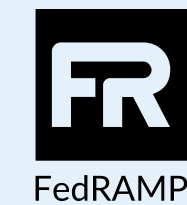


Zscaler for Higher Education



Learn more at zscaler.com/education

AT-A-GLANCE

The AI Security Platform Built on Zero Trust

SECURE YOUR USERS

- Replace legacy VPNs with policy-based Zero Trust access to apps and data
- Enable secure access for BYOD and managed devices
- Deliver a seamless user experience for any user, on any device, in any location.

SECURE YOUR CAMPUS

- Modernize campus and branch networking for secure connectivity
- Protect AI access, apps, and infrastructure
- Prevent data loss across web/SaaS with inline protection and consistent enforcement

SECURE YOUR RESEARCH

- Support compliance with Cybersecurity Maturity Model Certification (CMMC)
- Support adherence to ITAR (International Traffic in Arms Regulations)
- Manage secure third-party access to university data

315%

INCREASE IN ENCRYPTED ATTACKS

80%

INCREASE IN RANSOMWARE

576%

INCREASE IN PHISHING ATTACKS

\$3.86M

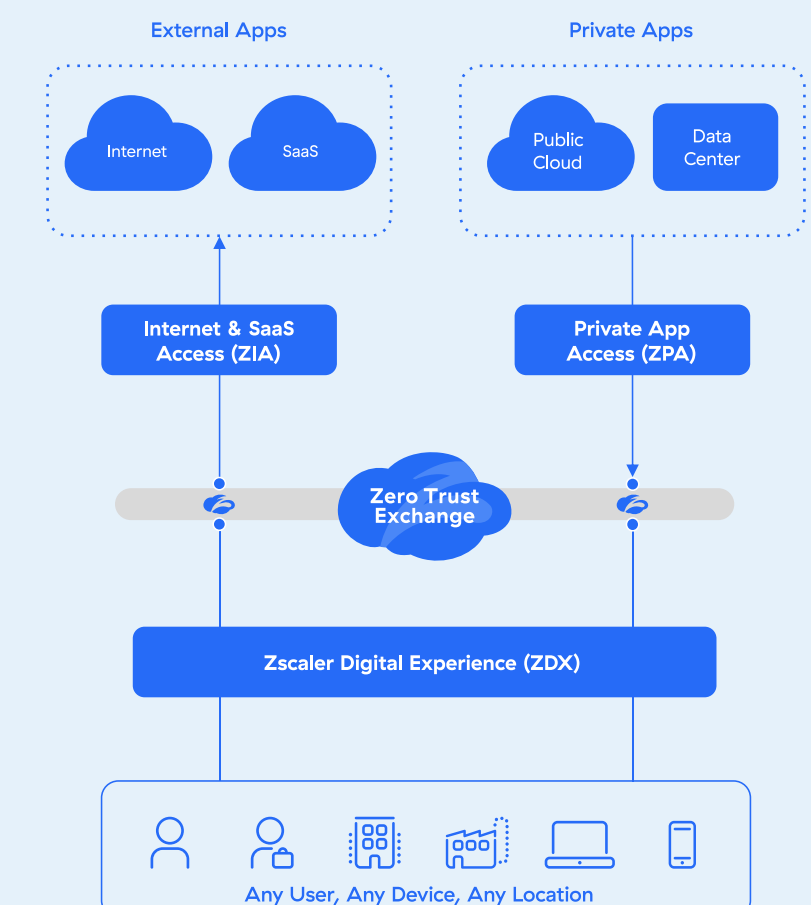
AVERAGE DATA BREACH COST

How Zscaler Can Help

- The University of South Carolina enabled a secure and scalable self-contained environment while meeting Department of Defense CMMC security service edge compliance requirements.
- Kern Community College District replaced legacy remote access solutions enabling precise app segmentation limiting lateral movement of threats.
- MCNC embraced local internet breakouts and securing over 1.5 million students and staff wherever they work.

Securely Transform Your Campus

Colleges and universities are under pressure to modernize security for networks, data, and AI while improving the student and faculty experience and lowering costs. Zscaler provides the tools to adopt a modern, direct-to-cloud, zero trust architecture that delivers secure, always-on access across campus and remote learning. FedRAMP/GovRAMP authorized and trusted by hundreds of organizations, Zscaler helps higher education stop cyberattacks and prevent data loss with the Zscaler Zero Trust Exchange.



The New AI Attack Surface in Higher Education

BALANCING ACADEMIC OPENNESS WITH THE REALITIES OF AI-DRIVEN THREATS

AI tools are evolving quickly, and some now go beyond only generating text to taking real actions on a user's device. OpenClaw is one of the first widely adopted examples of this new class – an AI agent capable of opening files, running commands, modifying settings, and interacting with local or online services. These capabilities expand academic exploration and creativity, but they also introduce risks most universities have not previously considered, especially in environments built on openness and experimentation.

Malicious extensions for OpenClaw are easy to create and hard to detect, giving attackers a path to steal data, execute commands, or move laterally across systems. For universities – where unmanaged devices, open networks, and hands-on exploration are the norm – this creates a meaningful risk. Similar footholds in past higher-education incidents have led to stolen research, exposed student records, and outages of critical campus systems.

Because universities cannot lock down their environments the way enterprises can, managing this risk requires a balanced, education-aligned approach that protects sensitive systems without limiting academic freedom. Rather than blocking tools outright, institutions can focus on a set of high-impact strategies that meaningfully reduce exposure while preserving the openness students and faculty expect. Platforms like Zscaler, which already process massive volumes of AI traffic, can help universities apply these protections consistently and with minimal friction.

Summary

Many universities are beginning to review how AI agents operate on their networks and adding common sense protections where it counts. Universities that are able to keep pace with the ever-evolving AI landscape will be able to prevent emerging AI tools from creating issues that are harder to unwind down the road, while still maintaining academic openness.

Contact your account executive for more information or zscaler.com/company/contact

FIVE HIGH-IMPACT STRATEGIES FOR UNIVERSITIES TO PROTECT AGAINST AI-BASED THREATS

1

Protect sensitive data without limiting open inquiry

2

Detect and disrupt malicious outbound activity without restricting legitimate research traffic

3

Allow AI experimentation while governing where institutional data can go

4

Connect unmanaged or guest devices in safer ways

5

Increase visibility on managed devices while accepting that not all devices can be managed

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.



Public Sector