clearswift

RUAG Cyber Security

Case Study
Clearswift Enhances Information Security in Microsoft Office 365

"

If potentially dangerous emails get through our network, it can take up a lot of our time to resolve – the Help Desk and other technical areas, to potentially the Networking and Systems teams would need to get involved. But this is avoided with Clearswift. The solution saves us potentially hundreds of man hours per year

Alex Kennedy, Assistant Director of Business & Data Operations, Volusia County Schools

"

Overview

Volusia County Schools is the public school district for Volusia County in Florida. The district operates over 80 schools with over 63,000 students and 7,300 teachers and administrators.

A business decision in 2017 motivated by the need to reduce business costs prompted Volusia County Schools to migrate from an on premise infrastructure to Microsoft Office 365 and Microsoft Azure cloud services. Volusia's IT department, however, understood the security functionality limitations with Office 365 and wanted to retain the same level of protection the Clearswift SECURE Email Gateway (SEG) had provided for their on premise system.

The Challenge

Basic Security Functionality in Microsoft Office 365

Email remains one of the most common digital collaboration tools for organizations globally and the threat landscape has subsequently evolved. Today, advanced security and data loss prevention features are needed to combat information borne threats across email – from within and outside the organization. However, Microsoft Office 365 only has basic security features built in such as anti-spam, anti-malware and URL scanning. In addition, any anomalies the platform detects and deems as a threat are 'blocked' which the IT department then has to deal with. For large organizations, the administrative time dealing with 'stop and block' solutions, or worse still, security threats that penetrate a network because they can't be captured with basic security functionality, can be time consuming and costly.

The solution

Enhancing Information Security in Office 365

- Unlike competitive security solutions on the market, the Clearswift SEG can integrate with Office 365, so Volusia was able to enhance information security in their cloud deployment to enterprise level protection.

- The Clearswift SEG incorporates unique Adaptive Redaction features (structural sanitization, document sanitization and data redaction) as well as advanced security tools such as Encryption, DMARC, DKIM and more. Working together simultaneously, the organization is protected from both inbound advanced threats and outbound sensitive data loss risks.

- Clearswift's deep content inspection engine scans email messages, including attachments, as they flow in and out of Office 365, automatically removing active code (the source of Ransomware attacks) or redacting sensitive information, but leaving the rest of the email to be delivered uninterrupted.

- The automated alteration to content in email and attachments occurs 'on the fly' on both inbound and outbound traffic, enabling continuous communication flow that is necessary for the schools to operate effectively.

The outcome

Advanced Threat Protection and Data Loss Prevention for Volusia's Office 365 Deployment

Schools and their associated administrative bodies handle vast amounts of sensitive information such as student contact details, social security numbers, Passport details, addresses and credit card details, all of which need to be stringently protected from inadvertent leaks or unauthorized exposure.

Alex Kennedy, Assistant Director of Business & Data Operations, Volusia County Schools said, "The functionality of the Clearswift SECURE Email Gateway and its web-based interface have always been key strong points for us. The solution's integration with Office 365 was a real bonus. We now have peace of mind that our new cloud email platform has the same level of protection that we had become accustomed to."

Given the huge amount of critical data stored and processed, Education is also a prime target sector to cyber-criminals. A key Clearswift SEG feature for Volusia was the ability to setup spoof sender notices to inform users that 'reply to email' is not the 'display name email' which is a real asset to the organization. In addition, the team commended the 'malicious content notification' for trigger code in messages as well as the delegated access granularity for different levels.

Alex disclosed, "A significant amount of phishing and spoofed emails are attempted, so it's crucial that these are detected and captured before they reach our team. Advanced security features to detect threats on inbound email traffic are as crucial as outbound data loss prevention features to protect sensitive information from unauthorized exposure across email."

As a result of integrating the Clearswift solution, the team at Volusia are more confident about the security of information flowing through their Microsoft Office 365 platform and also highlighted they have vastly more time to focus on more strategic tasks.

"From an IT perspective, Clearswift has enabled us to cut down on reactive security events. If potentially dangerous emails get through our network, it can take up a lot of our time to resolve - the Help Desk, other technical areas, to potentially the Networking and Systems teams would need to get involved. But this is avoided with Clearswift. The solution saves us potentially hundreds of man hours per year," Alex highlighted.

Volusia manages the Clearswift SECURE Email Gateway in house so the IT team can adjust content protection policies and security controls as and when business requirements change, but Clearswift also operates a 24/7 support service when technical assistance or advice is required.

"To sum up the best thing about Clearswift's solution – it would be 'its reliability'," says Kennedy. "The Clearswift SECURE Email Gateway has an excellent track record for Volusia. In addition, the support we receive from the team is always handled with a sense of urgency and they always keep us fully informed. The team understands that their product impacts security and how critical this is for our organization."