Tips for a Securing your Office 365 Environment

OSTERMAN RESEARCH

Barracuda
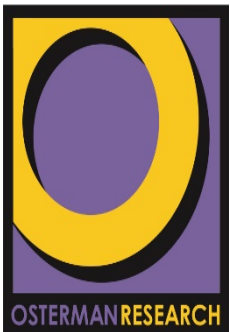
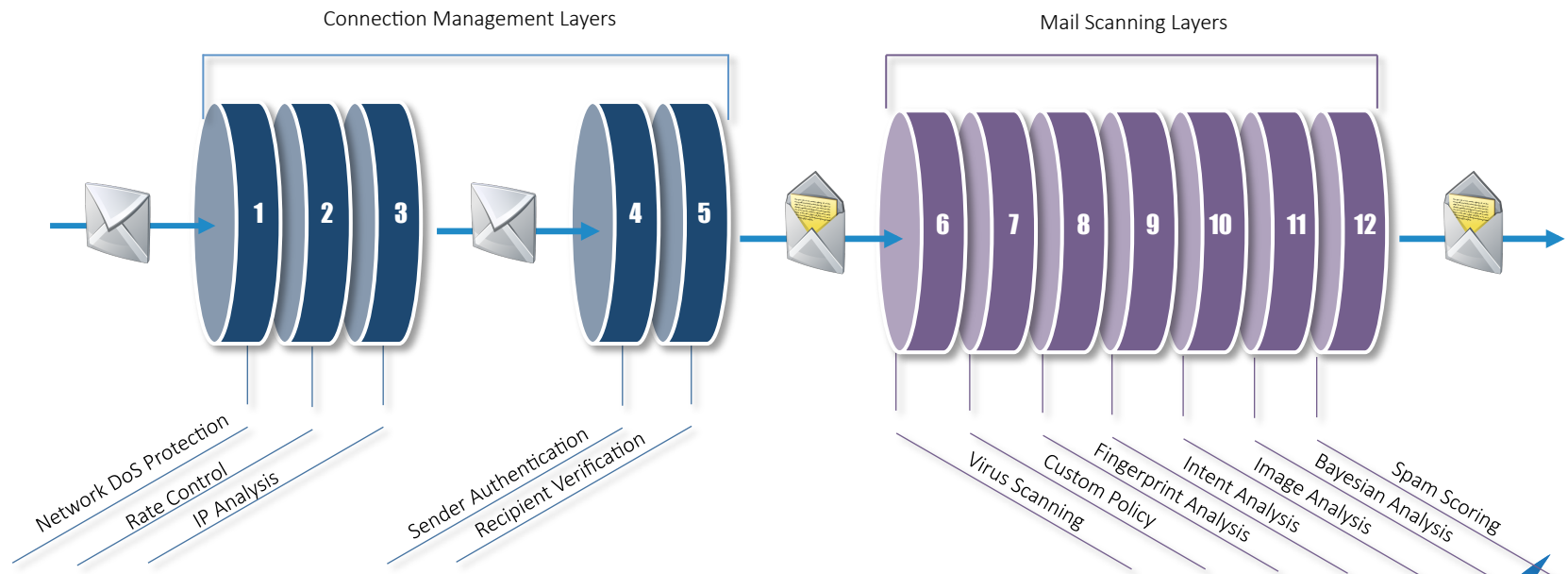# Now let's look at email security...
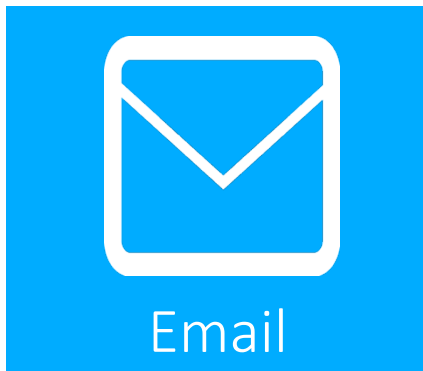
Email

Email Security...

Office 365 includes some security...

but you'll need more protection

To explain the differences, first let's look at just how email security works...

- Connection Management – all about the sender

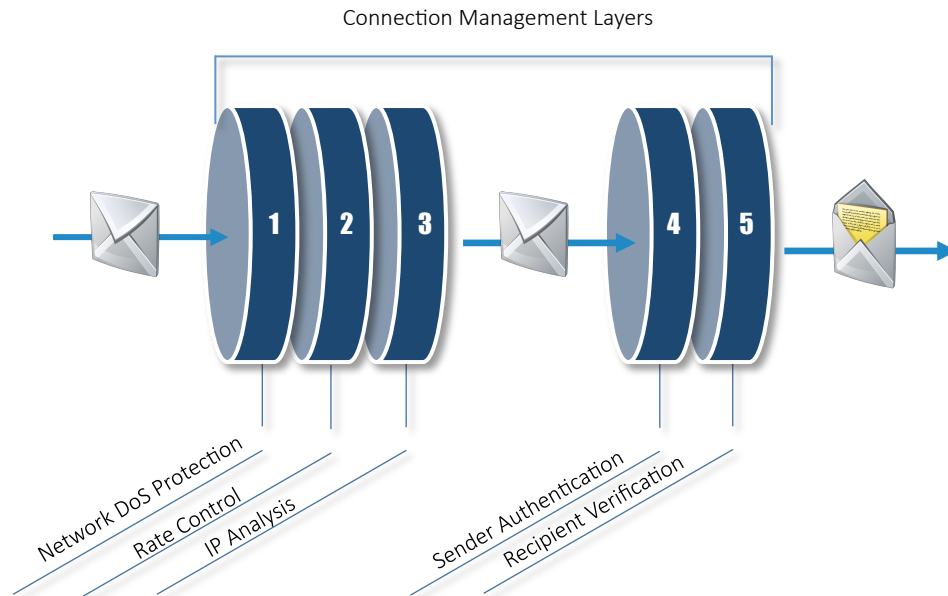- Mail Scanning Layers – what's in the body of the message

- Feature Overview

95% of spam is caught in the first 5 layers

Who's sending it – Are they real? - Is it a flood-based attack?

Are they a known spammer (blacklist)? - Are they trusted (whitelist)?

Connection Management Layers

1 2 3 4 5

Network DoS Protection
Rate Control
IP Analysis
Sender Authentication
Recipient Verification

EOP focuses on these layers

Until Jan 2015, limited IP Analysis (!)

EOP feature called IP Throttling – but does much the same as IP Analysis
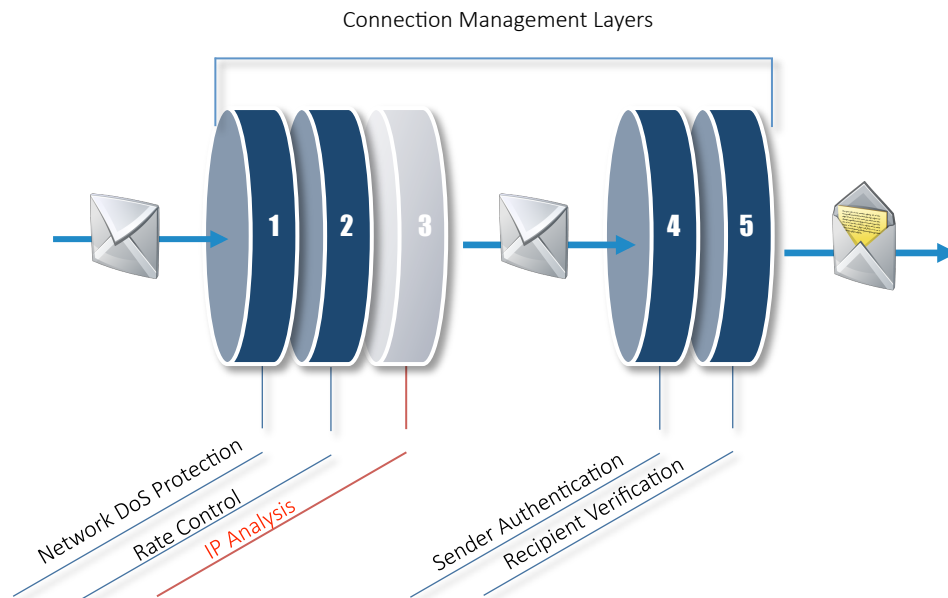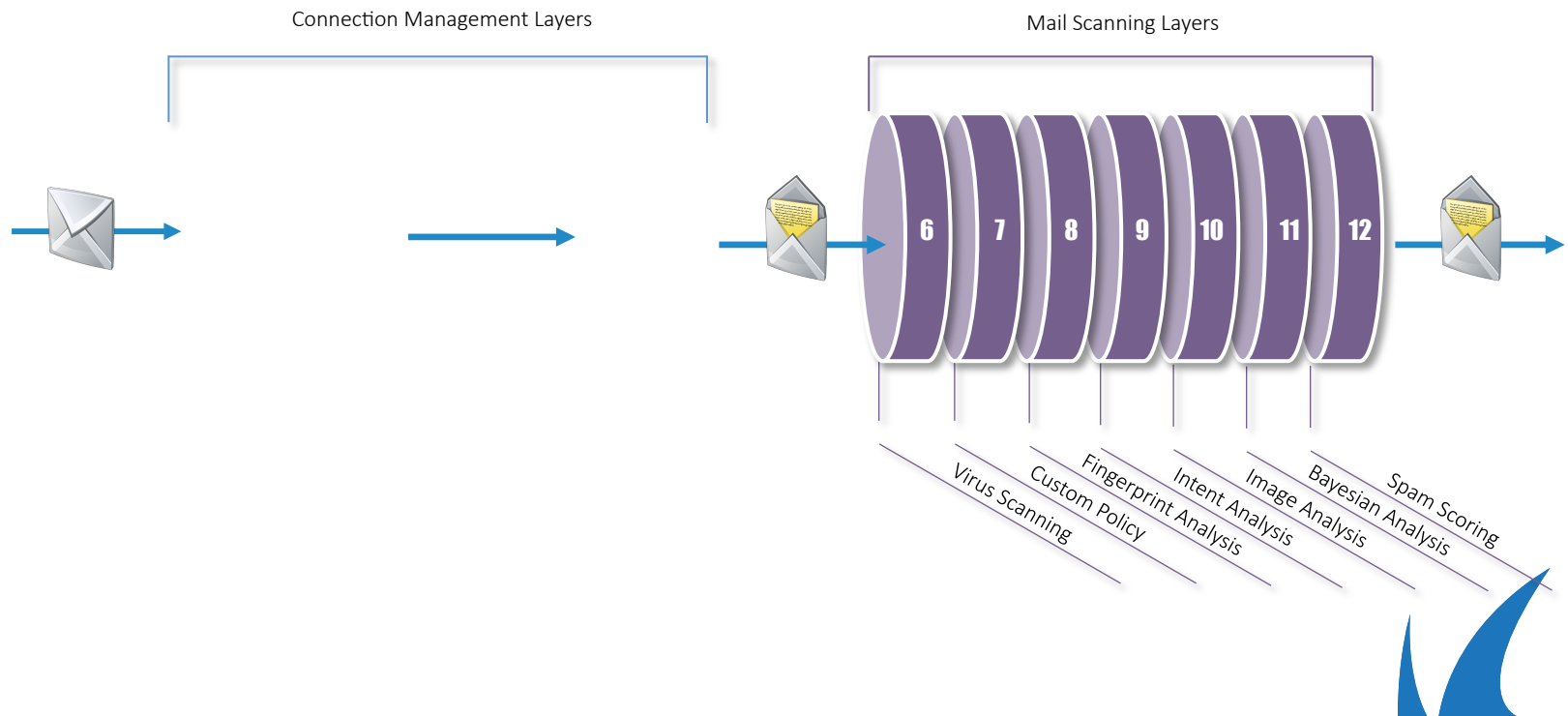
Is EOP Good Enough?

- Only part of the story – Connection Management *can* catch up to 95% of all threats

- EOP isn't that good – 25-30% increases in SPAM are reported

- *No ability to detect spear-phishing*

- Even Microsoft agrees

- Encryption will become standard by end-of-year

- Just launched optional Advanced Threat Protection (ATP)

ATP completes the picture

Focuses on what's contained *within the email*

Uses a variety of techniques, including machine learning, which haven't yet been disclosed....

Connection Management Layers

Mail Scanning Layers

6 7 8 9 10 11 12

Virus Scanning
Custom Policy
Fingerprint Analysis
Intent Analysis
Image Analysis
Bayesian Analysis
Spam Scoring

ATP might be overkill

- It's expensive - $24/user/year

- It sends content off to be analyzed and protects against malware buried inside – but this can take time

- But EOP vs ATP is only part of the picture

With Microsoft, you are starting over

- You will need to rely on Microsoft's provided lists

- There is no import capability for your existing whitelists

- It is difficult to even *find* blocked mail which you want delivered

- Impacts both whitelists and "ham" emails

What's a "ham" email?

- Looks like spam, but it's not....

- Typical ham emails are bulk emails to which recipients have subscribed, i.e. "trusted senders"

- Inclusion of these senders in "trusted" lists occurs at the user level

- At the IT level, you will be faced with either a flood of spam, or a torrent of frustrated users
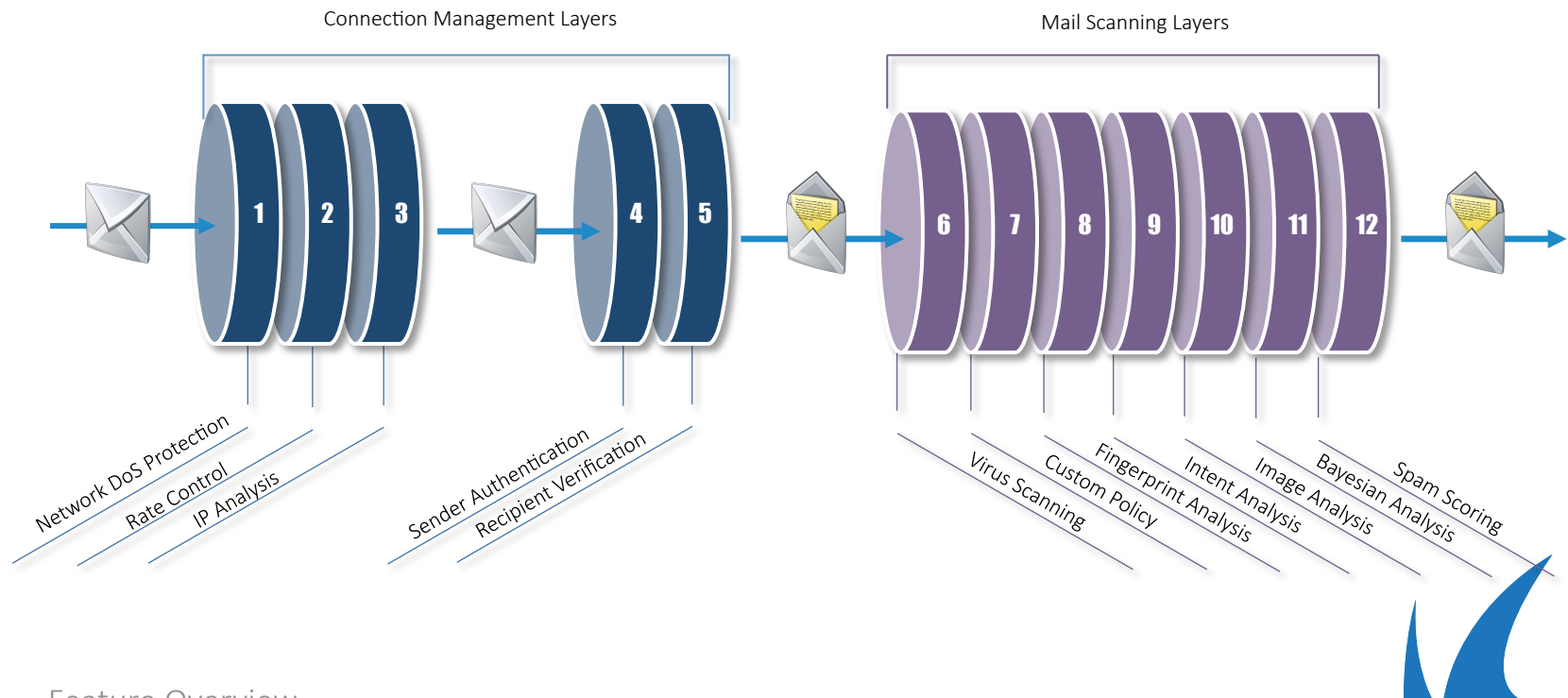
How do Barracuda offerings differ from Microsoft's?

- EOP's security is limited – *spam will get through*

- Barracuda's solutions include anti-phishing inspection

- ATP goes one step further and sandboxes questionable content

- Barracuda adds email continuity – can send and deliver email if Exchange server (or O365) is offline

Barracuda Email Security

- Barracuda Spam Firewall - appliance

- Barracuda Email Security Service – cloud service

Connection Management Layers

Mail Scanning Layers

1 2 3 — 4 5 — 6 7 8 9 10 11 12

Network DoS Protection
Rate Control
IP Analysis

Sender Authentication
Recipient Verification

Virus Scanning
Custom Policy
Fingerprint Analysis
Intent Analysis
Image Analysis
Bayesian Analysis
Spam Scoring

- Feature Overview