Bluefin®

Defending Campus Data: Cybersecurity and Compliance Strategies for Higher Education

2025

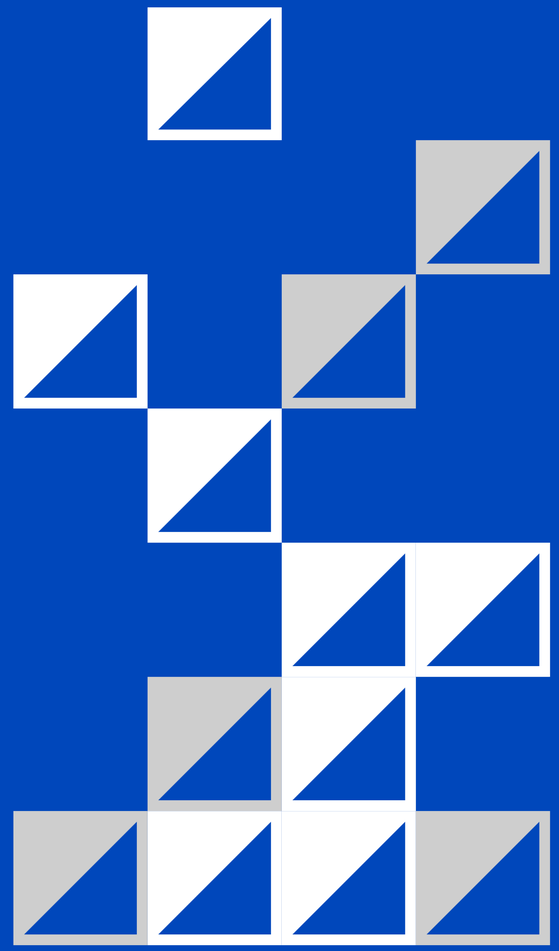
Welcome & Agenda

Housekeeping

- Webinar duration / Questions / Recording

Today’s Agenda

- The threat landscape in higher education
- Vulnerable data & compliance
- Security strategies & technologies
- Actionable next steps



Your Presenters

Terry Ford
SVP Strategic Partnerships
Bluefin

Pete Campbell
CISA, CISSP, CMMC RP, QSA
Manager, Security Advisor
Services & PCI Practice Lead
CampusGuard

Ruston Miles
Founder & Chief
Strategy Officer
Bluefin

Why Higher Education is a Prime Target for Hackers

- Decentralized IT and campus-wide sensitive data
- Heavy reliance on third-party vendors and cloud services
- Delayed breach detection and slow response
- Exposure of PII/PHI via email and system errors
- Insufficient IT staffing and frequent account turnover
- Human and insider threats (phishing, credential abuse)
- Inadequate patch management

70%
Was the increase in ransomware attacks on higher education in 2023

265
Ransomware attacks in higher education were reported in 2023

66%
Of educational facilities reported cyberattacks in 2024

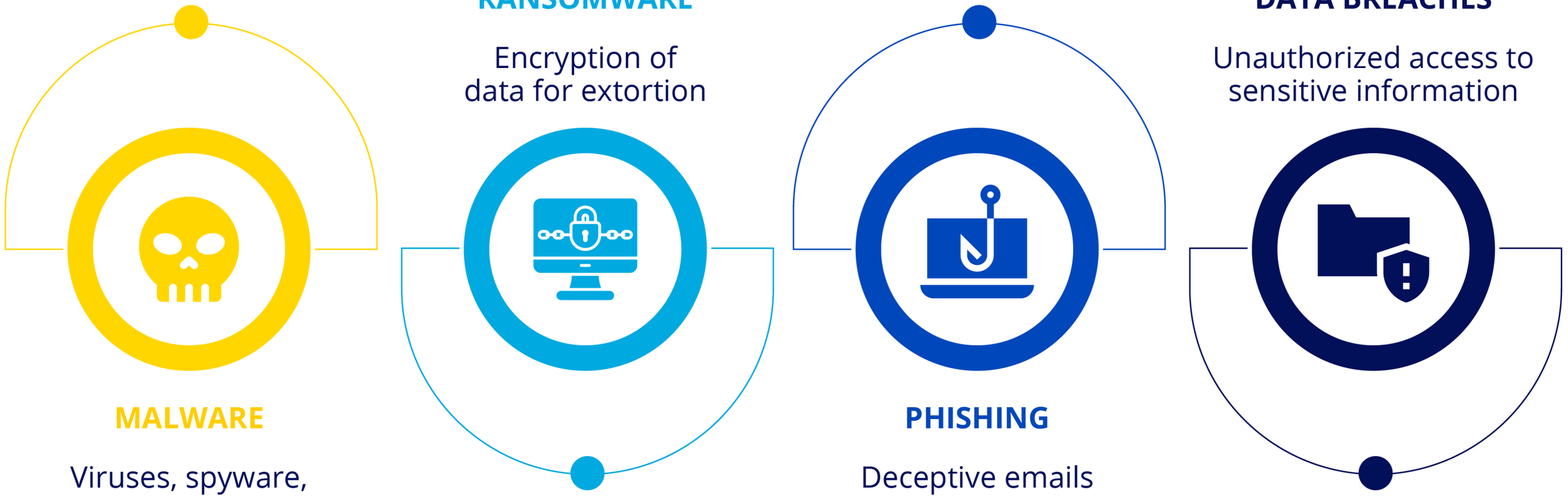
$4.88M
Was the average cost of a data breach in Higher Ed in 2024

4.8 months
Was the average time it took for Higher Ed to report attacks

92%
Of attacks against higher education were financially motivated

Top Threats in Higher Education

U.S. universities have large attack surfaces, averaging 244 domains each



What Can an Attack Surface Look Like?

What Needs Protection – and Where

Sensitive data types

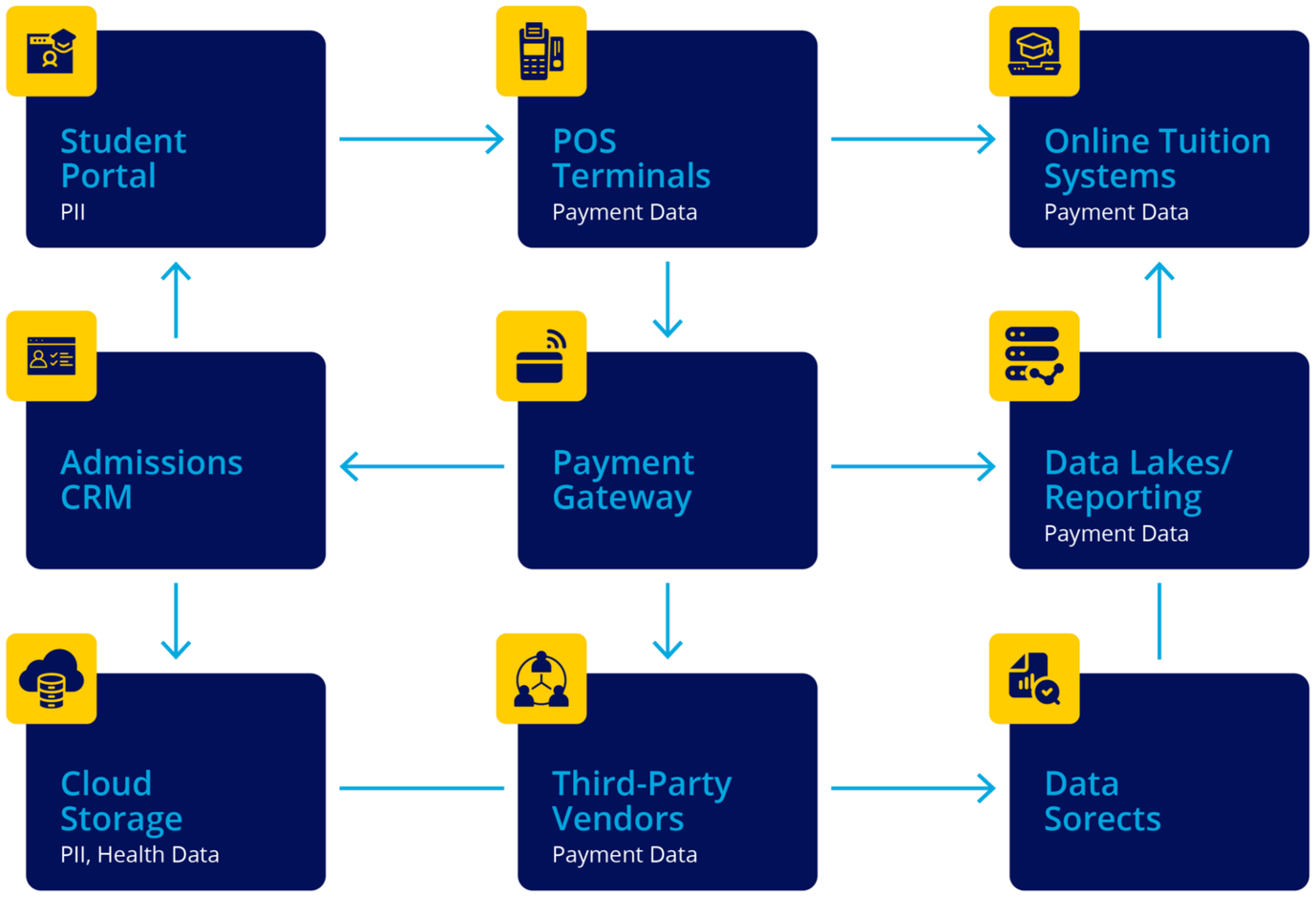
- Payment (tuition, donations)
- PII (student, alumni, faculty)
- PHI (counseling, health services)

Sensitive data type flow

- Intake
- Transmission
- Storage

Where it flows

- Admission portals
- Payment systems
- Learning Management Systems, CRMs, cloud storage



Compliance and Regulatory Pressures

Non-compliance = financial and reputational damage

PCI DSS 4.0

P2PE and scope reduction = Smart Security Strategy

- These measures free up your FTEs/budget, allowing you to focus resources where they matter most.

Attackers don't care about your scope – they care about access.

- Focus on layered defenses
- Overall information security
- PCI DSS provides a solid baseline; don't overlook essential controls just because they’re not required, including:

Asset Inventory: Know what you have and where it is in order to protect it.

Network and Data Flow Diagrams: Understand where data moves and where it’s exposed.

Pen Testing and Vulnerability Scans: Identify and fix weaknesses before attackers do

Other Regulations

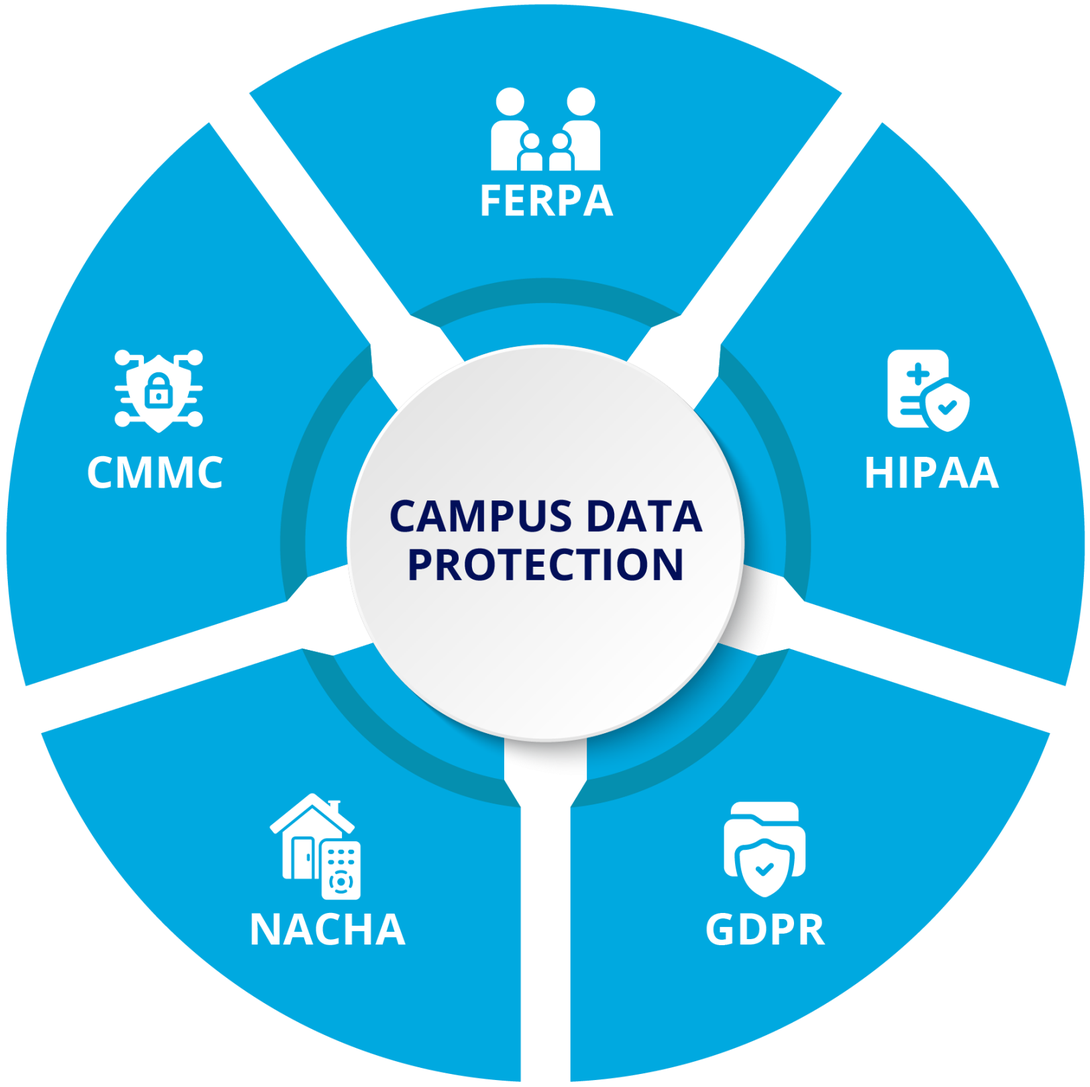
PCI DSS could be a starting point

- Many of its controls align with other broader security frameworks and can support compliance across multiple standards

Most institutions also face:

- HIPAA
- Nacha
- CMMC (if engaged in research)
- GDPR is potentially applicable
- FERPA
- GLBA

Cross-framework references are available; consider NIST CSF or CIS as overall baselines



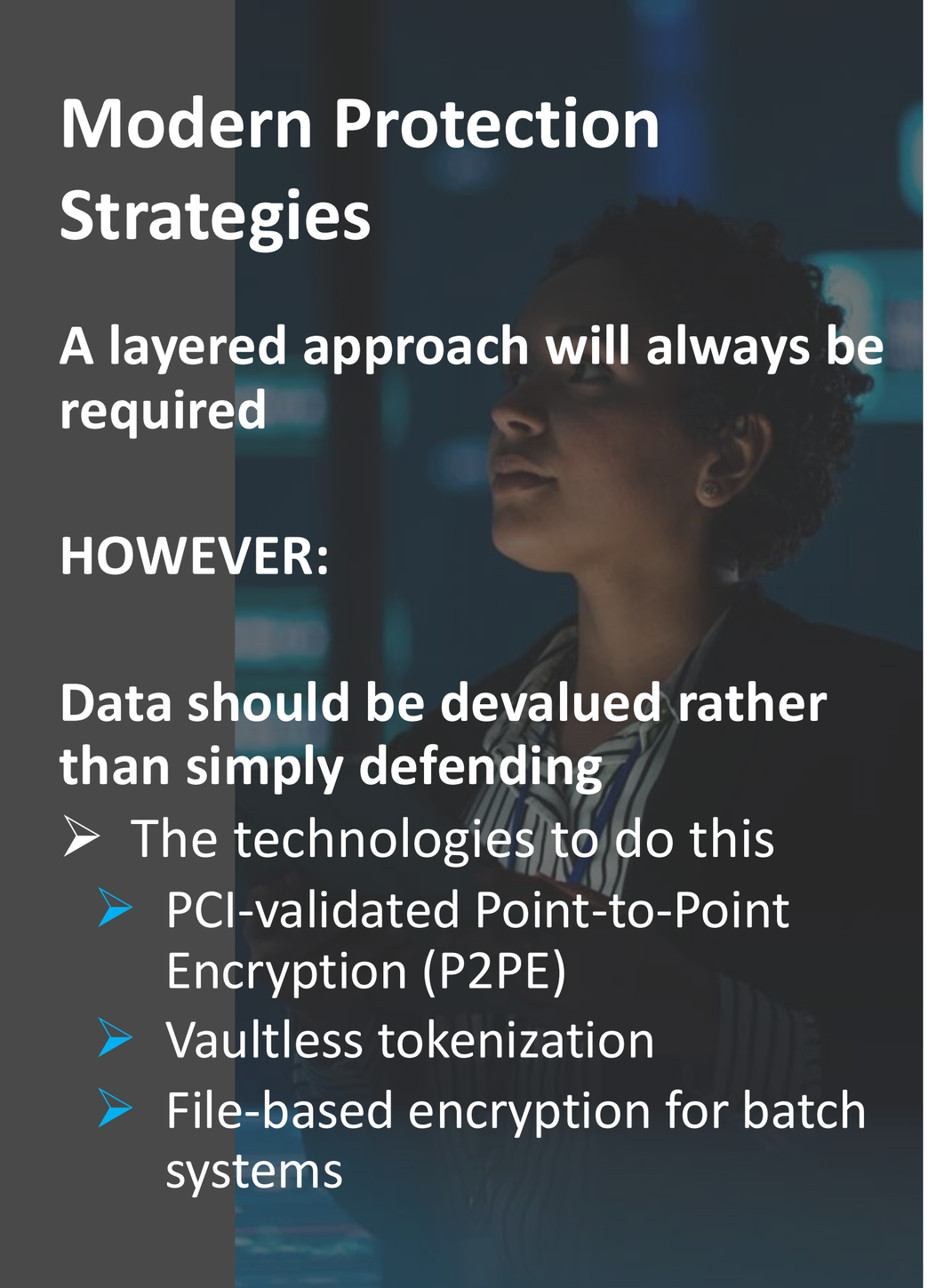
Modern Protection Strategies

A layered approach will always be required

HOWEVER:

Data should be devalued rather than simply defending

- The technologies to do this
  - PCI-validated Point-to-Point Encryption (P2PE)
  - Vaultless tokenization
  - File-based encryption for batch systems



Network Security

Endpoint Security

Identity & Access Management

Data Security

Understanding Today's Security Technologies

PCI-Validated P2PE

- Encrypts cardholder data at the exact point of capture (e.g., readers, terminals)
- Keeps data secure until it reaches Bluefin's PCI-validated decryption environment
- Significantly reduces PCI DSS scope for campus merchants
- Ideal for dining halls, bookstores, ticketing, and payment kiosks.

Vaultless Tokenization

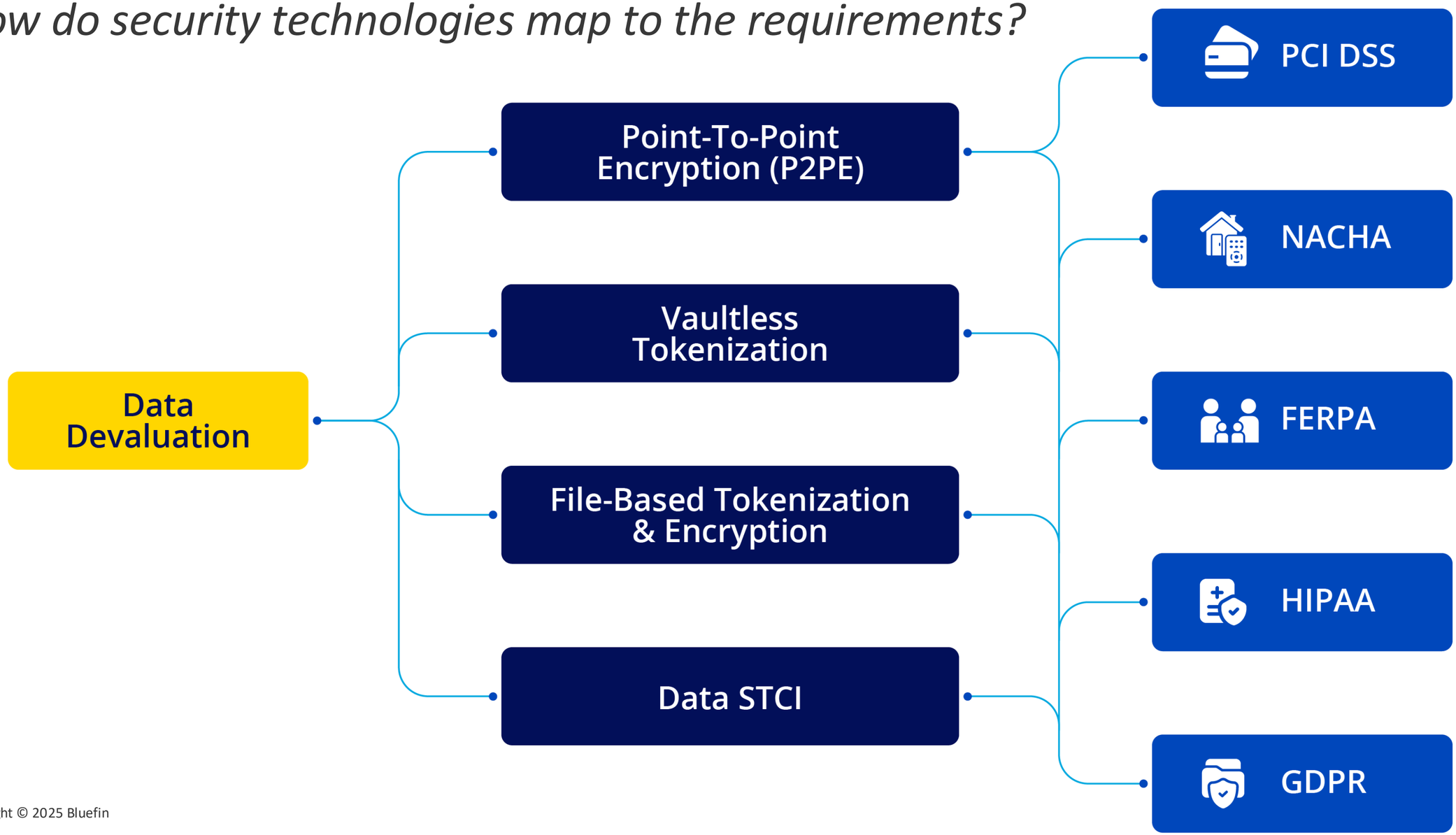
- No central vault—nothing to breach or maintain
- Format-preserving tokens easily integrate with legacy systems
- Secures sensitive data fields like student ID, SSN, and bank info
- Supports secure workflows across admissions, healthcare, and student services

File Based Protection

- Secures data with tokenization / encryption in batch files: ACH, financial aid, donor exports
- Protects sensitive info during SFTP or other file-based transfers
- Works with both legacy and cloud platforms (e.g., Ellucian, Workday)
- Critical for institutions using FTP workflows or scheduled exports

Data Devaluation and Compliance

How do security technologies map to the requirements?



The Campus Environment: The Blueprint for Protection

Endpoint P2PE Devices

- Bookstore, Dining Hall, Ticketing, Kiosk, Tuition Portal, & More
- Bluefin Device Partners

Decryptx & PCI-Validated P2PE

POS / Payment Gateway

- Campus Transaction Systems
- Bluefin Partner Gateways, ISVs, & POS

PayConex

Tokenization Engine

- Campus Platforms
- ERP, SIS, & CRM
- Secures PII, PHI, & PAN across student systems without redesign

ShieldConex

Cloud / Storage

- Data at Rest & Batch Processing
- Secure exports like tuition files, ACH, & donor

File-Based Processing Subsystem

Bluefin + Partners = Trusted Protection

Integrated and vendor-agnostic solutions to protect data campus-wide

Key Takeaways

- Higher ed is a growing target for cyberattacks.
- It’s not just payments: student PII, alumni records, and ACH data are at risk.
- Proven tools like P2PE, vaultless tokenization, and file protection are critical for security *and* compliance.
- Devaluing data makes breaches worthless to attackers.
- You’re not alone - Bluefin and our partners can help you build a resilient, future-ready campus.

16

Next Steps / Resources

Next Webinar: Understanding Nacha Compliance in Higher Education

Ruth Harpool, AAP, APRP, CTP
Treasury Solutions Advisor at CampusGuard and Co-Founder of The Payments Academy

Ruston Miles
Founder & Chief Strategy Officer
Bluefin

Resources / Downloads

https://www.bluefin.com/resources/webinars/education/

Solutions

P2PE / Tokenization / Secure Payments for Higher Ed
CampusGuard Compliance Services
Bluefin Partners

Guides / Studies

PCI DSS Compliance Guide & Quarterly Checklist
PCI Guidance for SAQ A Merchants on E-Skimming Attacks
Why SAQs Are Essential for PCI Compliance
SAQ A for E-Commerce: Deep Dive into Vulnerability Scanning
Bluefin / UCLA Case Study

Videos

How Bluefin is Securing the Future of Higher Education
How to Stop Data Breaches in 2025
PCI DSS Compliance: What to Know (Video Series)

Q&A / Thank You!

Terry Ford
SVP Strategic Partnerships
Bluefin

Pete Campbell
CISA, CISSP, CMMC RP, QSA
Manager, Security Advisor
Services & PCI Practice Lead
CampusGuard

Ruston Miles
Founder & Chief
Strategy Officer
Bluefin