SHIELDX

CASE STUDY

APEIRO™ + Iowa State University

Multi-cloud threat visibility on demand and within budget

INDUSTRY

- Higher Education

PROFILE

- On-premises, VMware vSphere 6.5 private cloud
- Planning expansion to Amazon Web Services® (AWS)
- On-demand, rapidly changing network
- Advanced practitioners conducting red-blue team exercises

WHY SHIELDX

- Industry-recognized, state-of-the-art multi-cloud security
- In-depth visibility and reporting
- Advanced security controls
- Security-on-demand, consumption-based model
- Flexible, low-cost infrastructure footprint

Gartner Cool Vendor 2017™

"APEIRO is the only multi-cloud security solution that could meet all of our requirements. ISU students now hone their skills using state-of-the-art security and we didn't have to make any unwanted compromises between threat visibility, scalability and cost."

IOWA STATE UNIVERSITY

Dr. Doug Jacobson

Director ISU Information Assurance Center and University Professor of Electrical and Computer Engineering

IOWA STATE UNIVERSITY ENTERS THE ISEAGE

Iowa State University (ISU) enrolls over 35,000 students annually with an internationally-recognized under-graduate and graduate program in cybersecurity. Leading with education best practices to help address the worldwide cybersecurity skills gap, the ISU Information Assurance Center has developed a curriculum that prepares its cybersecurity students for successful careers through interactive, real-world learning opportunities.

Through its signature ISEAGE cyber defense competitions, ISU students pit their skills and knowledge as "blue teams" to identify and defend against attacks initiated by seasoned cybersecurity "red teams." This exercise allows students to practice within an environment that simulates a large-scale, modern IT network laden with today's most advanced attacks initiated by the industry's top professionals.

THE GOAL

To prepare students for the real world, they must learn security in a changing landscape of regulation and cloud-based services, applications, and architectures that provide rich targets for attacks, especially attacks propagated laterally. These attacks can be difficult to stop using traditional network defenses designed for just perimeter security and access control. And they can be even more difficult to detect. Security practitioners need new solutions built specifically for the cloud to gain the visibility and intelligence required to accurately identify and detect breaches and then prevent or stop compromise in progress before it can shut down services, steal assets, expose data, or impact careers.

ISU wanted to provide its advanced students with a hands-on learning experience using a state-of-the-art multi-cloud security solution. To succeed in their mission, they needed to:

- Automatically identify and track suspicious behaviors inline and in real-time during ISEAGE competitions
- Provide a benchmark of student performance
- Deliver instructive insights into the forms of attacks perpetrated during the competition
- Help students understand the shortcomings of manual defenses in contrast to emerging automation, orchestration, and machine learning-based solutions
- Allow graduate students enrolled in the ISU "Information Warfare" course to visualize simulated cloud attacks they create

REQUIREMENTS

- Deep Packet Inspection (DPI)
- Comprehensive visibility
- Next-gen security and micro-segmentation for graduate learning
- Elastic scale for bursty, east-west traffic
- Identify compromises early in the kill chain
- Advanced intelligence for analysis
- Logging and reporting for audit and forensics
- Security-on-demand for fast turn-up and off
- Operate over commodity hardware to contain costs
- Consumption-based model to align with OpEx budget

RESULTS

- Faculty and student post-mortem analysis with in-depth reporting
- Real-time insight from ShieldX Indicator-of-Pivot (IoP) technology
- Lab learning from advanced tool set
- Program expansion readiness from platform flexibility
- Industry recognition as a 2018 SC Media Award Finalist

SC 2018 awards finalist

Contact Us
ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110

+1 408-758-9400
info@shieldx.com

www.shieldx.com

THE CHALLENGE

ISU constructed its lab and competition environment using VMware vSphere 6.5, with a future plan to expand to a public cloud, like AWS®. The problem ISU faced was finding a multi-cloud security solution capable of:

- Spanning multiple environments without vendor lock-in
- Having full, DPI-enabled visibility to monitor and report on activities during the competition
- Offering advanced security and scale for students, yet available on demand with a containable footprint and cost, practical for an academic institution

ISU naturally looked to software-based solutions for their flexibility and cost savings. They considered using virtual appliance or agent-based technologies, but both fell short of meeting these requirements. Network security appliances offered visibility but were resource-intensive and out-of-budget and could potentially cause undesirable performance issues. Alternative, agent-based approaches lacked the required network visibility and created operational challenges that would redirect the purpose of the competition from identifying threats to learning how to manage security operations and thus, were the wrong fit.

THE SOLUTION

ShieldX and its Certified VMware-Ready®, APEIRO was chosen because it offers the DPI and visibility expected of an enterprise-class security system while aligning perfectly with the ISU Information Assurance Center's infrastructure and budget requirements. APEIRO works natively and uniformly at scale and across environments—avoiding lock-in and without forcing unacceptable trade-offs between security, cost, and performance. ISU felt confident in the solution's ability to automate security insertion, orchestration, and inspection elastically to support competitions on their current VMware vSphere environment or future expansion to AWS or other popular virtualized environments if and when the department is ready.

In addition, APEIRO is true Software-Defined Security built on a containerized, microservices-based architecture. The Virtual Chassis dynamically inserts, orchestrates, and elastically scales out across their vSphere environment according to the security intent, constraints, and policies configured by ISU and their students. Beyond providing real-time security, insight, and analytics for their competitions, APEIRO offers ISU students an excellent example and learning opportunity with a state-of-the-art, multi-cloud security solution that their future employers will employ to protect their critical infrastructure and information.

THE SUCCESS

As planned, APEIRO easily installed and transparently inserted into their vCenter segments during the competition, collecting, monitoring, and analyzing the traffic and attack data within the resources allocated by the department. Using APEIRO and its IoP technology, the faculty has gained the in-depth visibility they need to evaluate their students' performance. They succeeded in their goals while keeping costs contained due to the APEIRO automation, self-orchestration, and lower infrastructure resource requirements.

As a teaching tool, ISEAGE participants can use the data captured by APEIRO to see trends in lateral traffic, its flows, and threats post-competition. From these exercises, ISU students can witness firsthand the importance of industry and academia collaboration and how cybersecurity professionals use automation, machine learning, and advanced security controls to detect and stop evolving cyber threats.

LEARN MORE

Contact us at www.shieldx.com to hear more about APEIRO or engage us on your unique mission to protect your organization. We're here to help.