

CASE STUDY

Ulster-Greene Arc

Ulster-Greene ARC is a non-profit agency that offers a full array of services from birth through adulthood to people who have autism and other developmental and intellectual disabilities.

The Challenge

To address data loss and web security, Ulster-Greene originally backhauled Web traffic from 35 locations to 3 central locations for URL filtering on traditional proxy servers. They faced a number of challenges with this solution. Backhauling so much traffic created significant latency and performance issues. Moreover, the URL filtering appliances could only define broad, static categories of filtering, but could not provide granular, dynamic control of web content.

Bart Louwagie, Director of IT at Ulster-Greene ARC, explained, *“We had blocked a lot of websites because we feared the chance that they may contain rogue elements like botnets, even if the website was legitimate. It was an issue that was hampering useful traffic from going to websites that it should be able to go to.”* Web filtering was based on the URL and it was impossible to know if the content of sites—even on everyday sites—was clean.

Finally, mobile devices and road warriors were left unprotected. *“When employees took their laptops on the road, it was difficult to get those laptops configured correctly, and we couldn’t enforce our policy for those users,”* said Louwagie. Data loss was especially important: Ulster-Greene had to protect private medical information and enforce appropriate use of the web in order to remain HIPAA compliant.

The Solution

With Zscaler’s cloud-delivered service, each of the 35 Internet gateways simply forwards Internet-bound traffic to the Zscaler cloud, where policy-based, in-depth bi-directional threat inspection is performed. This results in an improved security posture and prevents Personal Health Information (PHI) from escaping via Web 2.0 channels such as Webmail, Instant Messaging and blog postings.

Service subscription model over in-house appliances

Ulster-Greene no longer needs to purchase and maintain appliances in-house, nor does it need to backhaul traffic to centralized locations. This significantly improved performance, as Louwagie notes, *“We don’t have to transport the web traffic over our VPN to a central proxy location before it goes to the Internet.”* Zscaler’s distributed network and high-performance proxies ensure that Ulster-Greene business and security policy is enforced with a fraction of the latency.

Dynamic content filtering over static blacklists

Ulster-Greene’s original solution reflected traditional URL filtering models: static databases of 15-20 million blacklisted URLs. But with Web 2.0, much of the content on the Internet is user-generated and traditional URL databases do not have the ability to classify constantly changing page content. Ulster-Greene struggled with blocking websites entirely because they feared



THE CHALLENGE

- Backhauling traffic from 35 sites to 3 central locations for basic URL filtering introduced latency and caused performance degradation
- No granular control; broadly blocked access to web applications
- No protection for mobile users
- Needed to be HIPAA compliant and prevent data loss

SOLUTION EVALUATION

- Service subscription model over in-house appliances
- Dynamic content filtering over static blacklists
- Protecting Web 2.0 channels

THE ZSCALER DIFFERENCE

- Trusted security and DLP
- Lower total cost of ownership
- Enabling business

embedded security risks. With Zscaler's dynamic content classification technology, they receive pages that have been scanned on the fly at a very high speed, categorized and handled based on company policy.

Protecting Web 2.0 channels

"What if someone tries to send of confidential medical information through Gmail? Zscaler is thinking about that and has a solution," said Louwagie. Ulster-Greene's previous solution was to ban Gmail almost entirely: *"We would allow it for half an hour a day so that they could check their home email."* Even then, there was no way to inspect outbound traffic for information such as a Social Security number. *"Now we can allow users to visit a lot more websites than we were able to allow them to do in the past, while risking less data loss."*

The Zscaler Difference

Trusted security and DLP

"It was interesting... while testing Zscaler we actually found a serious issue with a non-secure website where we were entering social security numbers," says Louwagie. The Zscaler DLP solution uses multiple technologies of several proprietary algorithms to protect sensitive data, providing Ulster-Greene with trusted DLP. *"We also like that Zscaler is focused on understanding upcoming and modern threats,"* adds Louwagie. Zscaler's in-the-cloud service is ideal to detect malicious active content, botnets and other advanced threats such as Cross-Site Scripting—and is constantly updated to reflect upcoming threats. The Zscaler solution is able to secure and enforce policy for road warriors, who were previously entirely unprotected.

Lower total cost of ownership

The Zscaler service provides an order of magnitude savings in total cost of ownership versus traditional on-premise point products. Ulster-Greene no longer needs to buy, deploy or manage on- premise appliances. They spend less time on operational security chores such as managing and patching boxes: *"We have really reduced IT and management overhead,"* says Louwagie. In addition, they are no longer backhauling traffic, significantly saving in bandwidth costs.

Enabling business

"We really wanted to focus on our strategic policy in the organization to enable the business. Zscaler helps us because we spend less time on looking at web traffic," says Louwagie. With Zscaler, Ulster-Greene is now freer to focus on their day-to-day business operations. *"We have staff that is happier. We have a solution which allows us to focus on our business."*



"We now can enforce consistent Internet access policies, whether employees are at our office, on the road or at home. Zscaler's Web 2.0 security and Data Leakage Protection functionality is very easy, yet very powerful."

– Bart Louwagie, Director of IT,
Ulster-Greene Arc

About Zscaler

Zscaler is transforming enterprise networking and security with the world's largest Direct-to-Cloud Network, which securely enables the productivity benefits of cloud, mobile and social technologies without the cost and complexity of traditional on-premise appliances and software. The Zscaler Direct-to-Cloud Network processes daily more than 10 billion transactions from more than 10 million users in 180 countries across 100 global data centers with near-zero latency. Learn why more than 4,000 global enterprises choose Zscaler to enable end- user productivity, enforce security policy and streamline WAN performance. Visit us at www.zscaler.com.

CONTACT US

Zscaler, Inc.
110 Baytech Drive, Suite 100
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

zscaler.com

FOLLOW US

- facebook.com/zscaler
- linkedin.com/groups/zscaler
- twitter.com/zscaler
- youtube.com/zscaler
- blog.zscaler.com



Zscaler®, and the Zscaler Logo are trademarks of Zscaler, Inc. in the United States. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners