



CrowdStrike Customer Success Story



ASHLAND UNIVERSITY

INDUSTRY

Education

LOCATION/HQ

Ashland, Ohio

Ashland University Balances Academic Freedom with Rigorous Protection of Endpoints

Founded over 140 years ago, Ashland University empowers thousands of students to prepare for professions in a wide variety of careers through its award-winning bachelor, graduate and professional programs. As with many higher education institutions, Ashland University's dedication to enabling individual student success requires cultivating an environment of academic freedom while also ensuring protection of intellectual property, core services and systems.

To enhance the school's security posture and create a safe and open learning environment, Ashland University replaced its signature-based legacy solution with the CrowdStrike Falcon® platform in 2017. In less time than it took to remove the legacy solution, Ashland University implemented CrowdStrike agents on approximately 2,000 endpoints. With immediate, easily accessible visibility across its environment and access to intelligence on emerging threats, the private college can detect and respond to all types of malware in real time. The use of automated agent updates streamlines management of the CrowdStrike deployment and continually fortifies Ashland University against any attacks targeting its campus community.

INDUSTRY CHALLENGES

- The legacy solution relied on signature-based algorithms and did not provide an effective method for identifying unknown malware and other types of potential threats.
- Diminishing visibility and control over the increasing number of personal devices being used by students and staff escalated security risks.
- In contrast to business environments where internet access can be heavily controlled, educational institutions are expected to deliver open, unrestricted access to students to afford academic freedom, while maintaining a safe and secure environment for the campus community.

BUSINESS OUTCOMES

- Automated updates to on- and off-campus endpoints deliver immediate protection against emerging threats.
- The intuitive Falcon interface enhances speed and effectiveness when investigating new incidents.
- Cloud architecture enables collaboration with all organizations using CrowdStrike, which improves Ashland University's ability to detect and respond to any suspicious activity.
- High-fidelity telemetry provided by the CrowdStrike Threat Graph® database detected and prevented a zero-day attack within 12 hours of its appearance in the wild.
- The security team was able to use the Falcon platform to identify and mitigate an unprotected endpoint that was infected with malware and attempting to become a command control machine for other computers in the environment.

“We’re part of the global collection of organizations using the CrowdStrike Falcon platform and through the exchange of intelligence, we’re all effectively cooperating on security. If any of us detects suspicious behavior, CrowdStrike analyzes the threat and propagates preventative controls to everyone.”

Scott Stoops

Security Analyst Engineer
Ashland University

SOLUTION

The CrowdStrike Falcon® platform provides Ashland University with the balance needed to support an open learning environment while also ensuring core services and systems remain secure.

CROWDSTRIKE PRODUCTS

- Falcon Discover™ IT hygiene
- Falcon Insight™ endpoint detection and response (EDR)
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus



we stop breaches

