

# Proofpoint Solution Brief for Educational Institutions

## Proofpoint Messaging Security and Data Loss Prevention Solutions



The business of education presents unique challenges to the multi-tasking IT administrator who supports a complex IT infrastructure while meeting the requirements of very diverse user communities (faculty, students) and departments (Bursar's office, medical schools, traditional research and instruction, etc.). Email is core to the culture of information exchange and research, and university IT departments are tasked with fostering an environment for research and intellectual growth while, at the same time, managing email-related risks in many forms.

Proofpoint's email security and data loss prevention solutions defend against inbound messaging threats such as spam and viruses, outbound threats from infected or compromised machines and compliance/data protection risks. Technical controls for messaging security and easily modifiable templates for policy definition and reporting help IT managers to comply with industry regulations and create acceptable use policies with ease.

### security and compliance challenges in EDU

Proofpoint's higher education (EDU) customers have greatly benefited from our company's laser focus on email security—including Proofpoint MLX™ technology's unbeatable, 99%+ ongoing effectiveness against spam—without having to compromise their culture of open computing. Read on to see how the unique challenges of EDU are addressed by Proofpoint solutions for email security and data loss prevention.

Challenge for Educational Institutions	The Proofpoint Advantage
High spam volumes continue to grow and adversely impact productivity of students, faculty and staff	Highest anti-spam accuracy: Higher than 99% detection rate, lowest false positives Load-shedding: Throttling inbound email volume with dynamic reputation filters
Infected and vulnerable systems are a prime target for malware, botnets, virus outbreaks	Proven anti-virus technology: Choice of seamlessly integrated McAfee or F-Secure engines for signature-based detection Zero-Hour Anti-Virus Protection: Behavioral analysis for immediate response to the latest virus outbreaks
Limited IT resources, hard-to-use administrative interfaces	"Set it and forget it" administration: Automatic updates of anti-spam and AV signatures, unified management interface "No hassle" transition from your legacy anti-spam solution
Deployment needs fluctuate with user needs, making capacity planning difficult	Flexible deployment options: Appliance, hosted service, software, virtual appliance for VMWare
Open computing environments, less control over user systems	Outstanding end-user controls: Including end-user digests, email tag and forward features Policy education: End-user notification
Unique and complex compliance requirements for certain EDU organizations: FERPA, HIPAA, GLBA, PCI, and others	Simplified policy definition: Built-in templates, "smart identifiers" and codesets for common healthcare, financial, and privacy regulations Reporting: Built-in, customizable compliance-related reports
Limited time and resources to evaluate new vendors, often with no EDU experience	Dedicated focus on the EDU market: 100+ EDU customers, dedicated EDU account managers, EDU-friendly pricing

### Proofpoint's EDU Presence

- More than 100 EDU customers
- Deployments in educational institutions in 40 out of 50 states
- Half of the Ivy League universities
- Half of the Atlantic Coast Conference (ACC) schools
- 10 out of 24 of the largest City University of New York (CUNY) campuses (46% of all college students in NY attend a CUNY)
- 6 members of the Association of American Medical Colleges

#### Dramatic impact on spam

**"Proofpoint has made such an impact by cleaning up our inbound email and increasing user satisfaction as well as productivity. We are excited about using it for our outbound email and seeing similar stellar results."**

**Brian Cohen, CIO**  
The City of University of New York

**"Colleges and universities pride themselves on their open environments. They also take information security very seriously and have implemented bold steps to improve their practices. These steps are public, visible, and represent the best of higher education — bringing together technical experts, policy makers, and security researchers in colleges and universities, government, and industry."**

**Peter M. Siegel, CIO,**  
University of California at Davis  
and Co-chair of the EDUCAUSE/  
Internet2 Computer and Network  
Security Task Force

# Proofpoint Solution Brief for Educational Institutions

## EDU Concerns

All enterprises desire complete protection against threats to messaging infrastructure, but at what cost? Various factors exacerbate and contribute to the spam problem in educational institutions, including:

- Universities are prime targets for spam attacks, due to large number of email addresses in well-known domains
- Rapid evolution and increasing sophistication of spam attacks
- Non-English language speakers comprise a large part of student and faculty population—increasing traffic of foreign language spam
- Low effectiveness of many legacy anti-spam solutions used in EDU—open source, low-end, high-admin
- Restrictions on enforcing user behavior or securing desktop configurations, due to culture of open computing
- Students signing up on gaming or social networking sites—advertising their email addresses to spammers

### End User Digest and Controls

Give your users “do it yourself” control over their personalized spam quarantines and preferences. They can easily delete or release messages, report false-negatives, safe - or blacklist senders and much more.

- 1 Access multiple folders
- 2 Access to personal files
- 3 Message review
- 4 Column sort
- 5 Inbox view

**“Spam represents more than 90% of total email volume in educational institutions.”**

Proofpoint Analysis, Dec 2007

**“We were looking for a solution that did not need our constant upkeep to work effectively. Not only did we need a solution with stringent anti-spam and anti-virus capabilities, but we also needed the solution to have a comprehensive reporting system, automatic updates, an appealing Web interface and responsive technical support.”**

**Jeff Leisse**  
Manager of Web Applications  
La Salle University

## enemy #1: spam

### The Spam Challenge

The business of spam is all about harvesting valid email addresses, which in turn are used as the targets for spam campaigns. University environments usually support mail domains of thousands of users, providing spammers with a narrow target.

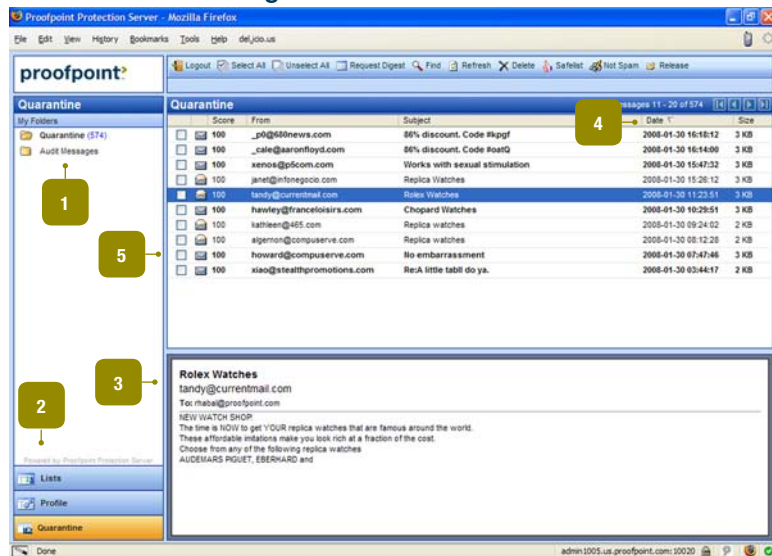
Spam attacks themselves are not static in their characteristics. Variants are being created continuously and sender IP addresses change constantly. Combine this with the latest spam techniques such as image-based spam, which randomizes images to bypass traditional filters, and most anti-spam solutions quickly become ineffective and obsolete.

EDU has traditionally embraced open source solutions for many IT requirements, but many such anti-spam solutions lack the sophistication to handle newer attacks. Furthermore, they often require constant administration and additional IT resources to keep spam and virus filters up-to-date, monitor performance and provision new anti-spam systems because of poorly-designed administrative interfaces and lack of scalability.

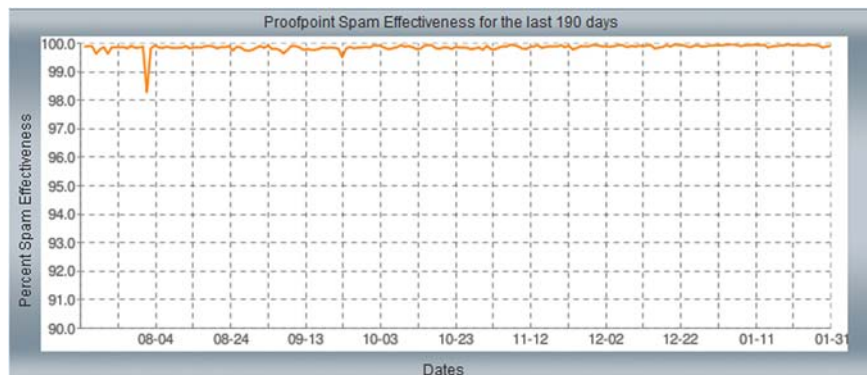
There is the additional challenge of balancing a culture of unrestricted computing with the responsibility of protecting users from spam and viruses. This often extends to monitoring spam and virus attacks launched from compromised EDU machines, impacting systems on the outside as well.

Add to this the permitted but risky user behaviors associated with the student population—such as signing up for social networking sites, gaming sites, news groups, and opt-ins for various online retail stores and you have an increased likelihood of potential spammers using these email addresses. And the cycle of spam continues.

### Personalized End-user Digests and Controls



### Proofpoint MLX Technology Delivers 99%+ Effectiveness Against Spam



# Proofpoint Solution Brief for Educational Institutions

## highest anti-spam accuracy

### Advanced Spam Detection, Powered by Proofpoint MLX

Who else can claim over a 99% detection rate, with the fewest false positives? Proofpoint has focused primarily on email security since its inception and has a dedicated research and development organization for spam research. The result of this research is patent-pending Proofpoint MLX machine learning technology, which uses advanced, “artificial intelligence” techniques to analyze hundreds of thousands of email attributes to decisively identify spam.

### Unique Combination of High-effectiveness and Low-overhead Administration

Proofpoint delivers numerous anti-spam benefits, including:

- **Detect and block high volumes of spam:** Gain performance and scalability at no additional cost, by dropping spam emails at the connection level using dynamic reputation filters. Additional features such as email firewall (checks for malicious connections) and sender validation (checks validity of recipient with an LDAP lookup, otherwise marks email as spam) further improve accuracy.
- **Keep up to date with new spam attacks:** Detect image-based spam, phishing attacks and the next as-yet-uncategorized spam types. Proofpoint MLX automatically adapts to new attacks as they appear and applies updates without admin intervention.
- **Support diverse user populations of non-native-English speakers:** Outstanding accuracy against spam in any language—including multi-byte character languages such as Japanese and Chinese. Group policies leveraging LDAP integration can be applied to users from different language groups, while allowing them to override the settings to view their anti-spam interface in the language they desire.
- **Seamless transition from legacy anti-spam systems:** Flexible deployment options, rich customization features—and Proofpoint spam detection is so good you won’t miss your old configurations.
- **Maintain a “hands-off” policy with student desktops:** Protect them at the gateway from inbound spam, phish and virus attacks—no client software required.
- **Educate users with custom recipient notification:** Users may not realize that spam from certain sites was probably due to over-subscribing to gaming sites or newsletters. Periodic reminders for them to limit posting their email address on these sites may prevent the problem from worsening.

### Proofpoint Helps Fight the Back-to-School Blues

As students arrive for a new semester with their own computers, many bring with them unwelcome guests:

- **Un-patched and vulnerable systems:** Ripe for infection by viruses, worms—many of which arrive via email.
- **Systems infected with computer viruses and malware:** Pose a potential risk to other network-connected systems as a launch platform for botnets and worms.

Preventing email-borne viruses is one of the top priorities when protecting EDU user systems... especially since the state of those operating system patches and client-side anti-virus software is unknown and not under admin control.

Through strategic partnerships with leading anti-virus vendors (McAfee and F-Secure), Proofpoint Virus Protection™ provides complete signature-based virus scanning functionality. To complement this signature-based solution, Proofpoint Zero-Hour Anti-Virus™ uses proprietary behavioral analysis techniques to stop emerging viruses well before they can be fingerprinted for signatures.

Responsibility to the extended user community is also a major concern for EDU administrators, so having these networks commandeered for a botnet attack is highly undesirable. Proofpoint helps detect computers that are infected with malware that has turned them into spam and virus-sending “zombies,” making it easy for IT staff to track down infected machines and disinfect them.

### It has to be simple

Due to their limited resources, many EDU IT departments continue to struggle with numerous point solutions built with usability as an afterthought. Effective email security systems for the EDU market need to deliver extraordinary ease of use for both expert and novice computer users.

### Set it and forget it with Proofpoint

No special rules need to be written for anti-spam and anti-virus protection. It’s all in there. Just turn it on and see immediate benefits. Done.

#### Worry-free administration

**“The Proofpoint Messaging Security Gateway has required absolutely no administration. The only time I need to access the system is to obtain weekly reports on spam and virus data. It is truly a ‘set it and forget it’ solution.”**

**James Walker**  
Senior Systems Admin  
Hofstra University

### Admin control = user concern

Educational institutions continue to support research, education, free speech and all other privileges supported by open computing. Requiring administrative control of end-user systems to support security initiatives isn’t acceptable—IT is an enabler, not a police officer.

With anti-spam solutions, students and researchers are often wary of external solutions that decide which emails they can and can’t see, resulting in distrust on the part of many EDU users.

### Proofpoint empowers users

Proofpoint gives end users full control over their personal spam quarantines and preferences, providing complete security combined with visibility. Features include:

- Personal end-user digests give users a full view into spam being quarantined on their behalf and allow them to easily un-flag spam, while still reducing inbox clutter.
- Email tag and forward allows users to use client-side email filtering to move spam-tagged emails to folders for later viewing or research.
- Recipient notification: Any event can be triggered by policy to send an email to the end-user or administrator.
- Compliance Incident Manager reports on compliance and data loss violations, and sends to a designated reviewer.

# Proofpoint Solution Brief for Educational Institutions

## EDUs have to learn their ABCs too

The alphabet soup of data privacy regulations—FERPA, HIPAA, GLBA, PCI and others—impacts many universities. Educational institutions often play multiple roles ranging from instruction and research in academic disciplines to medical and financial services. The latter two roles add an additional level of complexity with respect to messaging security and data loss prevention (DLP) as organizations struggle to meet the regulations that govern these industries. Monitoring, enforcement, and reporting requirements unique to each regulation add to the burdens facing today's EDU IT staff.

### Proofpoint Simplifies Data Privacy Compliance

Many of the regulations governing educational institutions which participate in health-care and financial lending focus on protecting private data—of students, faculty, patients, doctors, and researchers. Proofpoint solutions help simplify compliance with the industry's most comprehensive DLP feature set:

- **Designed for compliance:** Built with security best practices in mind – access control, strong passwords, and messaging encryption.
- **Simplified policy definition:** Templates and code sets for healthcare, financial, and privacy regulations. Regulations supported out of the box include Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), GLBA (Graham-Leach-Bliley Act) and PCI (Payment Card Industry), to name just a few.
- **Built-in and customizable reports:** To simplify compliance reporting for internal and external audits
- **Message tracing and advanced forensics:** Forensics tool to trace messages with content that may have been in violation of an industry regulation or acceptable use policy. For example, the tool could determine if a user sent sensitive content to an unauthorized user.

### Solutions Tailored to EDU not Easy to Find

IT administrators in EDU are wary of the “one size fits all” approach that many vendors take to providing technology solutions to their customers. Often, the unique requirements of the educational market aren't well served by solutions designed for commercial or federal government customers, where variations in pricing, usability, and end-user control could make the solution virtually useless in EDU. This concern extends to email security and data loss prevention vendors as well.

### Proofpoint has long history of satisfied EDU customers

#### *Over 90% of EDU prospects who evaluate Proofpoint end up buying*

Technology in support of educational institutions should be implemented with the unique requirements of their IT administrators and users in mind. Proofpoint has been partnering with IT administrators in EDU for years, as evidenced by more than 100 EDU clients that rely on Proofpoint. Add to this a dedicated team of EDU account managers, special pricing, and “futureproof” Proofpoint MLX technology and it's easy to see why Proofpoint is the ideal email security and data loss prevention partner for the cost-conscious EDU market.

#### *Our customers say it best*

Don't just take our word for it. See what our customers in the educational market have to say about how Proofpoint solved their toughest email security and data loss prevention challenges. Visit our Resource Center and browse through our case studies on EDU customers:

<http://proofpoint.com/resource-center/>.

#### *See for yourself*

Take the next step to learning more by viewing our free online demo which presents the key features and benefits of Proofpoint's unified email security and data loss prevention solutions:

<http://www.proofpoint.com/demo>.

### Address privacy requirements for HIPAA and financial regulations

**“The University of Texas Medical Branch (UTMB) has more than 12,000 employees. UTMB also records more than a half million visits and more than 35,000 inpatient admissions a year. So, we really need to know what's going on within our organization when it comes to inbound and outbound content. In addition, the 2005 HIPAA deadline is driving us to look at new compliance solutions to identify and secure non-public information, such as credit card and patient healthcare information. We are excited about Proofpoint 3.0 because it is a solution that will help us meet both HIPAA and financial privacy requirements.”**

**Lead security analyst  
University of Texas Medical Branch**

### The obvious choice for EDU

**“Proofpoint was the best solution, hands down. The Proofpoint Messaging Security Gateway impressed us with its flexibility, ease of administration and anti-spam and virus accuracy. The decision to go with Proofpoint was unanimous.”**

**James Walker  
Senior systems administrator  
Hofstra University**

### For more information

Please visit the Proofpoint Resource Center for product datasheets, white papers, and case studies which will directly impact you as an educational information technology provider:

<http://proofpoint.com/resource-center/>

©2008 Proofpoint, Inc. Proofpoint Protection Server is a registered trademark of Proofpoint, Inc. in the United States and other countries. Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint MLX, Proofpoint Dynamic Reputation, Proofpoint netMLX and Proofpoint on Demand are trademarks of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 02/08 REV A