Technical Validation

Email Security with Microsoft and Valimail — No SEG Required

By Jack Poller, Senior Analyst

October 2020

This ESG Technical Validation was commissioned by Valimail and is distributed under license from ESG.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

Introduction 3
Background 3
Valimail 4
ESG Technical Validation 5
Sending Service Visibility 5
ESG Testing 6
DMARC Enforcement 9
ESG Testing 9
The Bigger Truth 12

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Introduction

This ESG Technical Validation documents evaluation of the Valimail Enforce email security solution. We focus on how Valimail Enforce complements Microsoft Defender for Office 365 to increase Microsoft Office 365 security by accelerating the time to DMARC enforcement and simplifying and automating SPF, DKIM, and DMARC configuration and management.

Background

Email provides the core for corporate communication; ensuring the integrity of email is paramount to protecting the organization from attacks and compromise. Unfortunately, most organizations suffer from email-borne attacks, with 12% of surveyed organizations reporting daily attacks (see Figure 1). Thus, more than two-thirds (69%) of surveyed organizations consider email to be one of their top-five threat vectors, with 18% considering email to be their most important cybersecurity priority.[1]

Figure 1. Most Organizations Experience Email Attacks on a Regular Basis



Source: Enterprise Strategy Group

Most organizations have made the transition to using cloud-based email solutions, and three-quarters of organizations (73%) use either Microsoft Office 365 or Google Gmail for their primary email solution. Due to the pervasiveness of email-borne attacks, many organizations believe the native security controls in cloud-delivered email solutions are insufficient. These organizations are adding third-party security controls, and some of the drivers for supplementing native security controls, according to ESG research, are improving phishing detection and prevention (25%), improving email spoofing detection and sender verification (17%), and simplifying the inherent complexity of policy and administration (17%).[2]

[1] Source: ESG Master Survey Results, *Trends in Email Security*, July 2020.
[2] Ibid.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Valimail

Valimail Enforce simplifies and automates the process of configuring and managing SPF, DKIM, and DMARC. Organizations can deploy Enforce in combination with Microsoft Defender for Office 365 to provide comprehensive Office 365 email security. DMARC enforcement powered by Enforce authenticates emails to stop domain spoofing, impersonation attacks, and phishing of employees, customers, and partners; Defender for Office 365 provides native Office 365 content protection, scanning email contents, links, and attachments to prevent spamming and malware attacks.

Figure 2. Valimail Complements Defender for Office 365 to Increase Office 365 Email Security



Source: Enterprise Strategy Group

Administrators can use Valimail to automatically collect and analyze DMARC aggregate reports and identify all services that send email on behalf of the organization. Valimail shows which services will be authorized or blocked when the administrator enables DMARC enforcement, and helps the administrator automatically configure and immediately publish SPF, DKIM, and DMARC records. Administrators deploying Valimail benefit from:

- Visibility—automatic identification of all new and existing email sending services as well as the global legitimate, suspicious, and malicious email traffic originating from the organization's domains.
- Simplicity—Point-and-click authorization of sending services.
- Acceleration—minimal time and resources are required to reach DMARC enforcement, which quarantines or rejects bad email.
- Accuracy—automation and visibility reduce risk of false positives, ensuring valid emails are delivered while blocking illegitimate email.
- Scalability—Patented technology allows unlimited authorized senders, overcoming SPF protocol limitations without IP address flattening.
- Integration—One-click deployment and integration with Microsoft 365 including instant visibility into emails sent into Microsoft 365 that send email on behalf of the organization.

Valimail Enforce employs a zero-trust philosophy whereby all unknown sending services, servers, and IP addresses are considered untrusted. Administrators must explicitly grant access to a service to enable the service to send email on behalf of the organization. This zero-trust approach in combination with Microsoft Defender for Office 365 provides comprehensive Office 365 email security.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

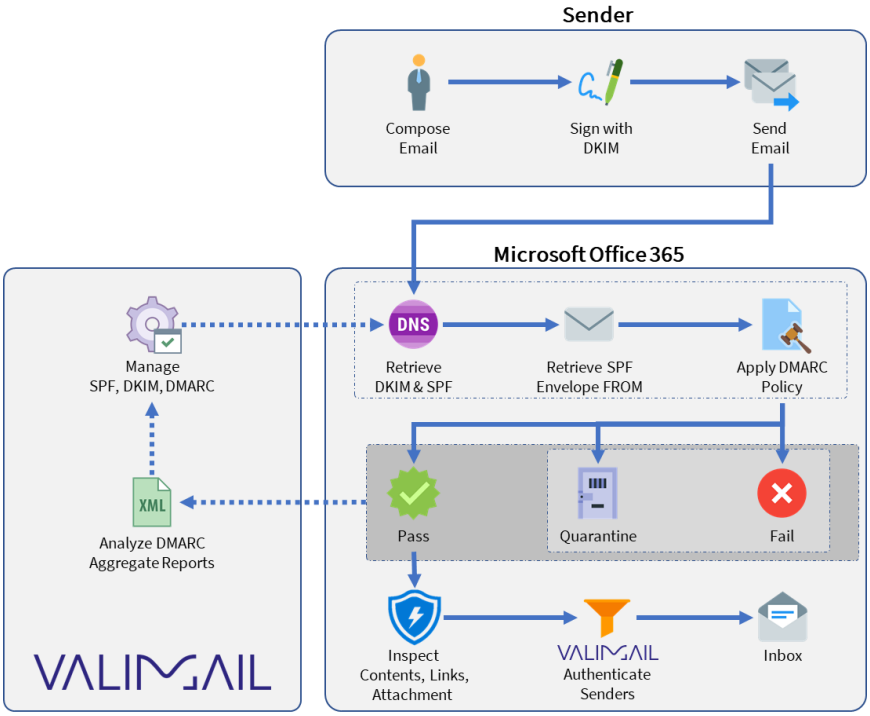
ESG Technical Validation

ESG viewed remote demos of Valimail that showed the speed and simplicity of DMARC and SPF management as well as how Valimail works in combination with Microsoft Defender for Office 365 to increase Office 365 email security.

Sending Service Visibility

The IETF has established three major protocols for email authentication: sender policy framework (SPF, RFC 7208); domain keys identified message (DKIM, RFC 6376); and domain-based message authentication, reporting, and conformance (DMARC, RFC 7489). All three protocols operate using records in the domain name system (DNS).

SPF verifies that the sending mail server is authorized to send mail for the domain by comparing the sending IP address with the published list of authorized addresses. In this way, SPF detects forged sender addresses during email delivery. However, many companies have difficulty configuring SPF correctly, due to limitations in the standard, such as the limit of 10 domain lookups within SPF records.



With DKIM, legitimate senders can digitally sign a message to show that it is genuine. The absence of a valid signature can imply that the mail is forged, and recipients can verify the signature using the domain's published public key.

Organizations use DMARC to publish an email authentication policy that specifies how the receiving email systems should handle authentication failures and where receiving mail systems should send authentication data on the emails they process for the organization. Organizations can configure the authentication failure policy to be none (email that fails authentication is delivered normally), quarantine (email is quarantined, typically by delivering to the spam folder), or reject (email is discarded).

In addition to applying authentication failure policies, receiving email servers send DMARC reports to addresses specified in the DMARC record. These reports contain aggregate information about the email received that appears to be from the sending domain. DMARC aggregate reports contain no personally identifiable information (PII). The aggregate reports are in XML format, making it difficult for administrators to read and understand.

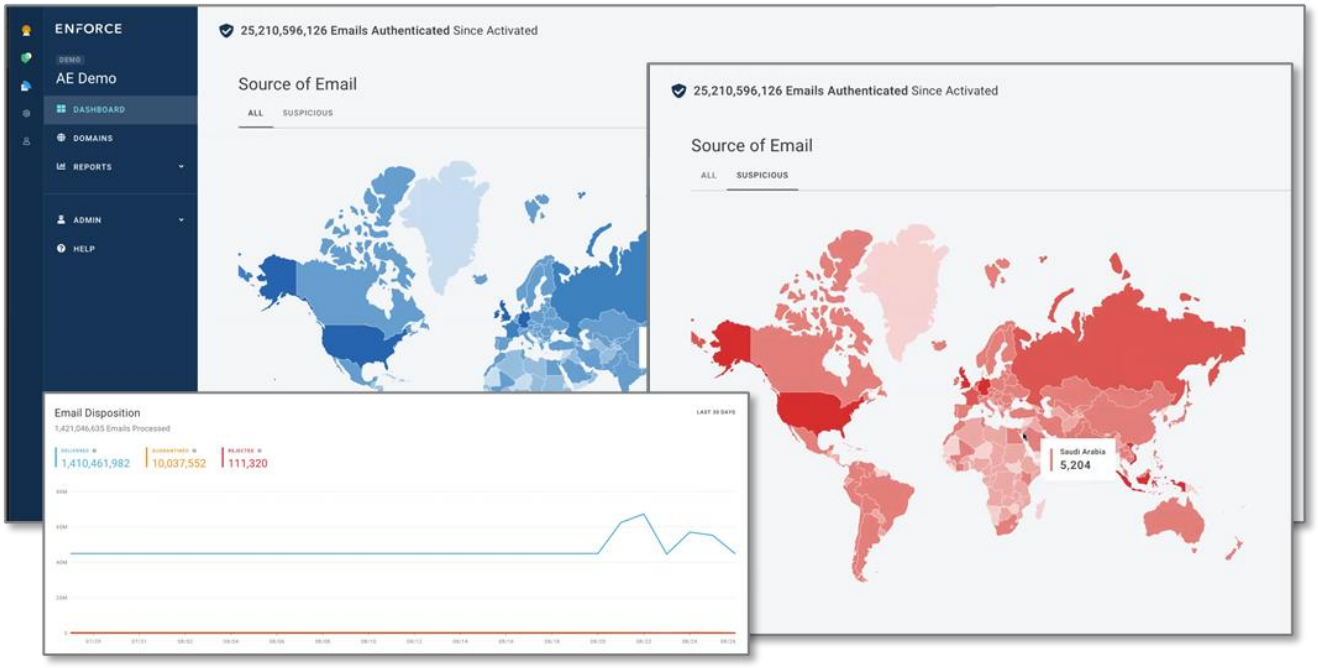
Valimail automates the management and monitoring of SPF, DKIM, and DMARC in several ways. It automates the collection and analysis of DMARC aggregate reports, providing visibility into all sending services for the domain and which emails are authenticating using SPF or DKIM or are not authenticating. In addition, administrators can use Valimail to authorize sending services, instantly update SPF, DKIM, and DMARC records, and enable DMARC enforcement, ensuring only authorized senders can send email using the domain.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

ESG Testing

ESG started by visualizing all senders using the domains we manage by viewing the Valimail Enforce Dashboard, which displays information analyzed from DMARC aggregate reports. As shown in Figure 3, the dashboard provides a geolocation heatmap showing server source location and email volume for the last 30 days. The ***SUSPICIOUS*** tab shows sources identified as suspicious—typically those servers sending email on behalf of the domain that are potentially malicious. The dashboard enables administrators to maintain situational awareness of all domain email senders. Displayed at the bottom is a graph showing volumes for categories corresponding to DMARC enforcement policies: delivered (none), quarantined, and rejected.

Figure 3. Valimail Enforce Dashboard

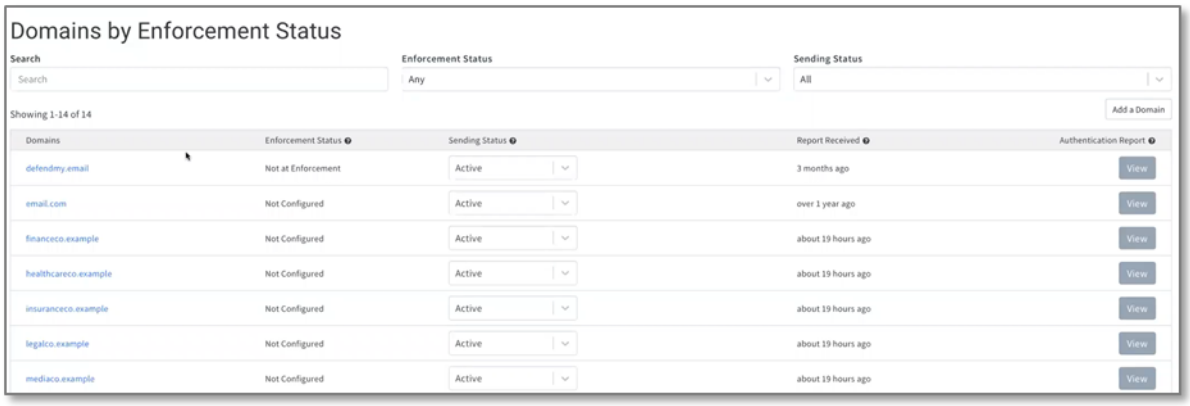


Source: Enterprise Strategy Group

We selected ***DOMAINS*** from the menu to drill down for details, displaying a searchable, filterable list of all domains managed by the account. As shown in Figure 4, the list includes each domain's DMARC enforcement status, sending status, and when the last DMARC aggregate report was received, and administrators can add domains using the ***Add a Domain*** button.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 4. Domains by Enforcement Status



Source: Enterprise Strategy Group

Next, we clicked on *insuranceco.example* to drill down for more information on this domain. The ***AUTHENTICATION REPORT*** tab displays passed and failed email volume (see Figure 5). We could select sub-tabs to show volume for all email, aligned SPF, aligned DKIM, or disposition. (SPF alignment is when the envelope <*MAIL FROM*> domain matches the message header <*FROM*> domain. DKIM alignment is when message header <*FROM*> matches the "*d=*" domain in the <*DKIM-Signature*> message header entry.)

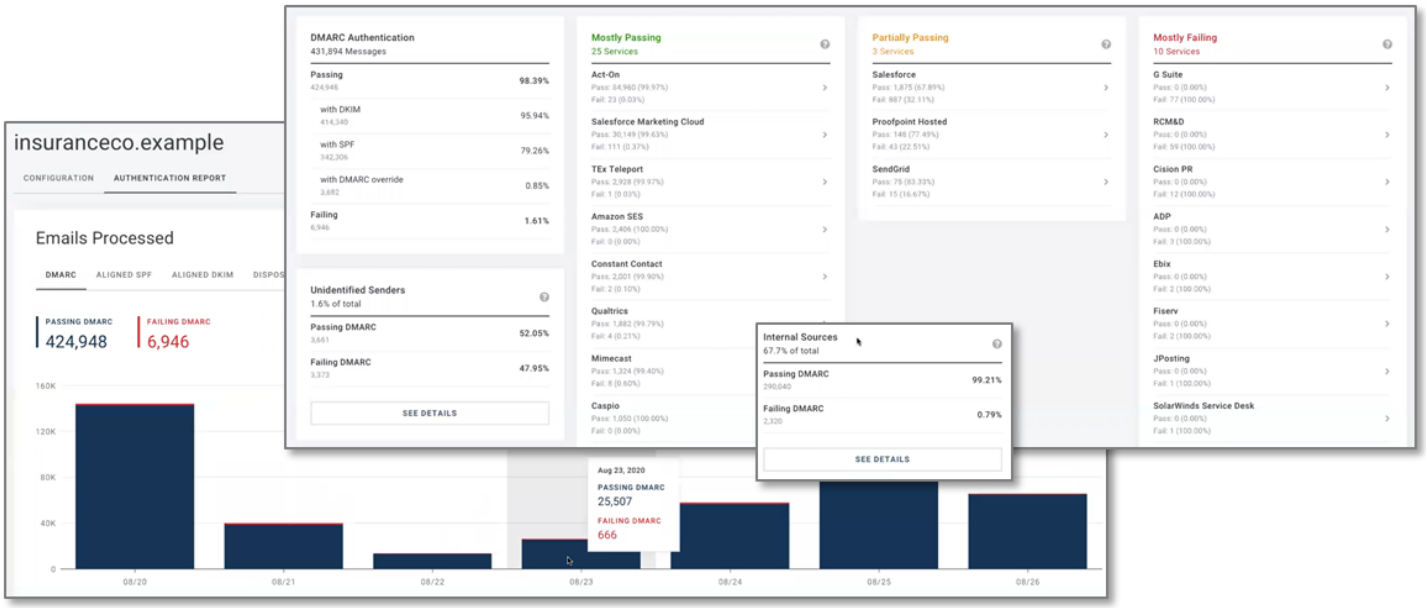
When an administrator enables DMARC enforcement by configuring the DMARC policy to reject (or quarantine), all failing email will be rejected or quarantined by receiving email servers. We used the ***AUTHENTICATION REPORT*** tab to understand the volume of mail that was passing or failing DMARC, and thus would be accepted or rejected when we enabled DMARC enforcement.

Because cloud services and SaaS applications often send email on behalf of the domain and users, administrators must correctly configure DKIM and/or SPF for each sending system. To simplify this process for administrators, Valimail uses its database of thousands of third-party emailing services to identify each sending service from the DMARC aggregate reports.

We selected the ***AUTHENTICATION REPORT*** tab to display those services categorized by passing, mostly passing, partially passing, and mostly failing DMARC enforcement. Using this information, we could identify which specific services would have issues when we enabled DMARC enforcement because email sent by those services on behalf of the domain would be rejected.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 5. Email Sending Services for Domain



Source: Enterprise Strategy Group

Why This Matters

SPF, DKIM, and DMARC are critical to authenticating email senders and preventing domain spoofing and phishing attacks. Designed when most organizations used a single email server, these protocols present challenges for modern organizations using multiple cloud services and applications with multiple email senders.

ESG validated that Valimail Enforce analyzed DMARC aggregate reports, enabling us to identify authorized, suspicious, and malicious email senders and services, and thus which services would be authorized or blocked when we enabled DMARC enforcement.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

DMARC Enforcement

Enabling DMARC enforcement prevents malicious actors from spoofing the domain for phishing and other types of attacks. However, with an incorrect configuration, organizations can inadvertently block legitimate senders and email.

Cloud services and SaaS applications present two challenges for SPF:

- Cloud service providers often use third-party mail solutions to deliver mail on behalf of the service and domain. Thus, it may be hard for email administrators to determine the correct SPF parameters.

  Valimail helps solve this problem with its database of SPF configuration and other information for thousands of services and applications.

- The SPF protocol specifies an "include" mechanism for recursive DNS lookups of SPF records, enabling organizations to incorporate the SPF records from multiple third-party providers. However, to prevent denial of service (DoS) attacks, the protocol limits receiving email systems to 10 lookups. Many organizations get around this limitation by listing email senders by IP address. However, with cloud-based senders, this solution is unwieldy and error-prone: It's not uncommon for SPF records to contain dozens of IP addresses, each of which must be maintained accurately, as cloud services often change IPs. It can also be risky, if IP address blocks are listed in SPF, because then every IP address within that block (which may be hundreds or thousands of separate addresses) is also authorized to send mail on the organization's behalf.

  When organizations use Valimail to host SPF records, Valimail avoids both the 10-lookup limit and the brittleness of listing IP addresses through its patented Instant SPF technology. This technology lets Valimail deliver a tailored SPF record to the mail receiver for each message that needs to be authenticated, based on the service that is sending that message. Valimail is able to do this because customer organizations have indicated in advance which services should be authorized and which should not be.

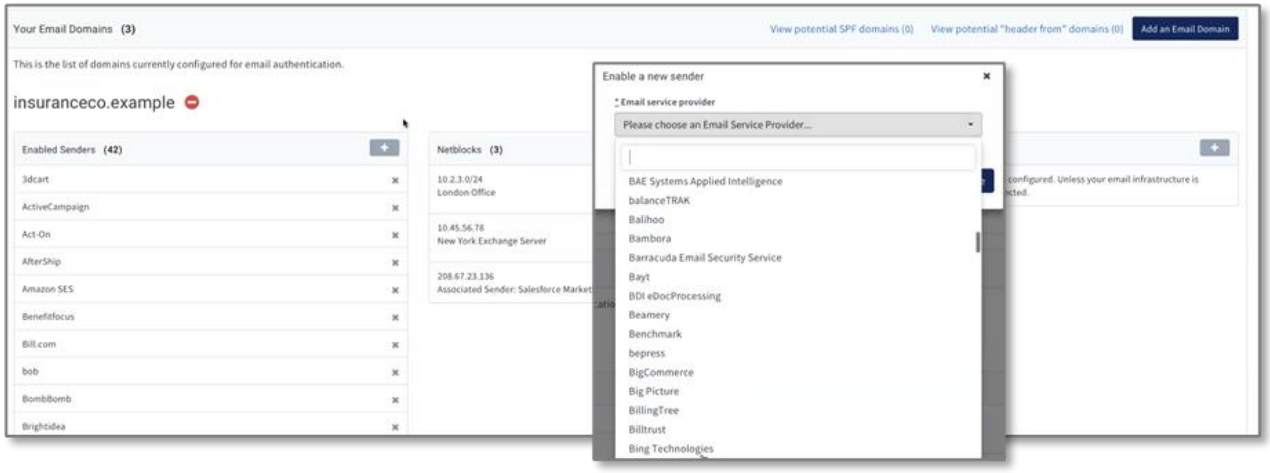
ESG Testing

The demo environment was configured to use Valimail to host the SPF, DKIM, and DMARC records. Thus, when ESG enabled DMARC enforcement, the change took effect immediately, and mail from unauthorized senders was blocked by Microsoft Defender for Office 365 and other receiving email servers.

Next, we authorized a new service to send mail on behalf of the *insuranceco.example* domain. We selected the ***CONFIGURATION*** tab, which displayed a list of all configured services and IP addresses (Netblocks), and then selected + to add a new service (see Figure 6). Valimail displayed a filterable list of thousands of available service providers, and we selected Billtrust, adding Billtrust to the list of 42 other authorized services. No changes to actual SPF records were required and we validated that Billtrust could immediately send email on behalf of insuranceco.example.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

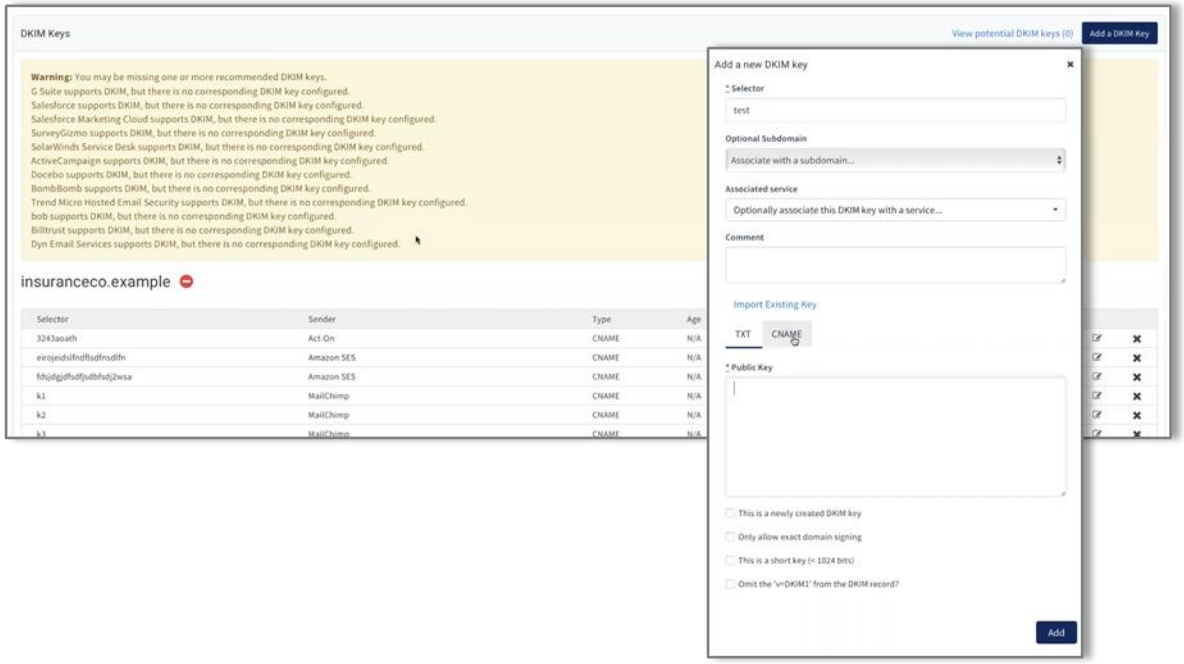
Figure 6. SPF Record Creation



Source: Enterprise Strategy Group

Valimail's database of services identifies which services use SPF and which services use DKIM. When services use DKIM, Valimail pops up a warning box and enables the administrator to create a DKIM key, as shown in Figure 7. Using the *Add a DKIM Key* popup, we could publish a new key. We created a new key and Valimail validated the entry to prevent errors and then published the DKIM in DNS. We validated that email generated by Billtrust was correctly signed using the new DKIM key.

Figure 7. DKIM Record Creation



Source: Enterprise Strategy Group

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Why This Matters

DMARC enforcement prevents unauthorized senders from spoofing the domain and deploying phishing attacks. However, properly configuring SPF and DKIM to authorize multiple senders is complex, confusing, and time consuming. Getting it wrong can result in blocking legitimate senders while enabling malicious activities.

ESG validated that Valimail simplified and accelerated configuration of SPF and DKIM, and we could easily authorize multiple services. Since Valimail was hosting our SPF, DKIM, and DMARC records, changes were instantaneous, and we overcame the 10-lookup SPF limitation. ESG validated that by using Valimail Enforce, we reduced the time and effort to protect our email environment with enforcement of sender authentication.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

Consistent with perceived risk, phishing and malware attacks are the most prevalent: In the past year, 33% of organizations have been penetrated by phishing, 27% by malware, and 18% by email spoofing and impersonation attacks. Email-borne attacks lead to loss of data and entry points for more sophisticated attacks, such as ransomware. Astoundingly, 22% of respondents have suffered from email-borne attacks that have led to the malicious transfer of funds.[3]

Valimail works in concert with Microsoft Defender for Office 365 to combat these attacks and increase an organization's Microsoft 365 email security. Valimail Enforce helps an organization identify all senders and correctly configure SPF, DKIM, and DMARC to authenticate email senders, ensuring authorized cloud services and applications can send email on behalf of an organization while preventing illegitimate senders. Microsoft Defender for Office 365 and Office 365 use DMARC enforcement in combination with content, link, and attachment inspection, and sender identity authentication to prevent spoofing, phishing, spamming, impersonation, and malware attacks. Valimail Enforce works hand-in-hand with Microsoft Defender for Office 365 to provide complete email security protection.

ESG's evaluation revealed:

- Valimail Enforce analyzed DMARC aggregate reports and provided summary and detailed information on all services sending email on behalf of the domain. We were able to quickly understand which services would be allowed or blocked when we enabled DMARC enforcement.
- Valimail Enforce simplified and accelerated SPF, DKIM, and DMARC configuration. Using Valimail to host these records ensured changes were propagated immediately and eliminated the 10-lookup SPF limitation.
- Valimail Enforce accelerated our time to DMARC enforcement.
- Valimail simplified the onerous and ongoing effort of managing and maintaining SPF, DKIM, and DMARC enforcement. With one click, we could authorize new services and changes took effect immediately.
- Valimail Enforce transparently integrates with and supplements the email security protection of Microsoft Defender for Office 365.

ESG evaluated Valimail using a demo environment. Due to the many variables in an organization's email infrastructure, it is important to perform planning and testing in your own environment to validate the viability and efficacy of any solution.

Many organizations have struggled with email security, adding layers of controls and complexity with third-party secure email gateways (SEG), or avoiding email security altogether due to the complexity, time, effort, and issues with misconfiguration.

Valimail, working in concert with Microsoft Defender for Office 365, can provide comprehensive email security by simplifying and accelerating the effort to authenticate email and get to DMARC enforcement. ESG believes that it is well worth checking out Valimail to see if Enforce can easily and quickly increase the security of your Defender and Microsoft 365 email deployment without the time, effort, cost, and complexity of SEGs.

[3] Ibid.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188