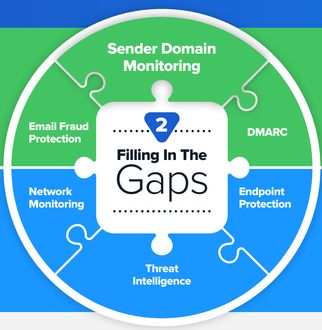
validity

An Overview of Sender Domain Monitoring

1 Threatening Your Brand Integrity

Email systems are increasingly the target of malicious actors, potentially causing significant harm to your brand and confidence in your emails.

When your email technology gets hacked, are you waiting for customers to complain on social media, or worse, for the news to pick it up? What else can you do about it?



Email Security falls into two buckets:

- Outbound Email Authentication (e.g. DMARC)
- Inbound Mail Protection (e.g. Mimecast)

...but neither of those tools can detect authentic mail being sent out by a compromised system.

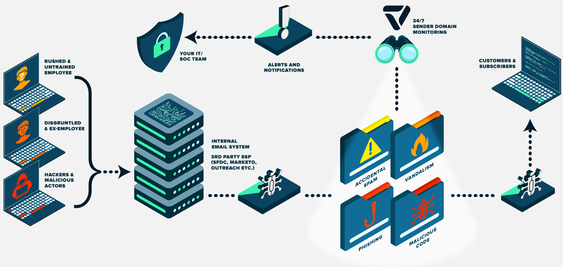
Cybersecurity relies on a layered strategy:

- Educated humans
- Internal detection and monitoring
- Perimeter and endpoint intrusion prevention
- Aggregate industry alerts of malicious actor signatures

... but today they cannot monitor external email activity for indicators of compromised systems.

3 What is Sender Domain Monitoring?

Sender Domain Monitoring is a simple to implement, non-disruptive security layer that provides real-time insight into and alerting on suspicious activity in the outbound email channel.



Key Features

- 24/7 Monitoring by Validity's Email SOC
- Alerting and notifications
- Email origination data
- Aggregate community data

Key Benefits

- Additional coverage along an emerging attack vector
- Early detection of suspicious activity
- Expediated root-cause analysis of active and previously compromised systems
- Ease of implementation, configuration, and maintenance

4 Sender Domain Monitoring Real-Life Example

Using our 24x7 monitoring methods, Validity saw indicators that a customer's email systems had been compromised and alerted them immediately. After further investigation, the company determined that an attacker had evaded their bot detection systems and created malicious fake user accounts. Once these accounts we created, the attacker sent "follow request" emails to both legitimate existing subscribers and new spam accounts. As a result, thousands of fake accounts were created and millions of unauthorized emails were sent from their IP.

After receiving the alert from Validity, the company disabled thecompromised emails. Moving forward, they made key updates to their bot detection software, onboarding process, user platform, and opt-in requirements.

validity

For over 20 years, tens of thousands of organizations throughout the world have relied on Validity solutions to target, contact, engage, and keep customers – using trustworthy data as a key advantage. The Validity flagship products – DemandTools, BriteVerify, Everest, GridBuddy Connect, and MailCharts – are all highly rated solutions for CRM data management, email address verification, inbox deliverability and avoiding the spam folder, and grid CRM applications. These solutions deliver smarter campaigns, more qualified leads, more productive sales, and ultimately faster growth. For more information, visit **Validity.com** and connect with us on **LinkedIn** and **Twitter**.

Validity.com
sales@validity.com