

# SaaS Defense:

## SaaS Defense: Helping SMBs Close the Cybersecurity Threat Detection Gap



### CUSTOMER BACKGROUND

**Industry:** Media

**Region:** North America

**Employees:** > 30,000

**Email Provider:** Microsoft 365

**Existing Email Security:** Proofpoint TAP

### Introduction

Datto SaaS Defense is one of the products we recommend to users of the Microsoft 365 office suite to protect against phishing and ransomware distributed via email and collaboration tools. This case study explains why it is so valuable.

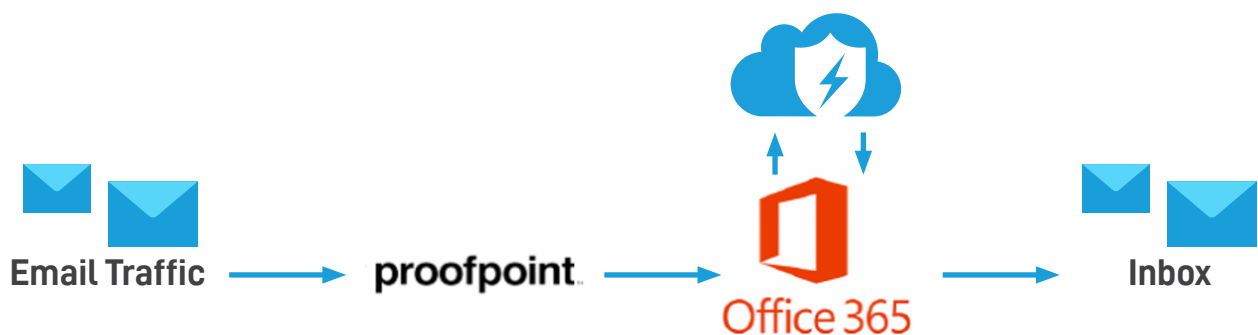
### Deployment

SaaS Defense uses the Microsoft 365 application programming interface and can be added to your account in just a few clicks. SaaS Defense is simple to manage and easy to understand and does not require additional security or IT resources to deploy. SaaS Defense was deployed as a 'last line of defense', on top of Proofpoint TAP to secure more than 30,000 Microsoft 365 mailboxes.

### Results: SaaS Defense vs. Proofpoint

The media company in this example was using SaaS Defense in addition to the Proofpoint TAP solution, and SaaS Defense was able to detect malicious emails that Proofpoint initially did not. Throughout a three-week period:

- SaaS Defense uncovered 50 malicious emails spread over numerous different campaigns that initially were missed by Proofpoint;
- SaaS Defense detected these 50 malicious emails in the range of 2-5 hours before Proofpoint identified them as malware
- Malicious content in these emails included advanced variants of attack families like Emotet, Dridex, Loda, and a Remote Access Trojan; and
- Multiple variants of the same attack were blocked by SaaS Defense at first encounter.



## Attack Variants Made Up Successful Campaigns

Most campaigns contained the same attack with slight variations. These variations, for example changing hashes or adding comments, turn known attacks into unknown threats, allowing malicious emails to bypass security.

**The attackers in this case used automation to generate unknown variants of known attacks in a short time, which successfully fooled Proofpoint. SaaS Defense detected all of them.**

### Examples:

- 23 Jan 2020: 28 attacks from the same EMOTET campaign within a span of 9 hours.
- 30 Jan 2020: 4 attacks from the same Loda campaign within a span of 5 hours.

## SaaS Defense Helps Close the Threat Detection Gap








Unlike other email security products which are data-driven, SaaS Defense's detection is based on a unique application execution model. While other products count on the knowledge of past threats to identify new ones, SaaS Defense's threat-agnostic approach is data-independent, allowing for high detection rates of both known and unknown threats. SaaS Defense's miss rate of unknown threats is low, thus significantly reducing the risk of successful email-based attacks.

## Security Against Phishing and Ransomware

Your business shouldn't be vulnerable to ransomware and other hacks just because someone clicked on the wrong email. Contact us today to discuss how we can protect you better with Datto SaaS Defense.

### 50 Malware Detected

#### Detection Timeline

|  |  |
|--|--|
|    | 3 malicious detections<br>04 Feb 2020  |
|    | 4 malicious detections<br>30 Jan 2020  |
|    | 6 malicious detections<br>28 Jan 2020  |
|  | 3 malicious detections<br>27 Jan 2020  |
|  | 28 malicious detections<br>23 Jan 2020 |
|  | 1 malicious detections<br>22 Jan 2020  |
|  | 1 malicious detections<br>22 Jan 2020  |

*Preview of the SaaS Defense detection timeline*