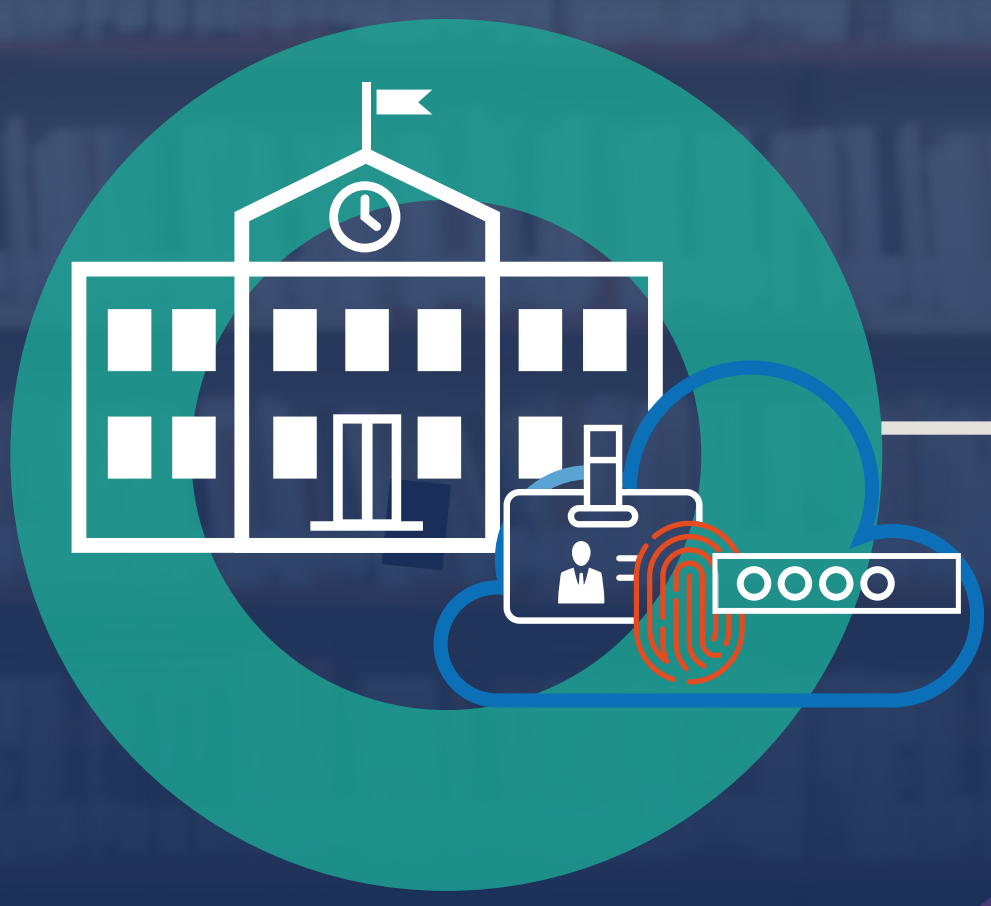
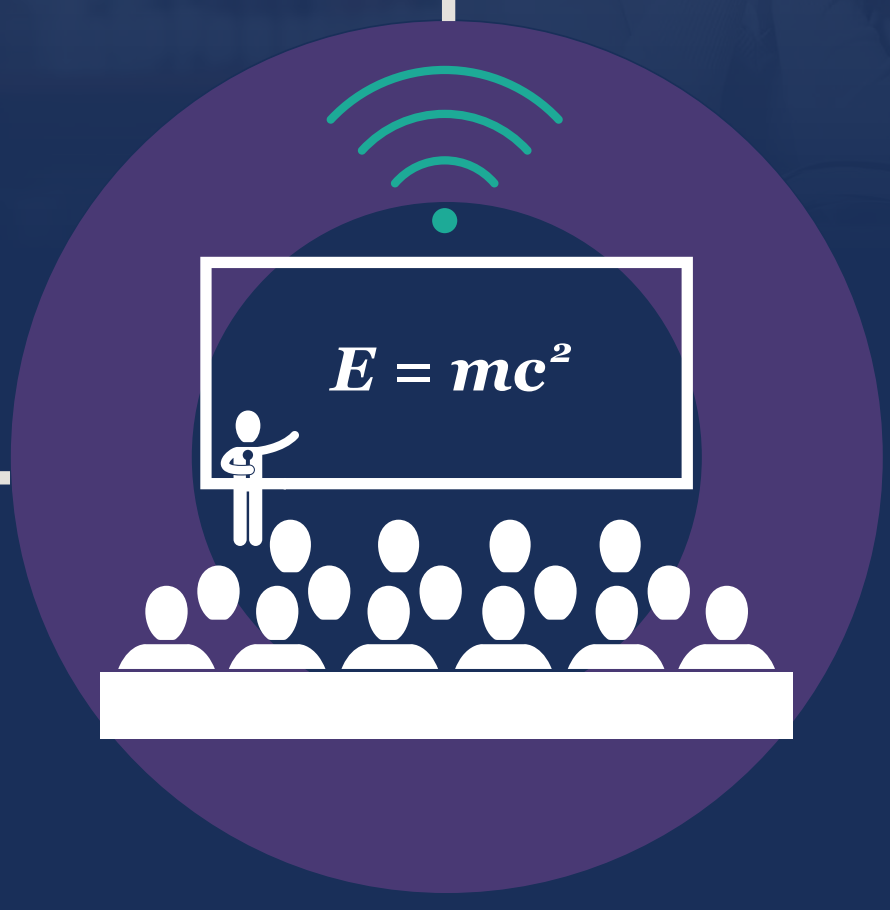
Testing and Validating Network Infrastructure and Security:

Identifying vulnerabilities and creating a plan



A private liberal arts and sciences university based in California faces the same IT security challenges that many higher education institutions must manage.



A significant issue is that **THE UNIVERSITY'S IT DEPARTMENT SERVES AS THE INTERNET SERVICE PROVIDER (ISP) FOR THE ENTIRE STUDENT BODY** over multiple campuses.

Another challenge is segmenting the student body from critical infrastructure that houses sensitive data. The university had implemented security features using its own IT staff, but wanted to test the current infrastructure to ensure the students and the school's assets were protected.

With this service, Optiv:

- Performed a network security assessment of IT assets and environments.
- Assessed current security posture compared with industry best practices.
- Identified vulnerabilities that could negatively affect the institution.
- Provided recommendations for remediation of any found issues.

Optiv's network security assessment services provided this client with many benefits, including:

Low-level risk:
found they have a low level of exposure with no current critical issues.

Identified third-party risk:
learned levels of risk for third-party vendor technology and how to remediate where possible.

Key findings:
received key findings and information on deficiencies and their implications.

Future plan:
determined short-term and long-term remediation goals to better secure data.

Learn more by downloading the Client Spotlight at www.optiv.com/resources/library or contacting references@optiv.com.