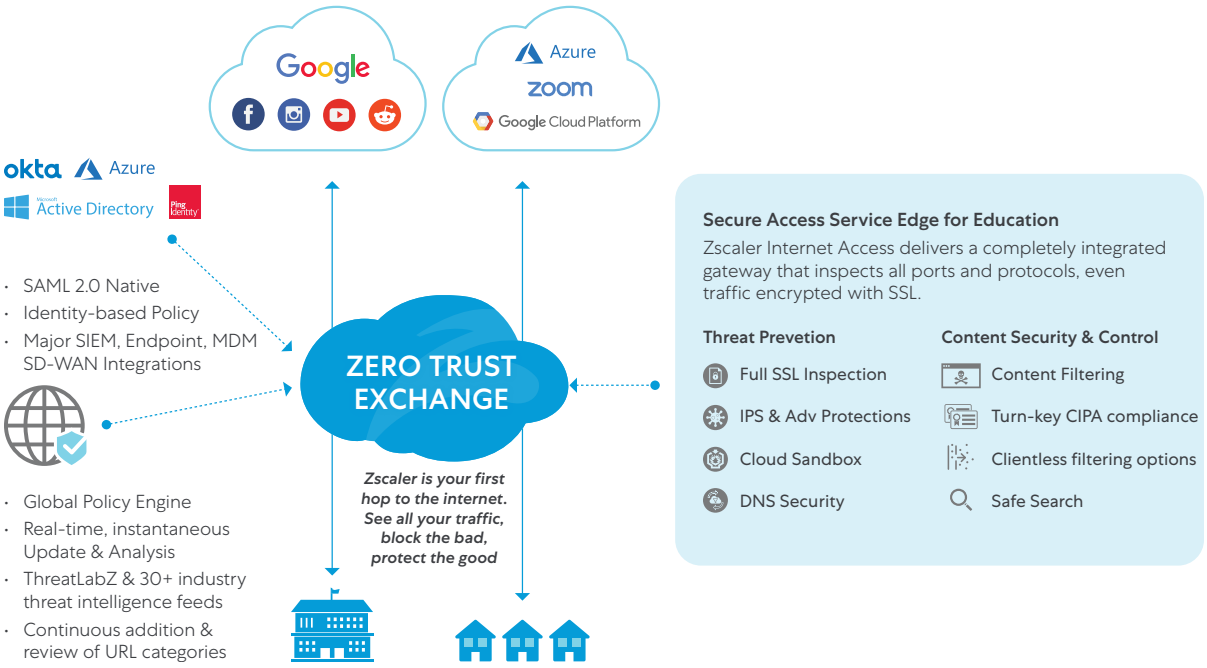
SOLUTION BRIEF

Securing the University for the Future
Zscaler™ for Higher Education

zscaler™

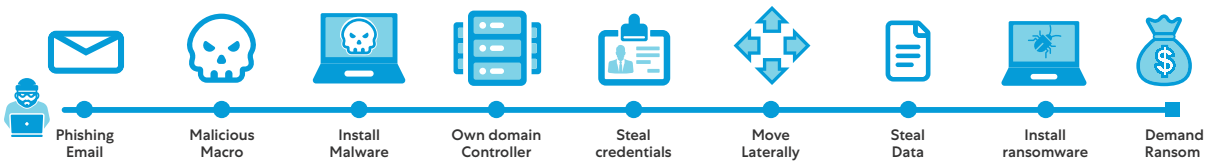
Higher education institutions have been on the cloud path for years. Forward-thinking CIOs have known that although there will always be the need for some infrastructure in the data center the majority of IT can be consumed via the cloud. The rapid move to online learning and remote work has accelerated the need for cloud adoption and digital transformation. SaaS and cloud-based infrastructure opens opportunities for new education models, expanding remote and online learning capabilities to students and teachers around the globe.

Securing cloud and on premise systems is a complex balance of championing the ability to access resources to drive academic discovery while protecting critical data, Personally Identifiable Information (PII), and Intellectual Property (IP). Zscaler's Zero Trust exchange provides customers a Zero Trust approach, only allowing the right users to access to the right data while also enabling each department to manage its own environment as needed. The Zscaler **Secure Access Service Edge (SASE)** architecture delivers secure connections while ensuring users are only a short hop from their applications.



Prevent Ransomware

The student, faculty, staff, and research data held within colleges and universities make them a ripe target for ransomware hackers. The way in which universities offer students access to their networks increases the allure for and vulnerability to these bad actors. A Zero Trust approach allows for ransomware risks to be mitigated. All internal communications are treated as potentially hostile and each communication between workloads must be authorized before it is allowed. In this way, Zero Trust can stop ransomware from moving laterally across the network, which can mean the difference between the malware encrypting a single laptop and encrypting hundreds of servers and datastores around the globe.



Zscaler Internet Access (ZIA) with **Advanced Threat Protection** and **Cloud Sandbox** delivers protection against ransomware, zero-day threats, and unknown malware. The Zscaler security cloud ensures that every packet from every user, on- or off-network, gets fully inspected from start to finish, with unlimited capacity to inspect SSL.

Zscaler Private Access (ZPA) provides secure access to private applications. Using a Zero Trust Network Access (ZTNA) architecture, ZPA doesn't connect users to the network, but rather it abstracts the network entirely from the user. This ensures that applications are never exposed to the internet, making them completely invisible to unauthorized users. All of this is done with the needs of faculty, staff, students, and third parties (vendors, contractors, and research collaborators) in mind -- removing the complexity and allowing seamless connection to systems both on premise and in the public cloud.

Securing Workloads in the Data Center and the Cloud

While many applications and systems are moving to the cloud, data centers are likely to remain a part of the campus infrastructure. Security solutions need to employ workload security and segmentation to meet this reality.

Zscaler Workload Segmentation is a new way to segment application workloads. Flat networks allow excessive access via unprotected pathways that allow attackers to move laterally and compromise workloads in cloud and data center environments. Shrinking segments and eliminating unnecessary pathways is a core protection strategy for workloads. However, the cost, complexity, and time involved in network segmentation using legacy virtual firewalls outweighs the security benefit. With Zscaler Workload Segmentation, microsegmentation happens in mere minutes rather than months —with just one click. From mapping data flows, to measuring exposure risk, to deploying policies for enforcement, our microsegmentation is quick and simple.

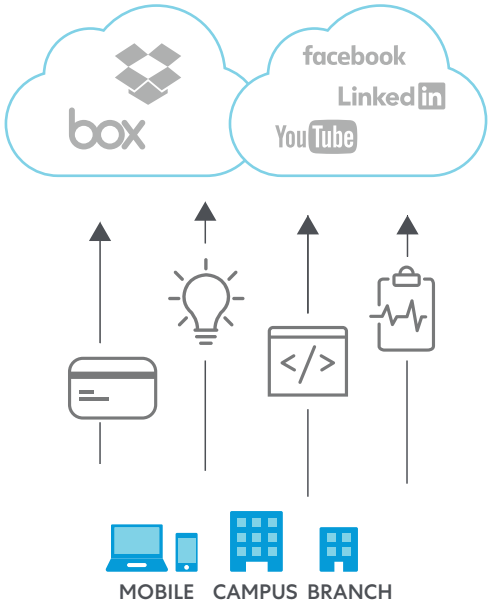
Zscaler Workload Posture remediates misconfigurations, secures sensitive data, and enforces least-privileged access. Workload Posture discovers assets and their configurations across IaaS, PaaS, and SaaS, enabling colleges and universities to understand the security posture of workload configurations mapped to policies, prioritize security gaps, and remediate prioritized issues automatically.

Data Protection

Higher Education institutions have unique needs when it comes to openness and collaboration. Users need access to courseware and data to complete their work, but much of that data can be proprietary. With the Zscaler platform, educational institutions can meet these competing needs and inspect the data that is being sent outside to gain visibility into what is being sent and who it should be shared with.

Zscaler also enables data protection with **Cloud Data Loss Prevention** that follows users and the applications they are accessing, always protecting against data loss. Zscaler inspects traffic inline, encrypted or not, and ensures SaaS and public cloud applications are secure, providing protection and visibility your IT teams need.

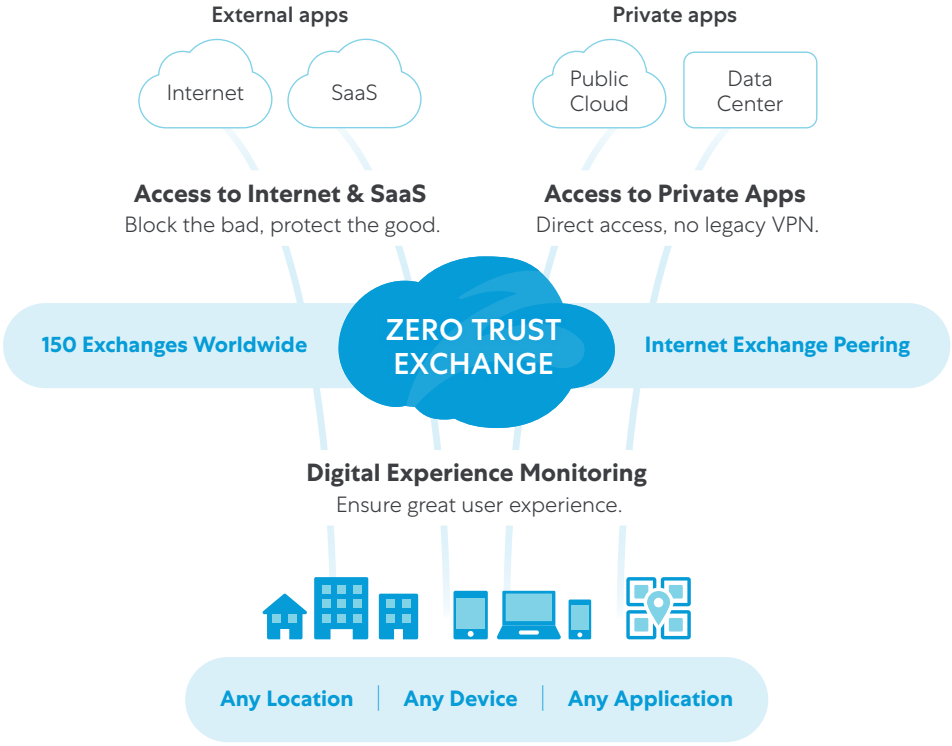
Zscaler Cloud Access Security Broker (CASB) mitigates the risk introduced by the inherent collaboration and sharing of SaaS applications. CASB enables organizations to securely adopt and govern the use of SaaS applications, IaaS offerings, and PaaS, providing real-time visibility and controls access and user activity across sanctioned and unsanctioned applications. The fully integrated platform eliminates overlay architectures and simplifies policy creation and administration, ensuring data is protected and compliance is maintained.



Enabling New Learning Models & Improving the User Experience

Colleges and universities can use virtual learning platforms to engage academics and experts outside of campus, expanding their course offerings. Additionally, schools can look to increase enrollment and reach via online class options without having to host more students on campus.

Zscaler can enable this expansion by providing secure remote access and a full security stack as-a-service for students, faculty, and staff, replacing the need for legacy VPN solutions and filling the gap left by traditional network-centric approaches to security. Built to work with Banner, Student Information Systems, Blackboard, Google, Zoom, WebEx and more, Zscaler ensures user experience is met and provides visibility into any issues with latency.



Additionally, with **Zscaler Digital Experience (ZDX)**, institutions can now fully monitor the cloud application experience simply and intuitively from the end-user perspective. ZDX restores visibility across the complete connection and quickly isolates user experience issues. ZDX delivers holistic, end-to-end user experience monitoring across any network, helping IT teams streamline troubleshooting and improve user productivity.

How Zscaler Helps Higher Ed Earn an "A" in Security

The delivery of Higher Education is changing rapidly. As more parties -- students, faculty, staff, third party partners -- connect and collaborate online, securing the data and the networks that data resides on becomes more complicated by the day. This complexity can be mitigated with a Zero Trust approach that verifies identity and access in a way that is seamless to users. In fact, Gartner listed Zscaler's approach as the sole "Leader" in its **Magic Quadrant for Secure Web Gateways**.

Figure 1: Magic Quadrant for Secure Web Gateways

Source: Gartner (December 2020)

To learn how we can help your institution meet your security needs today and into the future visit **zscaler.com/industries/education →**

About Zscaler

Zscaler accelerates digital transformation with its Zero Trust Exchange, a SASE-based platform that provides fast, secure connections between users, devices, and applications over any network. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc. 120 Holger Way | San Jose, CA 95134 | +1 408.533.0288