lastline™

CASE STUDY

Gwinnett County Public School System Chooses Lastline For Advanced Malware Protection

The Challenge

Cybercriminals have transitioned from casting a wide net with opportunistic attacks, to targeting specific organizations with the intent of stealing high-value information and data. Because of this shift, Gwinnett County Public Schools realized that to adequately protect its assets it was necessary to acquire new advanced malware detection technology.

"Businesses large and small are under constant cyber-attack. We have seen the threat landscape transform from traditional attacks centered on the network perimeter to sophisticated 'phishing' and "drive-by download"assaults directed at our end-users and endpoint systems," says Arden Peterkin, Security Architect at Gwinnett County Public Schools.

The Solution

The Gwinnett County Public School System evaluated several products while searching for the best advanced malware protection tool. It chose Lastline® because it was the only solution that:

a. Used Deep Content Inspection™ and detected the evasive malware that other systems missed

b. Provided a complete picture of the health of the network.

COMPLETE VISIBILITY

Deep Content Inspection is a unique isolation and inspection environment that analyzes suspicious objects and detects the threats that other advanced threat detection technologies miss. It provides security personnel at Gwinnett County Public Schools with unmatched visibility into malware behavior, completely dissecting advanced malware crafted to evade detection. Without these capabilities, the school system knew that there would be gaps in its security coverage.

Arden Peterkin, Security Architect at Gwinnett County Public Schools said *"Lastline provides us with deeper visibility and insight into web downloads and malicious attachments embedded within 'accepted' business applications and protocols, and 'passed-through' by traditional perimeter security solutions. Lastline also provides us with 'post-infection' awareness to quickly detect and remediate compromised endpoint systems that are 'calling home' to criminal networks."*

EXECUTIVE SUMMARY

Industry
Education

Company
Gwinnett County Public Schools

Description
Largest school system in Georgia

Challenge
Protecting 190,000 end-users against emerging web and email threats

Solution
Lastline Enterprise Hosted

Results
Can quickly detect and eradicate malicious files before they cause a full-scale security breach

"The challenge for all of us, CISOs, security managers, and security analysts alike, is to quickly detect and eradicate malicious files before they cause a full-scale security breach. Lastline Enterprise helps us satisfy this challenge."

EASE OF USE

Another reason the school chose Lastline over other vendors in the market was the product is easy to install, easy to navigate, and simple to manage. Within a matter of hours, Gwinnett County Public School System was able to deploy Lastline Enterprise and begin detecting malicious code.

"The feature we liked most about the product was the consolidation of web and email payload assessment into a single solution," adds Peterkin. *"Having one intuitive interface to manage shrinks our footprint without compromising detection and simplifies our workload."*

COMPLETE MANAGEMENT

Lastline enabled the security team to handle incidents with a speed and context that other solutions simply couldn't provide. The correlation of network activity and malware behaviors provide an incident-centric view of infections. Security personnel were able to intuitively navigate the console and review infections for a complete picture of the health of the network.

The Results

Lastline Enterprise now monitors the school system's network traffic (DNS, HTTP from proxies, and non-HTTP internet traffic), and all email and attachments. The mail system automatically copies all email and attachments to a special account. Lastline evaluates everything in that email account.

Security personnel receive real-time notifications of emerging threats that have penetrated traditional security defenses. These timely and comprehensive notifications enable the staff to react quickly and efficiently.

"In today's threat landscape of zero-day exploits and APTs, security incidents are inevitable," says Peterkin. *"The challenge for all of us, CISOs, security managers, and security analysts alike, is to quickly detect and eradicate malicious files before they cause a full-scale security breach. Lastline Enterprise helps us satisfy this challenge."*

Superior Protection, Simple to Try Out

When choosing Lastline, you gain the visibility you need to detect and respond to the advanced threats that other security tools miss.

Request a demo today at: http://go.lastline.com/request-lastline-trial.html

Experience the Lastline Advantage

For more information please visit www.lastline.com

LASTLINE CORPORATE HEADQUARTERS
203 REDWOOD SHORES PARKWAY
SUITE 620
REDWOOD CITY, CA 94065

AMERICAS: +1 (877) 671 3239
EMEA: +44 (0) 207 749 5156
APAC: +65 6829 2207
WWW.LASTLINE.COM

lastline™

© 2017 Lastline, Inc. All rights reserved. Lastline is a registered trademark and the Lastline logo is a trademark of Lastline, Inc. All other trademarks are the property of their respective owners. Lastline technology is protected by U.S. Patents 8910285 and 9361459. Additional patents pending. | v. 041517