Forcepoint

Customer Story

Liberty University Secures Data at Scale to Safeguard AI Innovation

Liberty University operates far beyond the scope of a traditional academic institution. It has more than 140,000 residential and online learners across every time zone, a 7,000-acre campus and the operational complexity of a hospital, airport, law firm, financial services, and Division I athletics. Liberty University functions as a global digital city, while still maintaining an open academic environment.

Protecting such a vast, hybrid ecosystem falls to Brian Johnson, Director of IT Security. A former U.S. Army military intelligence officer who later led advanced cyber and opensource intelligence programs in the defense sector, Brian oversees a 16-person cybersecurity team responsible for protecting Liberty's most sensitive assets including, student records, financial aid data, and PCI payment information.

Early in his tenure working in security, Johnson experienced a DDoS attack that revealed critical gaps in data visibility and has since served as a turning point in Liberty's modernization journey. What has come of this is a deliberate, data-first transformation made possible with Forcepoint Data Security Posture Management (DSPM) and Data Security Everywhere approach.

LIBERTY UNIVERSITY

Customer Profile:

- Liberty University is a major higher education institution with more than 140,000 learners across every time zone. Its mission-focused, open academic environment requires a security posture capable of protecting diverse, highly sensitive data at massive scale.

Industry:

- Education

HQ Country:

- Virginia

Product(s):

- **Forcepoint Data Security Posture Management (DSPM)**

The Challenge: Limited Visibility, Manual Processes, and AI Driven Risk

Shortly after stepping into his role, Johnson encountered a major DDoS incident that exposed a fundamental problem: **"Getting visibility is really key to being able to sleep at night,"** he recalls. Without end-to-end insight into systems, users and data, his team couldn't effectively defend the environment, let alone prepare for future threats.

Data sprawl from decades of modernization

When shifting workloads across on-prem and cloud systems, organizations face substantial challenges such as:

Duplicated and inconsistent data stores

- → Dark data accumulated over time
- → Little clarity into where sensitive information lived
- → Misalignment between technical ownership and data usage

Similarly, other higher-ed institutions have even abandoned audits after discovering they couldn't locate their sensitive data, which is a cautionary tale Liberty was determined not to repeat.

Coming from a defense background, Johnson initially found manual classification intuitive, but it quickly became clear it wouldn't work at Liberty.

Misclassification was common, since most users lacked the context to label data accurately. The constant prompts frustrated faculty and staff, interrupting their daily workflow and limiting compliance. It also slowed everyday productivity, forcing people to make security decisions they weren't trained for.

Ultimately, the approach simply couldn't scale across an environment as large and dynamic as Liberty's. As Johnson put it: **"Users are not going to embrace having to label and classify every email they send... That's not normal."**

As AI adoption accelerated across campus among professors, students, researchers and operational staff, new risks quickly emerged.

Liberty began encountering locally hosted models with unclear data flows, instances of shadow AI operating outside central IT oversight and situations where mislabeled or sensitive data could inadvertently enter training models. Even internet-connected AI tools posed a threat, often sitting just one prompt away from unintended disclosure.

Johnson emphasized that misclassification, whether human or automated, could have dangerous consequences if sensitive data inadvertently fed into AI systems.

The Solution: A Data-First Strategy with Forcepoint DSPM

Brian aligned Liberty's transformation with Forcepoint's Data Security Everywhere framework:

1. **Discover:** Locate all sensitive data across on-prem and cloud
2. **Classify:** Automatically contextualize file severity
3. **Prioritize:** Identify what data matters most
4. **Remediate:** Apply controls to prevent inappropriate access or movement
5. **Monitor continuously:** Detect drift, misconfigurations, and new risks

> Forcepoint's data security everywhere approach... meshes really well with my approach and Liberty's approach to data security."
>
> **Brian Johnson**

Forcepoint replaced Liberty's unscalable, user driven labeling model with automated, intelligence driven discovery and classification with Forcepoint Data Security Posture Management.

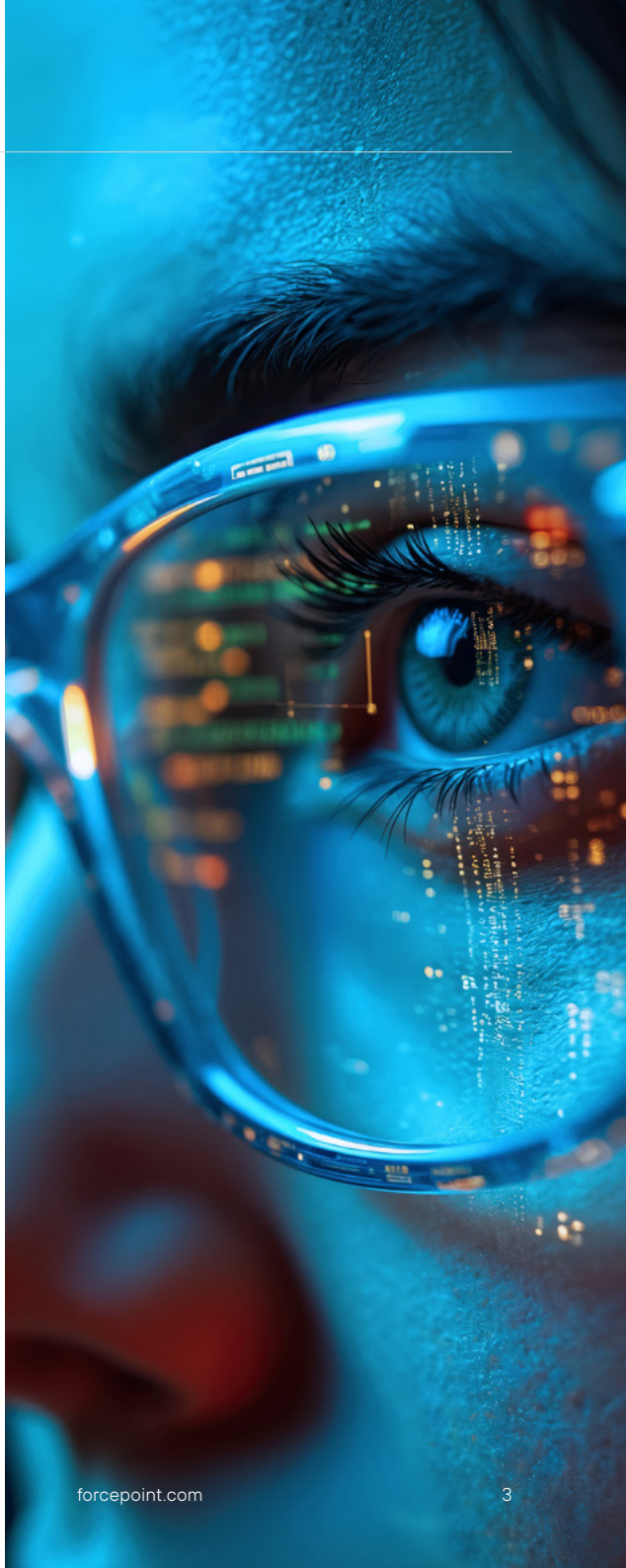
By embedding this capability directly into the university's data flows, Liberty was able to reduce misclassification, minimize the burden on users and improve the overall accuracy and consistency of its data handling practices.

This shift also created a stronger foundation for future AI governance, ensuring that sensitive information is correctly identified before it ever enters an AI workflow. Together, these advancements allowed the security program to scale significantly without disrupting academic or administrative operations.

To complement its improved visibility, Brian recognized the need to layer in DLP alongside real time alerting and reporting, controls he described as essential to preventing sensitive data from being shared, stored, or transmitted inappropriately.

Knowing where data lives was only the first step. Liberty also needed the ability to prevent sensitive information from being shared, stored, or transmitted improperly, and to spot hygiene issues the moment they occurred.

Together, the solutions provided the team with actionable insights to prioritize the most critical incidents, strengthening their ability to respond quickly and effectively. As Johnson emphasized, **"it is essential to 'layer in DLP' on top of posture management to reinforce prevention in real time and keep sensitive data from slipping through the cracks."**



AI-Aware Governance and Shadow AI Prevention

Forcepoint's data-first model positioned Johnson's security team as an active stakeholder in AI initiatives.

With central IT visibility, Johnson's team is better positioned to:

- → Review all proposed AI models and locally hosted systems
- → Validate data pathways and internet egress
- → Identify sensitive data before it enters a model
- → Ensure research teams aren't training models in the dark

This governance framework supports innovation without compromising privacy or compliance.

The Results: Authoritative Data Visibility, AI-Ready Controls and a Culture Shift

With Forcepoint DSPM, Liberty University now has a single source of truth for where its sensitive data resides and how it moves across the network, which is an essential foundation for compliance, AI governance and overall cyber resilience. This clarity allows Johnson and his team to understand their data landscape with a level of confidence that simply wasn't possible before.

A major advantage of this transformation has been the reduction of friction in productivity across the university. By shifting classification away from manual user workflows and toward automated, behind-the-scenes intelligence, Liberty significantly improved accuracy, reduced false positives and removed both the operational burden and user frustration that had plagued earlier labeling efforts. Staff no longer wrestle with constant classification prompts, and the security team now benefits from cleaner, more consistent signals. Overall, the shift has notably increased user satisfaction and strengthened trust in the security program.

With safer and more accelerated AI adoption, Liberty University continues to strengthen its foundation for responsible, scalable use of AI across the institution:

- → Security collaborates with academic and research teams
- → Sensitive data stays out of unauthorized models
- → Internet connected AI systems are scrutinized before deployment
- → Shadow AI risks are mitigated

Perhaps most importantly, these advancements have enabled a cultural shift. Johnson's team has evolved from perceived gatekeepers into strategic partners who help the university innovate faster and more safely. As he explains,

"Don't be the Department of No... We work every day to be ambassadors, partners and protectors without breaking the business."