KVC Health Systems

We all need connection.

KVC HEALTH SYSTEMS ELIMINATES EMAIL SECURITY INCIDENTS WITH VADE FOR M365

Adopting Vade for M365 resulted in a 15% or higher improvement from previous solutions.

ABOUT KVC HEALTH SYSTEMS

KVC Health Systems is a private, nonprofit organization with 35 locations across Kansas City, Kentucky, Missouri, Nebraska, and West Virginia. Founded in 1970, KVC Health Systems provides behavioral healthcare, child welfare, and community health and wellness services, as well as healthcare consulting to private and government organizations.

THE CHALLENGE

Employing 1,600 staff and supporting 63,000 children and families across five states, KVC Health Systems (KVC) recognized that it was an attractive target for cybercriminals. "Healthcare data has the highest revenue on the open market," said Erik Nyberg, Vice President of IT at KVC. "It would be detrimental to our reputation—if not our organization—if we had a leakage of that information."

Prior to late 2018, KVC had experienced an abundance of phishing and spear phishing emails. After migrating to Microsoft 365, email attacks increased exponentially. "The executives were emailing me once a week about something that got through," said Nyberg. "It was always a pain point, but it just increased after switching to Microsoft 365."

In previous years, email attacks were focused on KVC's c-suite, but as with many organizations, that trend changed. "Executives have seen it all now," said Nyberg. "They don't fall for very much." Today, Nyberg said, hackers are researching KVC through social media and other online data to discover employees who have access to the organization's systems, including finance, HR, and security.

In addition to garden variety phishing emails, KVC received extremely sophisticated, targeted phishing and spear phishing emails that were engineered to appeal to employees in the organization. "Our entire organization's mission statement is to help people," said Nyberg. "When an email comes in asking for help, the bad guys could have a much higher success rate."

Despite using a variety of email security products over the years, no solution had a catch rate sufficient to protect Microsoft 365. "I've never been happy with

WHY KVC CHOSE VADE

- ✓ Improved catch rate
- ✓ Ease of deployment
- ✓ Native integration
- ✓ Simplified email management

THE ADDED VALUE OF VADE FOR M365

In a recent three-month period, Vade blocked nearly 18,000 email threats targeting KVC employees.

Threat type	Total threats detected by Vade
Phishing	2,751
Spear phishing	593
Malware	145
Spam	13,138
Scam	1,266
Total	17,893

Of those 18,000 threats, Vade blocked nearly 5,600 that EOP missed.

Threat type	Unique threats detected by Vade
Phishing	714
Spear phishing	243
Malware	31
Spam	4,435
Scam	175
Total	5,598

an email security solution," said Nyberg. "Something that stops 80% of bullets just isn't enough."

SOLUTION

KVC knew they needed a new solution, but they weren't convinced there was an email security product on the market that could significantly improve protection for Microsoft 365. "I was familiar with all the products out there, and I knew that none exceeded the 80–90 percent catch rate." After meeting with Vade, Nyberg agreed to start a proof of concept (POC) with Vade for M365. "They said they could do better than 90 percent," said Nyberg. "'OK', I said. 'Show me.'"

Vade for M365 is an AI-based email security solution that is natively integrated with Microsoft 365. Unlike secure email gateways, it sits inside the Microsoft 365 tenant, layering with and complementing Microsoft Exchange Online Protection (EOP), while being transparent to users and invisible to cybercriminals.

Vade for M365's anti-phishing technology uses artificial intelligence, including machine learning (supervised and unsupervised) and deep learning (computer vision), to crawl URLs and webpages in real-time. Analyzing the origin, content, and context of emails and webpages, machine learning models recognize sophisticated obfuscation techniques that cybercriminals use to bypass email filters, including creating URL aliases with shorteners, redirecting legitimate webpages to phishing pages, modifying brand logos, and spoofing email addresses.

To block spear phishing attacks, unsupervised anomaly detection and natural language processing identify patterns and anomalies common in spear phishing emails, warning the user with a customizable banner.

To augment threat detection and ease the burden of investigation and incident response, Vade for M365 includes Auto-Remediate. Email threats that initially bypass the filter are automatically removed from mailboxes and directed to a folder designated by the admin. As the AI-engine continues to learn, it improves itself based on user feedback and threat intelligence.

RESULTS

The volume of catches in Vade for M365 took Nyberg by surprise. "Vade actually hits the 90's to mid-90's catch rate. I didn't think there was a product out there that could do that." Additionally, Vade for M365 catches a large volume of emails that bypass native Microsoft 365 email security. Over a three month period in 2019, Vade detected nearly 5,600 email threats EOP missed.

Another motivating factor for adopting the product was the native integration with Microsoft 365 and the ease of deployment, including the quick setup and the simple interface. "We definitely like the simplicity of Vade on the IT side," Nyberg said. "Going through the Microsoft 365 admin to whitelist or blacklist something is an extremely painful, 10–15 minute process. With Vade it's five seconds. Vade is 90 percent more simple than using Microsoft 365."

Finally, in the nine months since deploying Vade for M365, KVC hasn't' experienced a serious email attack that affected the organization. "Most years," Nyberg said, "at least one to two phishing attacks or attempts get through. I haven't had an email situation since I went online with Vade."

> ***"The catch rate of Vade for Microsoft 365 is a 15%, if not higher, improvement from any email filter I've seen. Vade catches what Microsoft misses."***
>
> **Erik Nyberg, Vice President, IT**