WHITE PAPER

The Identity-First Campus

Protecting the Entire Student Experience

ENTRUST

SECURING A WORLD IN MOTION

On Campus, Identity Is the Foundation of Everything

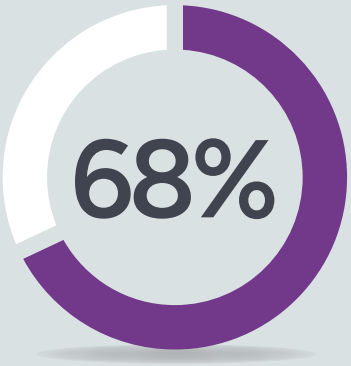
Higher education institutions hold some of the most sensitive data of any sector – student financial records, health information, research IP, and personal identifiers for tens of thousands of people. At the same time, cybersecurity threats are growing at an alarming rate, enrollment competition is intensifying, and students – ready to start their new experiences – arrive on campus expecting instant, frictionless, and personalized digital experiences. Meanwhile, administrators are asked to meet all of these demands while keeping costs under control and sensitive data secure.

The campus ID program touches all of it. It's the mechanism through which institutions first establish trust with a new student, the credential that authenticates thousands of daily interactions, and the entry point that bad actors probe when looking for weaknesses.

Entrust brings together three integrated capabilities – ID Issuance, Authentication for Secure Transactions, and Secure Monitoring and Cryptographic Security – to help institutions issue trusted credentials, authenticate every interaction, and maintain visibility and control across their entire environment. The result is a campus that earns student trust from day one and keeps it.

$3.8M

Average cost of a data breach in education[1]



Of breaches involve a human element, such as errors or falling for social engineering.[2]

57%->36%

American confidence in higher education has dropped sharply. Protecting student data is how institutions rebuild that trust.[3]

1. 2025 IBM Cost of a Data Breach Report
2. 2024 Verizon DBIR
3. EDUCAUSE Review Top 10, 2025

The Data Risk Facing Higher Education

Higher education holds some of the most valuable data a cybercriminal could want, and the sector pays for it. Institutions face nearly 2,300 cyberattacks per week, with the highest vulnerabilities and lowest readiness of any industry when it comes to identifying and remediating threats.[4]

A successful cyberattack can shut down campus operations for days, trigger regulatory penalties under FERPA, HIPAA, and GLBA, and cause reputational damage. For many institutions, the challenge is compounded by tight budgets, staffing shortages, and legacy infrastructure that was never designed for today's threats.

Beyond the threat itself lies another layer of difficulty – the complexity of the campus environment. A university must manage identity and access for a constantly rotating population – new students every semester, visiting researchers, contractors, part-time faculty, and thousands of staff – each with different access rights and risk profiles. And unlike most industries, higher education operates on open, collaborative networks that were built for the free flow of information and not for the security demands they now face. That openness, while necessary to academic culture, creates vulnerabilities that are difficult to close without the right infrastructure in place.

Students feel the impact too. Long lines at the ID office, multiple cards for different services, and slow access processes indicate that an institution is behind, and those signals matter.

The Entrust Campus ID program is built to meet every one of these challenges.

4. EDUCAUSE Review, Cybersecurity in Higher Education: Don't Let the Hackers Win, May 2024

Entrust Solutions for Higher Education

Research shows that students with a great onboarding experience are 35 times more likely to enjoy their overall university experience, and there is a 73% correlation between onboarding satisfaction and long-term institutional loyalty.[5] For today's students, a personalized campus ID is an expectation. It's often the first tangible thing a new student receives from their institution, so getting it right from day one builds the relationship that keeps them enrolled.

Entrust addresses the full spectrum of campus identity and security needs through three integrated solutions. Each is designed to work independently or as part of a comprehensive program, giving institutions the flexibility to modernize at their own pace.

Trusted Credentials, Delivered at Scale

Entrust issuance solutions replace centralized, line-forming card production. Staff can capture student photos and data from any secured device on campus and print cards at multiple locations simultaneously.

Highly personalized and incredibly durable cards, with full-color design imaging and institutional branding, give students an ID that reflects their identity. And with support for Apple Wallet and Google Pay, institutions can provision digital credentials from the same platform, giving students the option to carry their ID on their phone.

Authentication: Verify Every Identity, Secure Every Interaction

From dorm access to high-value research systems, every campus interaction requires reliable and secure identity verification. Entrust supports multi-factor authentication (MFA), smart card-based access, and contactless NFC technology, all while enabling fast, secure authentication across every physical and digital touchpoint without friction for legitimate users.

For privileged access to sensitive administrative systems, step-up authentication ensures the right controls are in place, aligned with NIST frameworks and Zero Trust principles.

Secure Monitoring and Cryptographic Security Platforms (CSPs)

Entrust remote monitoring and management (RMM) software gives institutions real-time visibility across their entire ID issuance infrastructure, such as printer fleet health, firmware updates, certificate lifecycles, error codes, and supply levels – all from a single dashboard. Certificate lifecycle management (CLM) automates the discovery, renewal, and revocation of digital certificates, eliminating an often overlooked vulnerability in campus IT infrastructure.

For institutions handling sensitive research data, financial transactions, or federally regulated information, Entrust Hardware Security Modules (HSMs) provide the cryptographic root of trust that protects the keys that protect everything else. FIPS-compliant and tamper-resistant, Entrust HSMs meet the requirements of GLBA, FERPA, and NIST 800-171.

5. Salesforce Connected Student Report, Third Edition, 2022

Building the Campus Your Students Can Trust

Higher education is under pressure from many directions, and the institutions getting it right are starting with identity.

Entrust gives institutions the tools to do just that: issue trusted physical and mobile credentials from a single platform, authenticate every campus interaction confidently across physical and digital touchpoints, and maintain the visibility and cryptographic security infrastructure needed for the complexity and compliance requirements of higher education.

Learn how Entrust can help your institution build a modern, secure campus identity program by visiting our **Campus and School ID Card Solutions page.**

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION