



CASE STUDY



ASHLAND UNIVERSITY SELECTS WEBDEFEND® AS CRITICAL COMPONENT IN OVERALL THREAT MITIGATION AND EVENT CORRELATION MODEL

ABOUT BREACH SECURITY

Breach Security, Inc. is the leading provider of real-time, continuous web application integrity, security and compliance that protects sensitive web-based information. Breach Security's products protect web applications from hacking attacks and data leakage and ensure applications operate as intended. The company's products are trusted by thousands of organizations around the world, including leaders in finance, healthcare, ecommerce, travel and government.

"We had WebDefend plugged into the network and watching traffic within a couple of hours. The set-up for an appliance of this caliber is highly intuitive,"

– **Mark Usher**
Network Analyst
Ashland University

ABOUT ASHLAND UNIVERSITY

Ashland University is a mid-sized regional teaching university, historically related to the Brethren Church. Their mission is to serve the educational needs of all students -- undergraduate and graduate, traditional and non-traditional, full and part-time -- by providing educational programs of high quality in an environment that is both challenging and supportive.

As a teaching university, Ashland University serves the educational needs of all students – undergraduate and graduate, traditional and non-traditional, full and part-time – by providing educational programs of high quality in an environment that is both challenging and supportive. The Princeton Review named Ashland University as a "Best in the Midwest" university for 2009. In addition, U.S. News and World Report placed Ashland University in the top tier of Midwest institutions in the new edition of U.S. News and World Report's America's Best Colleges survey.

The university sought a web application firewall (WAF) as part of its overall threat mitigation and event correlation model. After evaluating several appliances, Ashland decided on Breach Security's WebDefend for its feature set, including host-based agents, application profiling and defect detection, extensive reporting, and granular policy management. In addition, the university was impressed by WebDefend's intuitive interface, which was highly important in their decision, as well as the device's flexible deployment options, benchmarking and positive reviews.

Other key components in Ashland's decision to use WebDefend include Breach Security's direct involvement in open source development, recognized expertise in the web security community, and knowledgeable and accessible sales and service staff. Lastly, Ashland knew of colleagues at other institutions who had already deployed WebDefend and were happy with the product.

"We had WebDefend plugged into the network and watching traffic within a couple of hours. The set-up for an appliance of this caliber is highly intuitive," said Mark Usher, network analyst for Ashland University. "WebDefend's ease of deployment and management were outstanding product features, which was a nice surprise."

During the initial WebDefend assessment at Ashland, the product immediately started logging numerous SQL injection attempts, content spam and other untrustworthy traffic making connection with a couple of the university's sites that were running blogs and client applications. Ashland now has WebDefend deployed out of band, watching 13 different sites averaging 18,000 visits per day, and configured to block unwanted traffic either via a host-based web agent or TCP resets. The product's extensive site profiling and application defect reporting has also aided the university's web development team in cleaning up security holes and broken links.

"WebDefend offers its clients a thorough policy set, site profile learning, event detection and blocking capabilities. Of the traffic WebDefend tags as critical, 98 percent is unwanted traffic – any remaining potential 'false positive' traffic is usually a result of application errors," said Usher. "WebDefend serves as a great tool to aid an organization in application assessment and reduction of vulnerabilities and threats."