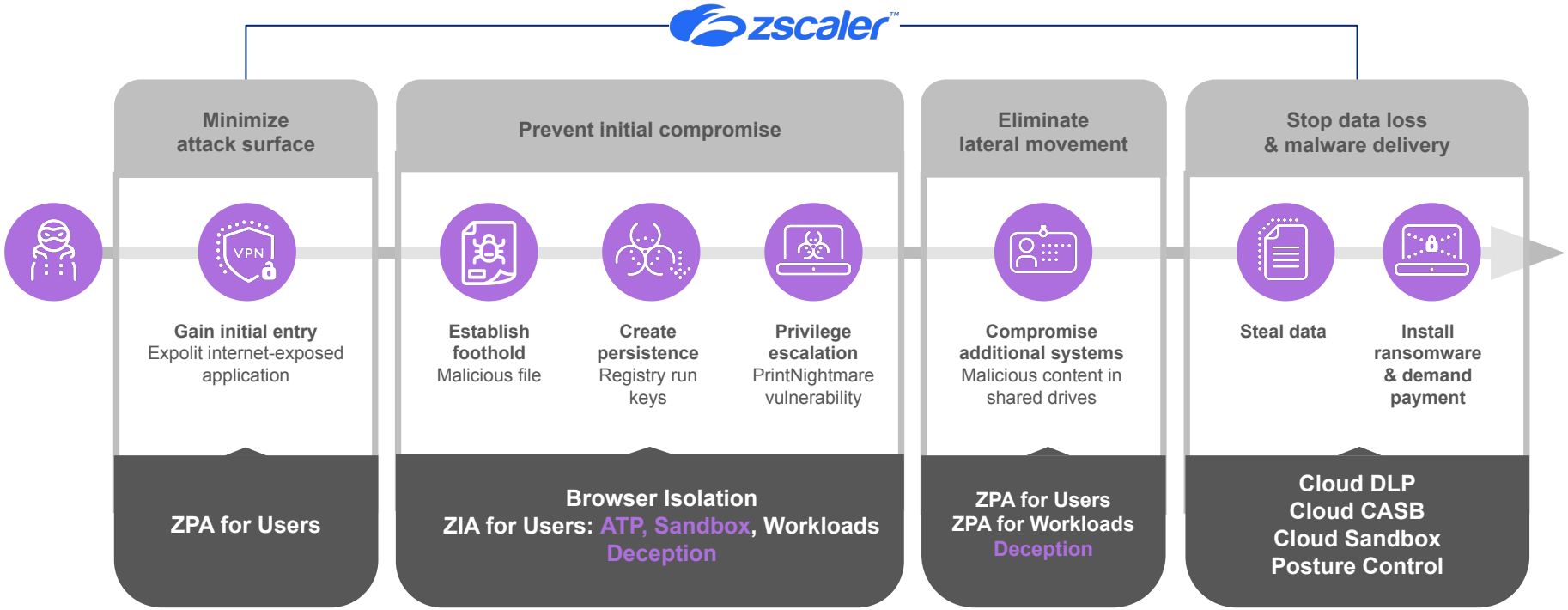
Fast facts:

- Ransomware attack
- 600,000 students impacted
- 56% of K12 schools report being hit by ransomware
- 45% of K12 schools pay ransom

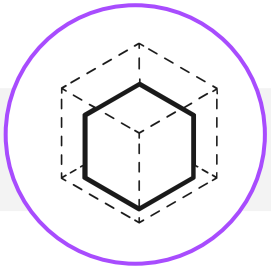
Outcomes:

- Operations slowed/halted
- Access to email, computer systems, and applications stopped to slow infection
- Prompted response from:
  - White House
  - FBI
  - Department of Homeland Security

Aligning these attack techniques to the killchain

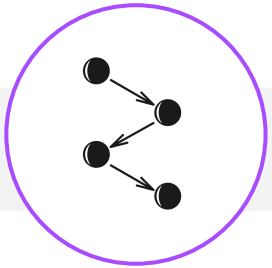


Zscaler holistically prevents cyber attacks and data loss



Reduce Attack Surface

Stop Compromise



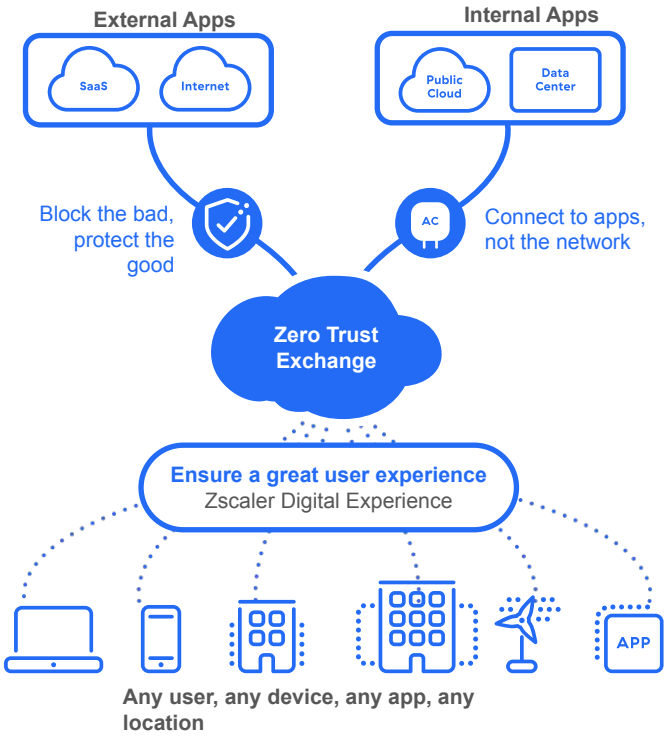
Lateral Movement

Data Loss

ZPA	ZIA	ZPA + CNAAP	ZIA+Data Protection
Zscaler Private Access • Privileged Remote Access Zscaler Internet Access • Browser Isolation	Zscaler Internet Access • Intrusion Prevention • Cloud Sandbox • Cloud Firewall/IPS • Secure Web Gateway • Browser Isolation	Zscaler Private Access • Deception Zscaler for Workloads • Workload Protection • Posture Control	Zscaler Internet Access • Cloud Sandbox • Secure Web Gateway • Browser Isolation DLP + CASB • Data at rest • Data in motion

The Zscaler Zero Trust Exchange Platform

Protect against cyberthreats & data loss while enhancing app access & experience for the hybrid workforce



Zscaler for Users

- Secure Internet and SaaS access (ZIA)
- Secure private app access (ZPA)
- Digital Experience (ZDX)

Zscaler for Workloads

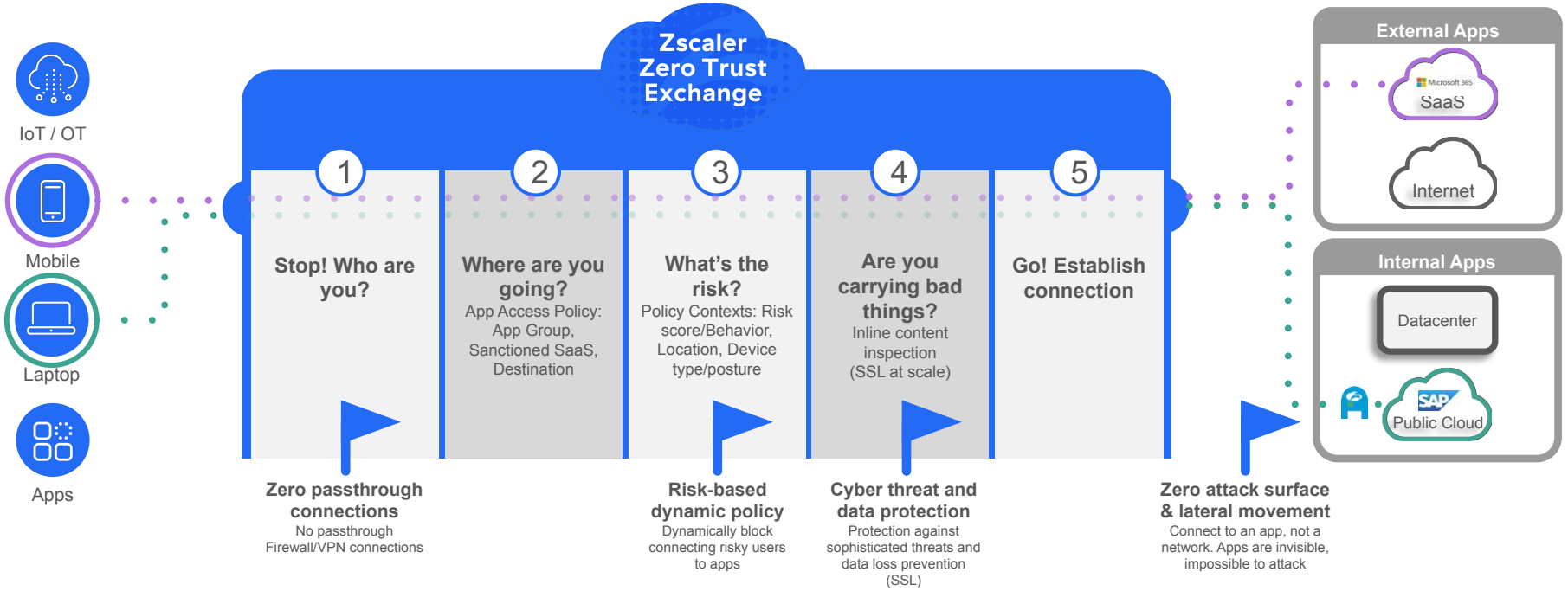
APP

- Secure internet access
- Secure Workload-to-workload communication
- Configuration and exposure scanning (CNAPP)

Zscaler for IoT and OT

- Secure internet, SaaS and private app access
- Privileged access to OT

The Zscaler Zero Trust Exchange provides comprehensive security built on least-privileged access



Stop advanced cyber threats with Zscaler

Risk-based policy | AI/ML | Automation | Defense in-depth | Cloud-delivered

Protect Users

Secure connectivity with advanced risk-based security and access policies

Stop Attacks

Detect and block known and unknown threats with inline AI/ML and decoys

Speed Response

Enrich investigations with corroborated threat intel to simplify incident response

35x
reduction in infected machines

85%
reduction in ransomware

74%
security FTE time saved

Sources: ESG Economic Validation Study; Zscaler

Case study: Seesaw messaging app exploitation

Popular school messaging app hacked to send explicit image to parents

Fast facts:

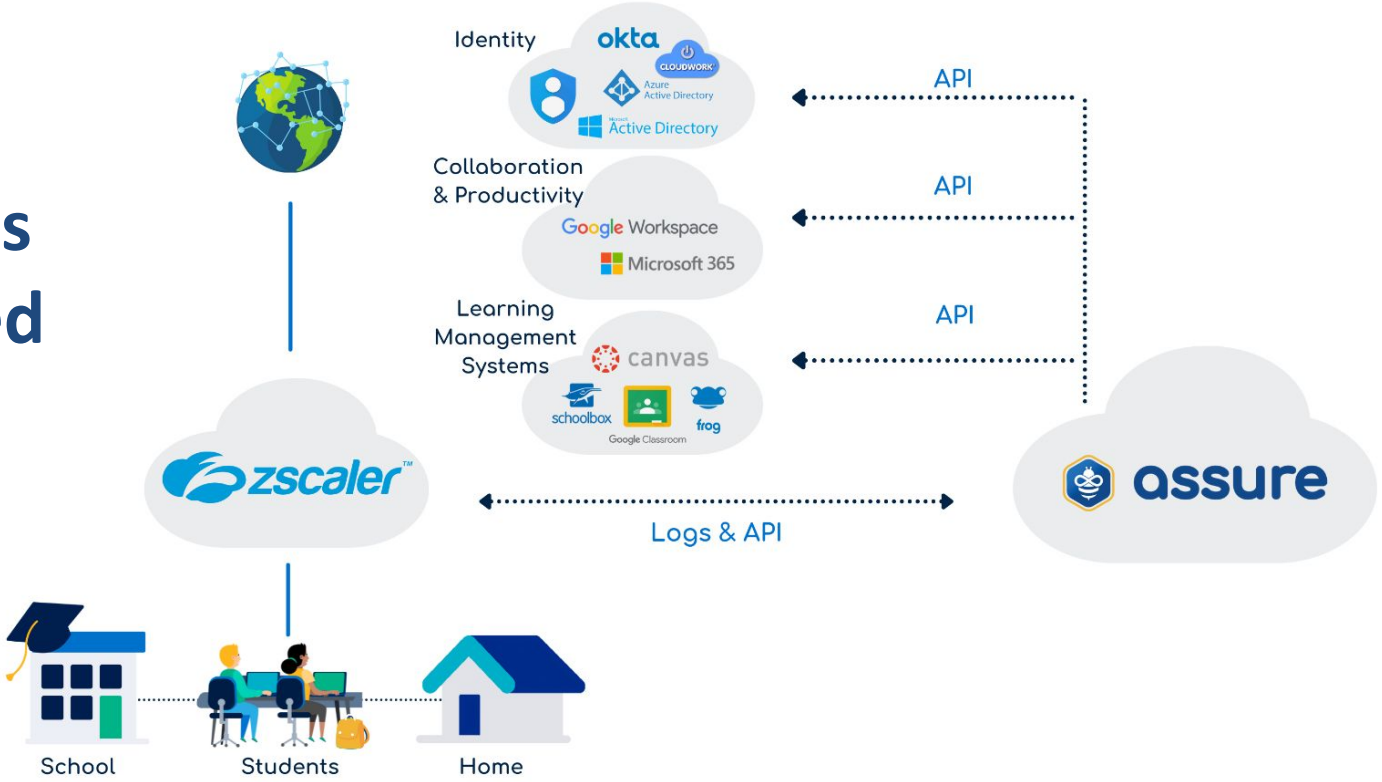
- Exploited messaging app with credential stuffing
- Sent lewd images via app
- 10 million app users
- States affected:
  - Illinois
  - New York
  - Oklahoma
  - Texas

Outcomes:

- Horrified parents
- Compromised accounts
- Lack of trust in application/breakdown in communication

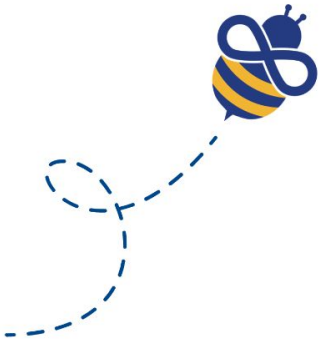
The intersection of security and student safety

Leveraging Technologies Already Used By Schools



saasyan

Applied Intelligence



1. Crowd-sourced words & phrases dictionary
2. Fuzzy logic & near-term analysis for misspelt words
3. Natural Language Processing to pick up context
4. Cohort analysis to identify outliers
5. Recurrence analysis to detect alarming patterns

In summary…

1. Attacks targeting K12 schools are on the rise, evident by recent headlines
2. A zero trust architecture provides protection against threats and data loss
3. The intersection of security and student safety is crucial

Thank you!