Barracuda

SKO FY20

The journey

E-Safe NCAA - Email Security

Scott Berding

Trivia

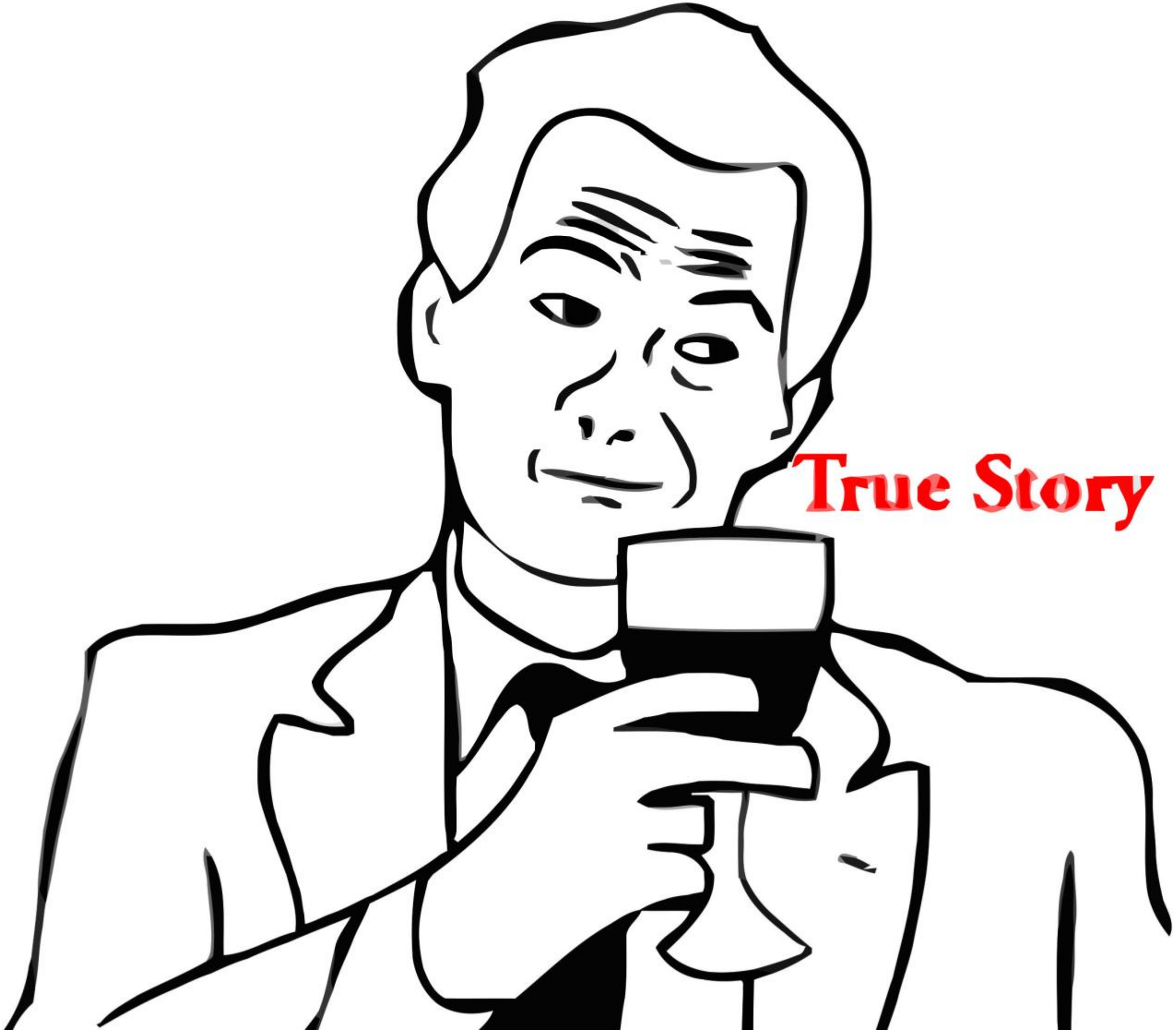
The email security market is a mature market with single digit growth?

False

It’s an $18B market growing at 22%

Trivia

#1 reason for non-adoption of Office 365 is security concerns?



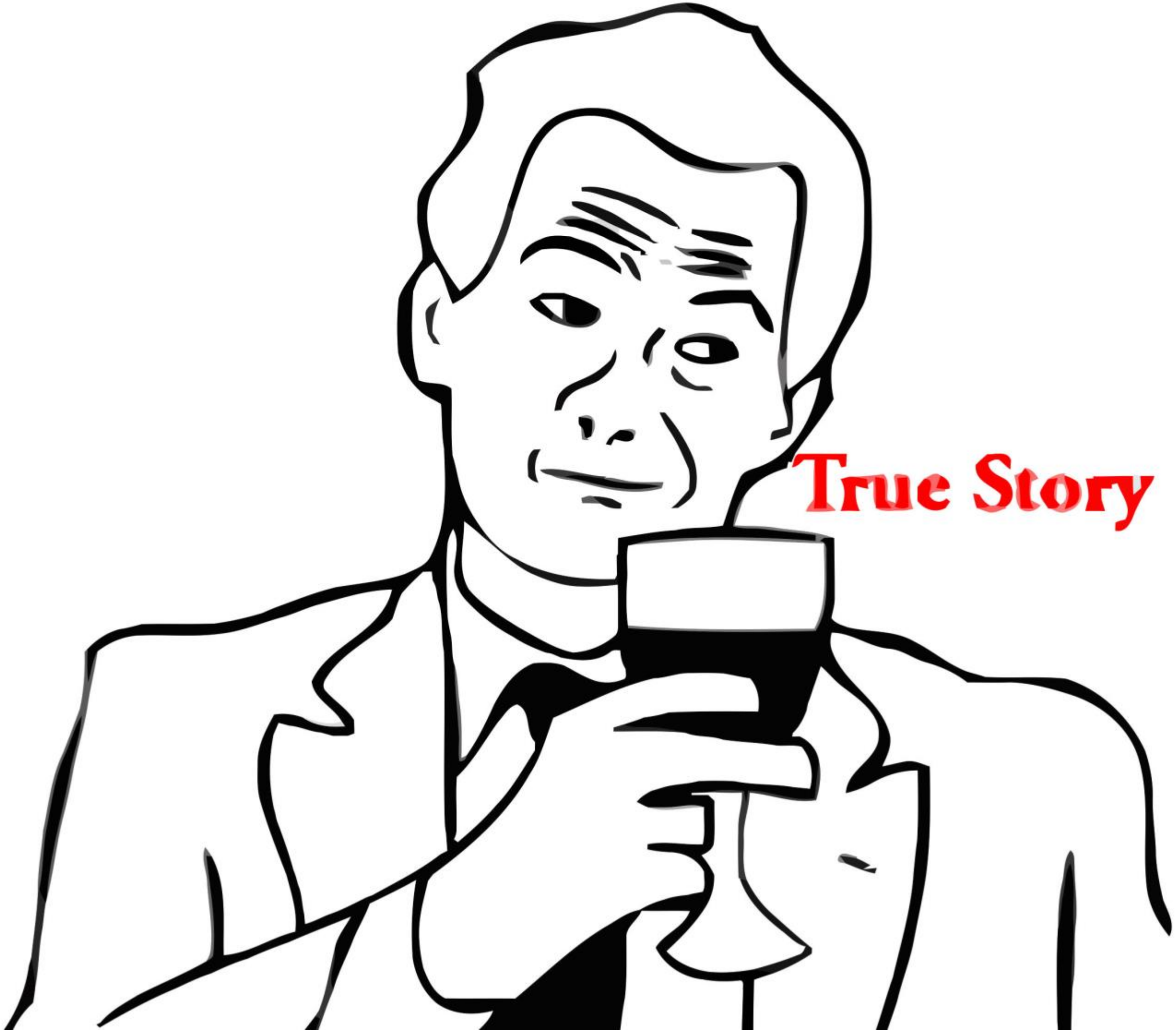
True Story

True

Per Gartner, 37% of businesses say security is biggest blocker for O365 migration

Trivia

A majority of Office 365 users rank email as the number one capability their organization is currently using?



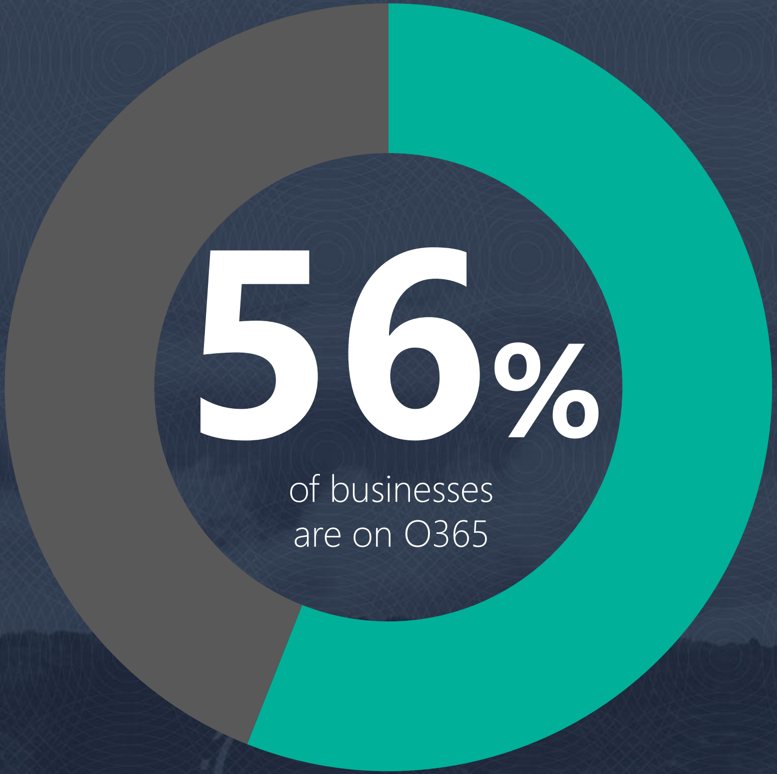
True Story

True

Per Gartner, 51% of businesses say email is the number one capability they are using

The trend to Office 365 continues…

Office 365 adoption is gaining ground



Adoption of Office 365 is growing at **55% YoY**

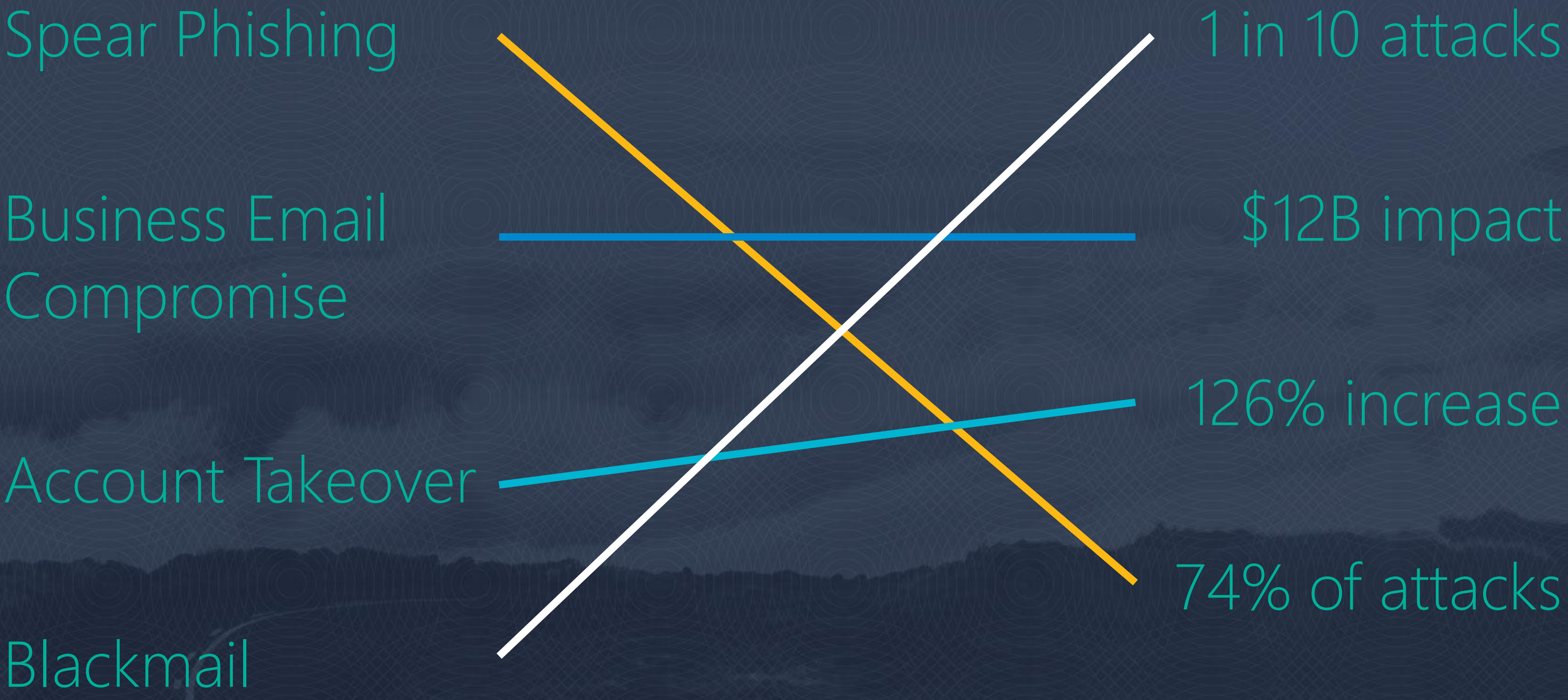
Organizations are evaluating their email security needs with migration

Microsoft native security not enough

Email is thriving. So are advanced threats.

74% *of ALL ATTACKS start with EMAIL*

We live in interesting times



Spear Phishing

Business Email Compromise

Account Takeover

Blackmail

1 in 10 attacks

$12B impact

126% increase

74% of attacks

Let’s recap

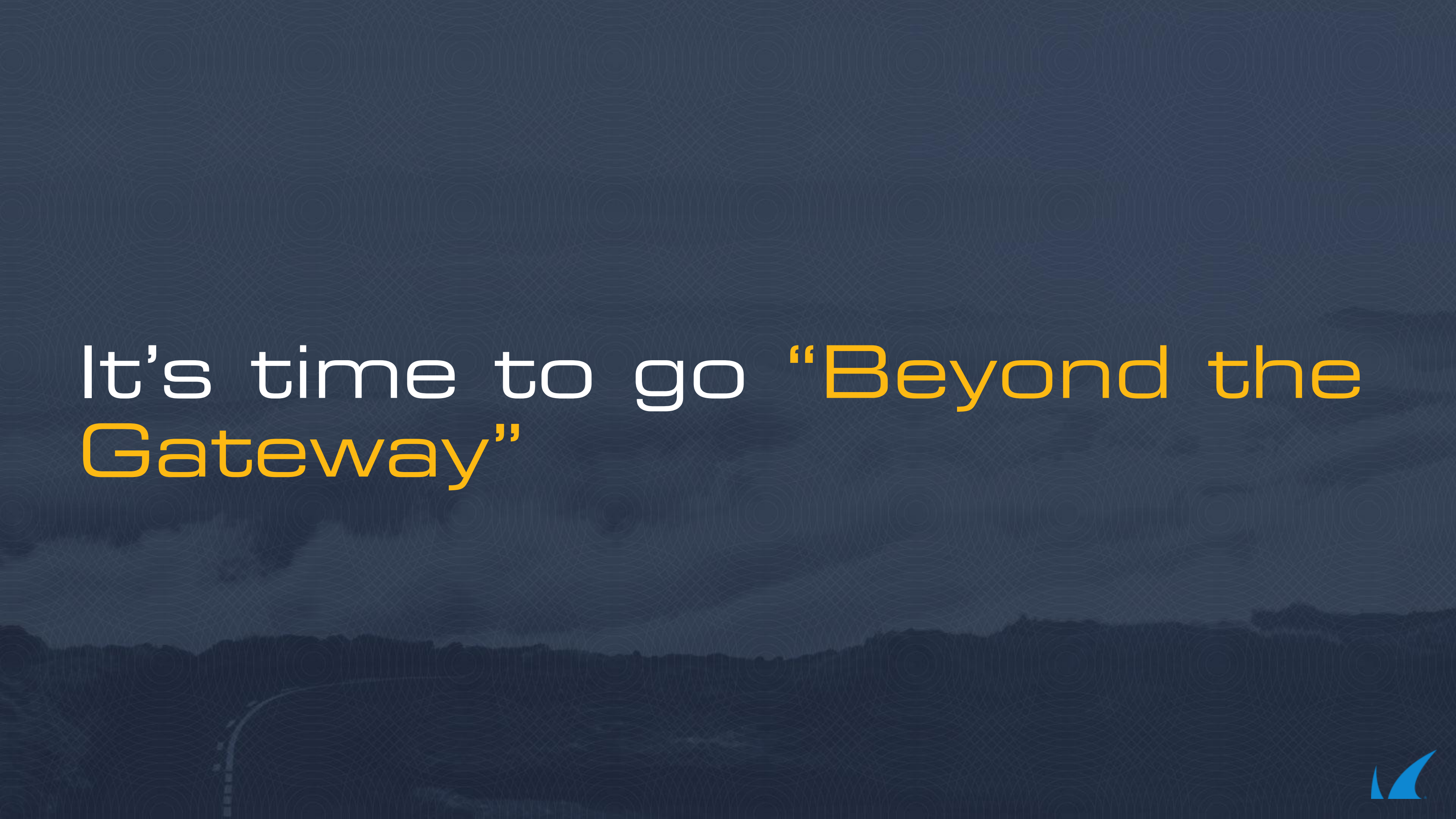
Email security is still a big concern

Microsoft betting future on Office 365

Email remains #1 (application, and threat vector)

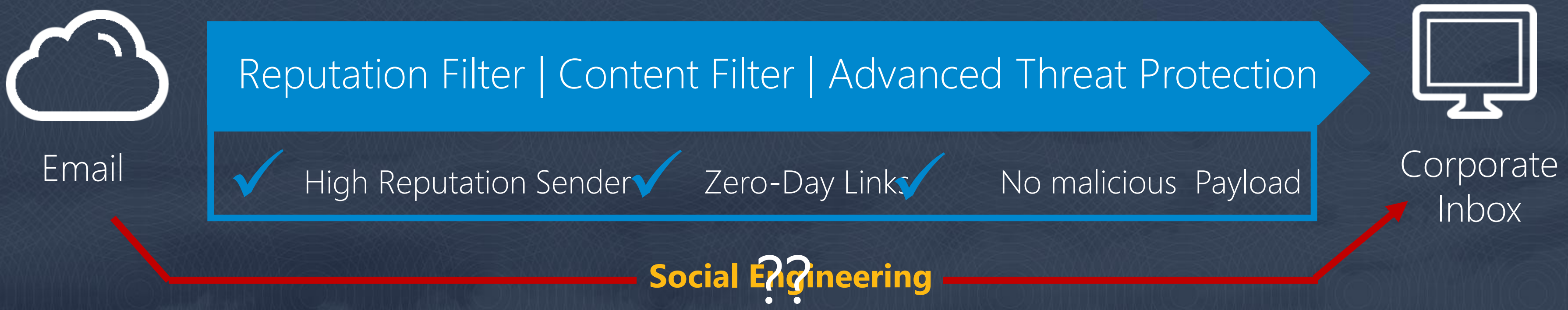
Customers feel the pain of advanced threats

So what does this all mean?



It’s time to go “Beyond the Gateway”

Traditional security losing its relevance



Email

Reputation Filter | Content Filter | Advanced Threat Protection

✓ High Reputation Sender ✓ Zero-Day Links ✓ No malicious Payload

Corporate Inbox

Social Engineering

??

POC: Mimecast vs. Barracuda Sentinel

ALAIN PINEL
REALTORS

Industry:
Real Estate

Employees:
2,500

Region:
United States

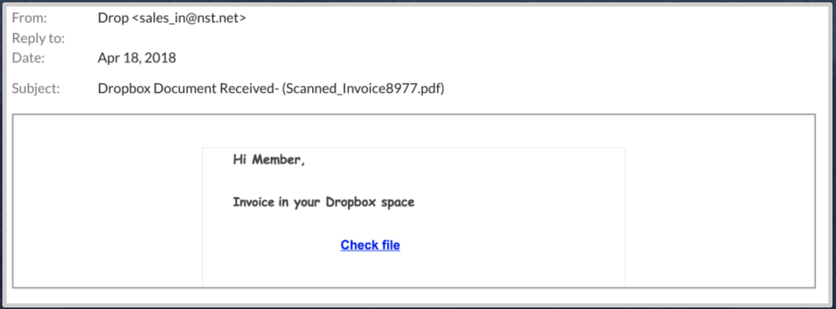
Current Solution:
Mimecast

Background:
Ran Email Threat Scanner on last year's email

Results

- Barracuda Sentinel found *2,391 attacks* not detected by Mimecast over the past year
- Mimecast didn't detect *388 Dropbox attacks* in 1 day
- Mimecast was unable to stop targeted socially engineered attacks

Example



From:	Drop <sales_in@nst.net>
Reply to:	
Date:	Apr 18, 2018
Subject:	Dropbox Document Received- (Scanned_Invoice8977.pdf)

Hi Member,

Invoice in your Dropbox space

Check file

POC: Microsoft ATP vs. Barracuda Sentinel

Fortune 500 Company

Industry:
Manufacturing

Employees:
13,000

Region:
United States

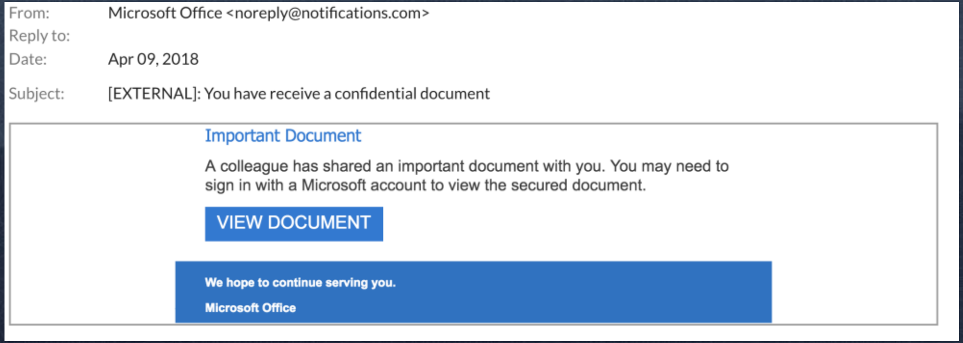
Current Solution:
Microsoft ATP

Background:
Ran Sentinel for one month side by side

Results

- Barracuda Sentinel found *621 attacks* that were not detected by Microsoft ATP
- *366 Microsoft impersonations* missed by Microsoft ATP in one month

Example



From: Microsoft Office <noreply@notifications.com>
Reply to:
Date: Apr 09, 2018
Subject: [EXTERNAL]: You have receive a confidential document

Important Document

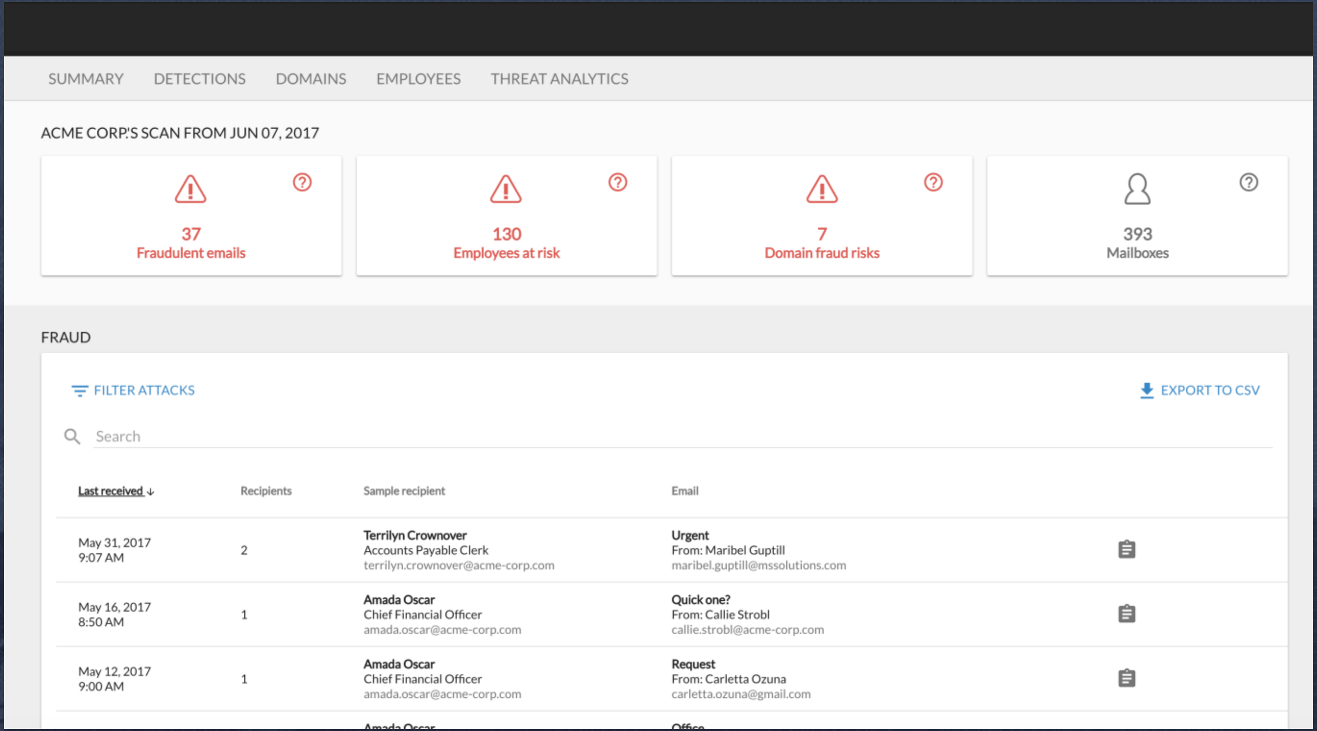
A colleague has shared an important document with you. You may need to sign in with a Microsoft account to view the secured document.

VIEW DOCUMENT

We hope to continue serving you.
Microsoft Office

Silver bullet

Barracuda Email Threat Scanner (ETS) https://scan.barracudanetworks.com/signup



ACME CORP'S SCAN FROM JUN 07, 2017

37 Fraudulent emails

130 Employees at risk

7 Domain fraud risks

393 Mailboxes

FRAUD

Last received ↓	Recipients	Sample recipient	Email
May 31, 2017 9:07 AM	2	**Terrilyn Crownover** Accounts Payable Clerk terrilyn.crownover@acme-corp.com	**Urgent** From: Maribel Guptill maribel.guptill@mssolutions.com
May 16, 2017 8:50 AM	1	**Amada Oscar** Chief Financial Officer amada.oscar@acme-corp.com	**Quick one?** From: Callie Strobl callie.strobl@acme-corp.com
May 12, 2017 9:00 AM	1	**Amada Oscar** Chief Financial Officer amada.oscar@acme-corp.com	**Request** From: Carletta Ozuna carletta.ozuna@gmail.com
		Amada Oscar	**Office**

Are you leveraging the Power of ETS?

Scans Office 365 to identify threats already in users inboxes

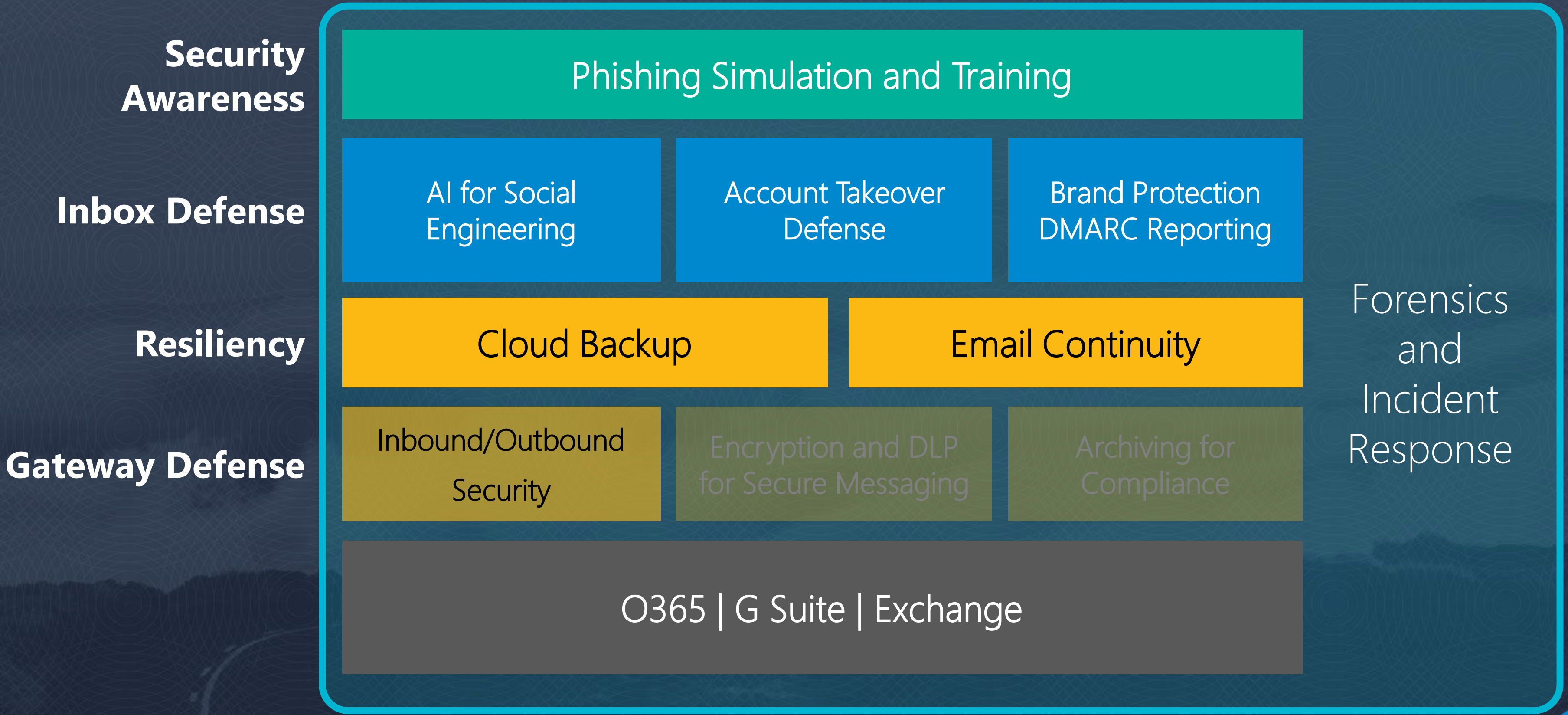
Provides detailed report of all threats discovered

Shows prospects beyond a doubt how gateway security solutions fail to protect

Highlights clear need for ‘beyond the gateway’ security

Proves Barracuda Sentinel provides best protection against advanced threats

Barracuda Complements Microsoft (EOP)



Security Awareness

Phishing Simulation and Training

Inbox Defense

AI for Social Engineering

Account Takeover Defense

Brand Protection DMARC Reporting

Resiliency

Cloud Backup

Email Continuity

Gateway Defense

Inbound/Outbound Security

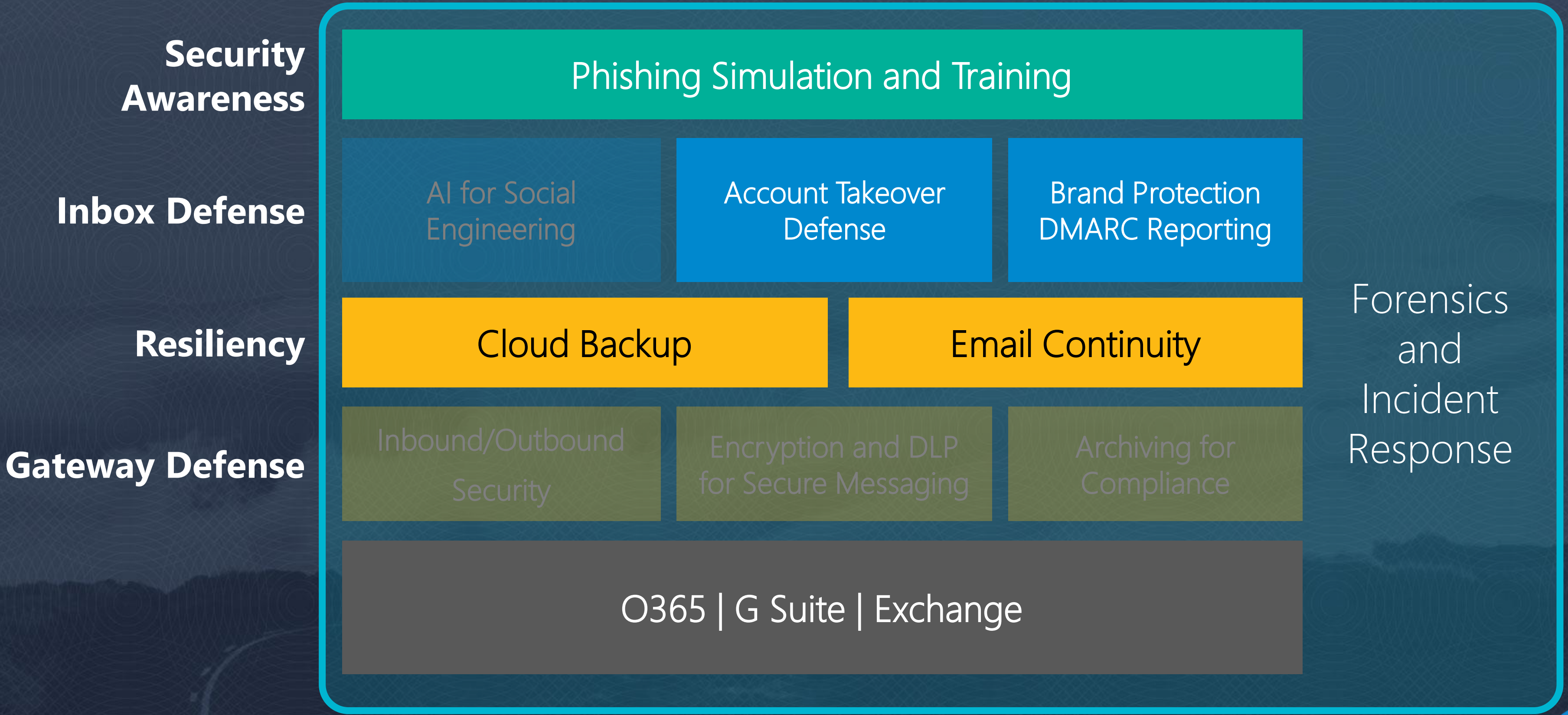
Encryption and DLP for Secure Messaging

Archiving for Compliance

O365 | G Suite | Exchange

Forensics and Incident Response

Barracuda Complements Microsoft (ATP)



Security Awareness

Phishing Simulation and Training

Inbox Defense

AI for Social Engineering

Account Takeover Defense

Brand Protection DMARC Reporting

Resiliency

Cloud Backup

Email Continuity

Gateway Defense

Inbound/Outbound Security

Encryption and DLP for Secure Messaging

Archiving for Compliance

O365 | G Suite | Exchange

Forensics and Incident Response

Discovering customer pain points

Secure inbound/ outbound mail	What are you using for email gateway?
Prevent phishing and account takeover	Do you get spear phishing emails?
Stop domain spoofing	Have you heard on DMARC? Do you have it implemented?
Respond to phishing attacks	How long does it take you to respond to phishing attacks?

Discovering customer pain points

Secure inbound/ outbound mail	Treat Intelligence
Prevent phishing and account takeover	API | Artificial Intelligence | Account takeover protection
Stop domain spoofing	DMARC Reporting
Respond to phishing attacks	Forensics and Incident Response

What is Sender Authentication?

Sender Authentication is a way for mail gateways to determine authenticity of an incoming email. It uses a collection of techniques (SPF, DKIM, DMARC) to provide verifiable information about the origin of the email, as well as validating that the content of an email hasn't been modified in transit.

Operational Issues w/ SPF and DKIM

- Difficult to ensure that every message can be authenticated using SPF or DKIM
- Recipients have difficulty discerning between legitimate and fraudulent emails that don’t authenticate
- Senders have hard time validating their email authentication deployments
- Even when SPF and DKIM are configured properly, email receivers are reluctant to reject unauthenticated messages.

Sender Policy Framework

SPF or Sender Policy Framework is used to determine whether or not an email originated from a mail server that the domain owner has authorized, whether it's their own mail server or a 3rd party hosted solution

SPF consists of a TXT record in DNS called a "SPF Record"

A SPF record is made up of three parts:

- The version of SPF
- The mechanism(s) permitted to send messages for the given domain
- The qualifier at the end of the SPF record

SPF: Lets Break it Down

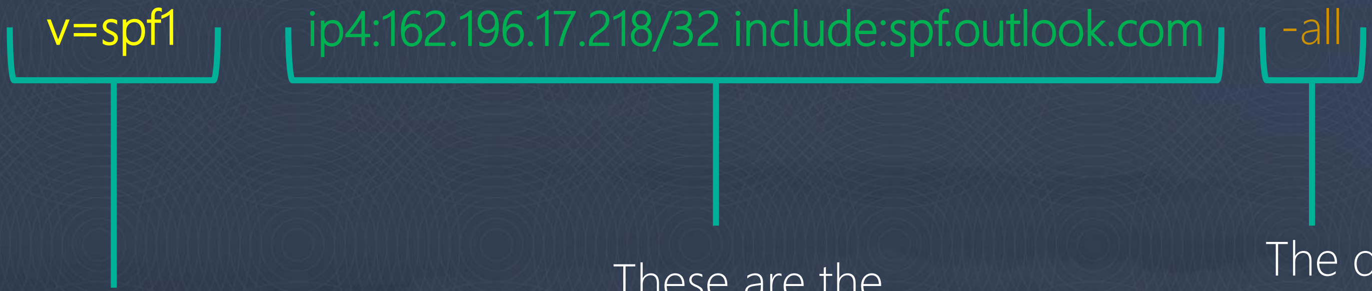
Version – There is only one version of SPF in use today (v=spf1)

Mechanism – There are eight different mechanisms defined in RFC. You will typically only see/use four (4) of them.

Qualifier – Each mechanism can be combined with a qualifier. There are four (4) qualifiers, but only two are commonly used

SPF: Lets Break It Down

+ for a PASS result
? for a NEUTRAL result (No Policy)
~ for SOFTFAIL
- for FAIL



v=spf1 ip4:162.196.17.218/32 include:spf.outlook.com -all

This is the version of SPF to use. It must come at the start of the SPF record

These are the mechanisms which specify where an email is authorized to originate from.

The qualifier comes last and indicates what you want done with an email that doesn't match any mechanism(s)

A	If the domain name has an address record (A or AAAA) that can be resolved to the sender's address, it will match.
IP4	If the sender is in a given IPv4 address range, match.
IP6	If the sender is in a given IPv6 address range, match.
MX	If the domain name has an MX record resolving to the sender's address, it will match
PTR	*Deprecated – Do Not Use*
EXISTS	*Do Not Use*
INCLUDE	References the policy of another domain.

SPF: Tips and Tricks

- SPF checks are performed against the ENVELOPE FROM domain.
- SPF does not survive mail-forwards
- You can only have one SPF record in DNS
- You can link multiple SPF records together with INCLUDE statements
- There is a limit of 10 DNS queries
- SPF is outlined in RFC 7208 - https://tools.ietf.org/html/rfc7208

SPF: Tools

With an IP and email address, you can test to see what the results of a SPF check would be

https://vamsoft.com/support/tools/spf-policy-tester

The test will go through and break down the SPF record line by line as it tests each mechanism.

Try it out! Put in your Barracuda email and an IP and see what happens. If you want it to pass, use 64.235.144.25

DomainKeys Identified Mail

DomainKeys Identified Mail or DKIM is a way for senders to digitally “sign” their emails. It uses public key cryptography to ensure that emails sent over the Internet are not altered in transit. The presence of a valid DKIM signature also provides a certain level of trust to the email.

DKIM: Lets Break it Down

When an email is sent to a recipient, the email software generates a signature based on the content of the message and the sender's private key. The signature is added to the email header and the message is sent to the recipient.

An example signature is shown below:

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=default;
    c=relaxed/simple; q=dns/txt; l=1234; t=1117574938; x=1118006938;
    h=from:to:subject:date:keywords:keywords;
    bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
    b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

DKIM: Lets Break it Down

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=default;
    c=relaxed/simple; q=dns/txt; l=1234; t=1117574938; x=1118006938;
    h=from:to:subject:date:keywords:keywords;
    bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
    b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

Field	Description
v	Version
a	Signing algorithm
d	Domain
s	Selector
c	Canonicalization algorithm for the header and body
q	Default query method
l	Length of the canonicalized part of the signed message body
t	Signature timestamp
x	Expiration time
h	List of signed header fields

d= : This is the domain that signed the email

s= : The selector used to find the corresponding public key in DNS

b= : The actual digital signature of the contents (headers and body) of the mail message

bh= : The body hash

DKIM: Tips and Tricks

- DKIM signing is only natively available in Office 365 and Google.
- Office 365 (by default) signs emails with the onmicrosoft domain
- There can be multiple DKIM signatures in an email
- DKIM *will* survive mail forwarding
- DKIM is needed for effective DMARC implementation

DKIM: Tools

Validating a DKIM signature can be tricky, especially if the customer is using a link protection service.

You must use the RAW source code prior to any modifications by the email gateway

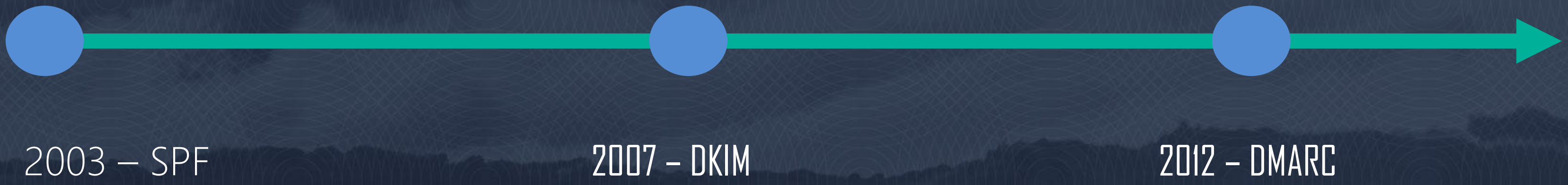
To validate a DKIM signature, you must take the entire source code and paste it into a DKIM testing tool

Here is a good site to use to check DKIM signatures - http://www.appmaildev.com/site/testfile/dkim

DMARC

DMARC stands for Domain-based Message Authentication, Reporting, and Conformance.

It is slowly becoming the new standard for sender authentication. It is the evolution of SPF and DKIM



2003 – SPF

2007 – DKIM

2012 – DMARC

DMARC: SPF/DKIM are Insufficient

SPF/DKIM do not cover all use cases, e.g.

- SPF: Forwarding and Mailing Lists
- DKIM: Emails modified by mailing lists and gateways

Admins do not have visibility into misconfigurations

↓

Email recipients experience false positives

↓

Email recipients do not consistently respect SPF/DKIM

DMARC: How does it help?

DMARC integrates with existing inbound email authentication processes. It helps email recipients to determine if a message *aligns* with what the receiver knows about the sender. If not, DMARC includes guidance on how to handle the *non-aligned* messages

DMARC is designed to satisfy the following requirements:

- Minimize false positives
- Provide robust authentication reporting
- Assert sender policy at receivers
- Reduce successful phishing delivery
- Work at Internet scale
- Minimize complexity

DMARC: What does it look like?

A DMARC record is a TXT record in DNS, just like SPF.

It will always use the sub-domain “_dmarc”. For example, _dmarc.barracuda.com

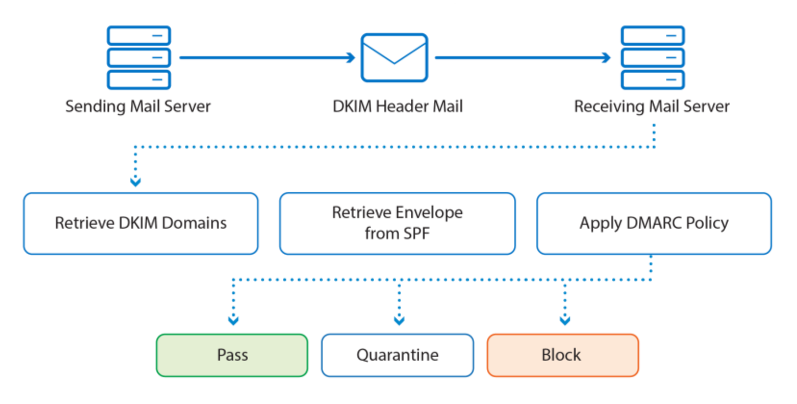
There are nine different tags you can use, but only two are required.

```
"v=DMARC1; p=none; fo=1;
rua=mailto:rua+barracuda.com@dmarc.barracudanetworks.com;
ruf=mailto:ruf+barracuda.com@dmarc.barracudanetworks.com"
```

Tag Name	Required?	Purpose	Sample
v	required	Protocol version	v=DMARC1
p	required	Policy for domain (can be none, quarantine, or reject)	p=quarantine
pct	optional	% of messages subjected to filtering	pct=20
rua	optional	Reporting URI of aggregate reports	rua=mailto:rua+barracuda.com@dmarc.barracudanetworks.com
ruf	optional	Addresses to which message-specific forensic information is to be reported (comma-separated plain-text list of URIs).	ruf=mailto:ruf+barracuda.com@dmarc.barracudanetworks.com
rf	optional	Format to be used for message-specific forensic information reports (comma-separated plain-text list of values).	rf=afrf
aspf	optional	Alignment mode for SPF	aspf=r
adkim	optional	Alignment mode for DKIM	adkim=r
fo	optional	Dictates what type of authentication and/or alignment vulnerabilities are reported back to the Domain Owner	fo=1

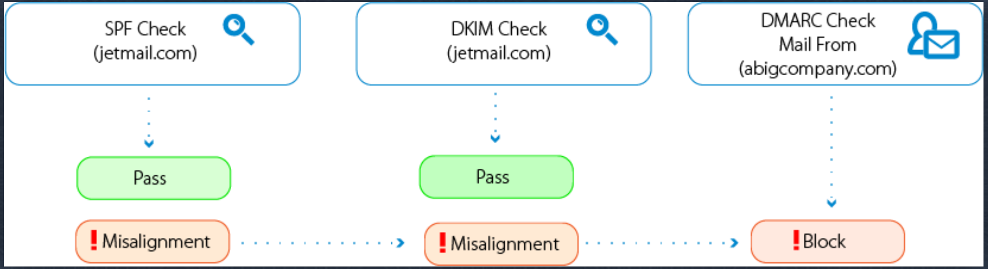
DMARC: How does it work?

DMARC takes SPF/DKIM a step further by ensuring alignment between the HEADER FROM and either the ENVELOPE FROM *or* the DKIM domain.



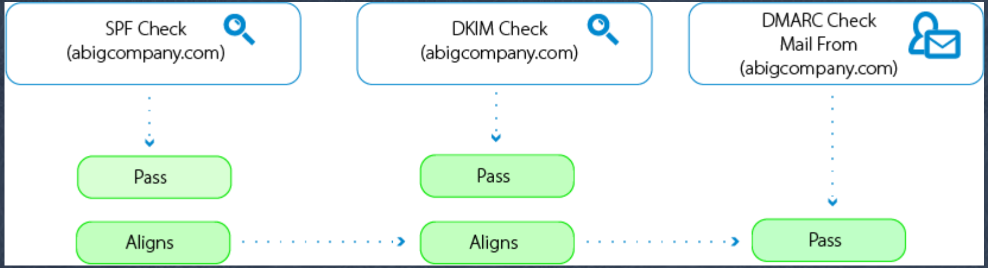
1. DKIM domain is retrieved from signature (d=domain.com) and public key is used to authenticate the email. Results are recorded
2. Envelope domain is retrieved and SPF record check is performed. Results are recorded.
3. Domain in Header From address is compared to both the DKIM domain and the SPF (envelope) domain.
4. If the Header From matches either the SPF *or* DKIM domain *and* that respective check passed, then the DMARC policy is applied.

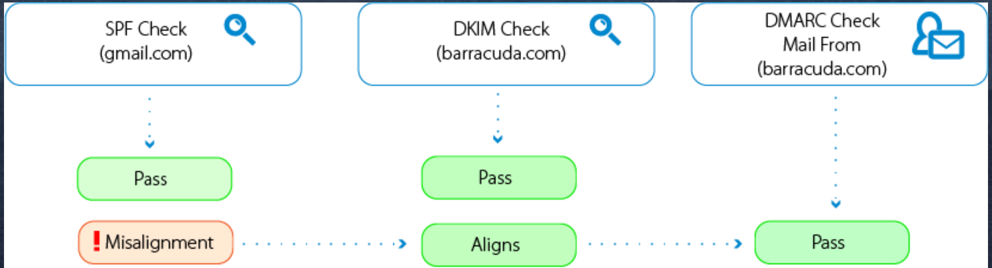
DMARC: Examples



SPF, DKIM, and DMARC checks are made against ABigCompany's email. Both SPF and DKIM checks pass. However, the DMARC check fails due to misalignment.

SPF, DKIM, and DMARC checks are made against ABigCompany's email. Both SPF and DKIM checks pass. This time, the mail from domain aligns with the SPF and DKIM domains and the DMARC check passes.





SPF and DKIM both pass, but SPF does not align. Since DKIM aligns, DMARC passes.

DMARC: A Unified Framework

Admin gets visibility into senders using her domain

- Put control back in admin's hands

Helps fix misconfigurations

- Builds confidence in correctness of SPF/DKIM setup
- Enhance email deliverability

Communicates unauthenticated email policy to recipients

- Demonstrates the sender's configuration is trustworthy

Leverages both DKIM and SPF

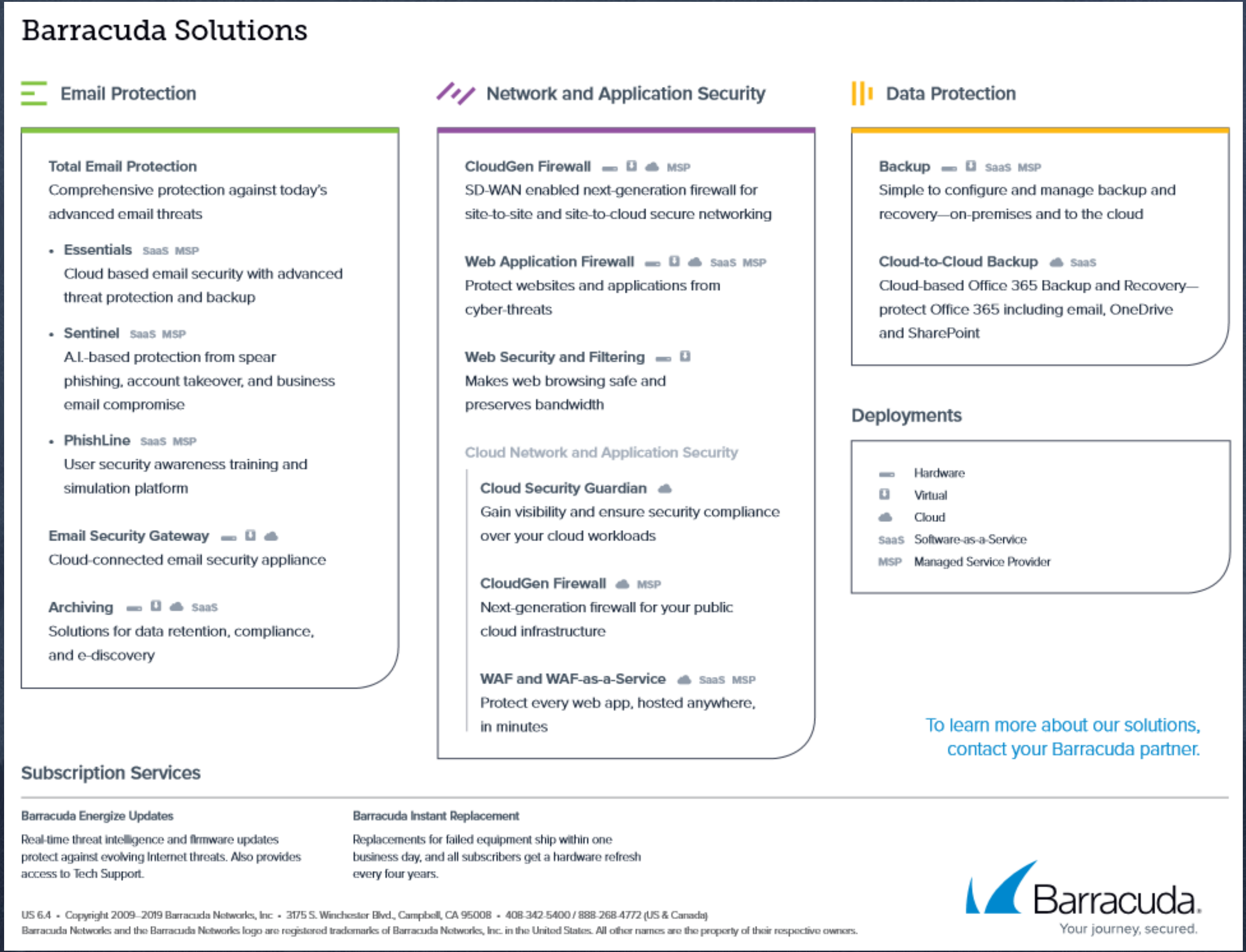
- Best of both worlds

DMARC in Essentials and Sentinel

Within Essentials, we offer the ability for the administrator to authenticate inbound messages against SPF, DKIM and DMARC.

Within Sentinel, we offer the reporting piece for DMARC to give administrators insight into their domain use/misuse.

tldr: Essentials enforces and Sentinel reports



Barracuda Solutions

Email Protection

Total Email Protection
Comprehensive protection against today's advanced email threats

- **Essentials** SaaS MSP
  Cloud based email security with advanced threat protection and backup
- **Sentinel** SaaS MSP
  A.I.-based protection from spear phishing, account takeover, and business email compromise
- **PhishLine** SaaS MSP
  User security awareness training and simulation platform

Email Security Gateway ▬ ▣ ☁
Cloud-connected email security appliance

Archiving ▬ ▣ ☁ SaaS
Solutions for data retention, compliance, and e-discovery

Network and Application Security

CloudGen Firewall ▬ ▣ ☁ MSP
SD-WAN enabled next-generation firewall for site-to-site and site-to-cloud secure networking

Web Application Firewall ▬ ▣ ☁ SaaS MSP
Protect websites and applications from cyber-threats

Web Security and Filtering ▬ ▣
Makes web browsing safe and preserves bandwidth

Cloud Network and Application Security

Cloud Security Guardian ☁
Gain visibility and ensure security compliance over your cloud workloads

CloudGen Firewall ☁ MSP
Next-generation firewall for your public cloud infrastructure

WAF and WAF-as-a-Service ☁ SaaS MSP
Protect every web app, hosted anywhere, in minutes

Data Protection

Backup ▬ ▣ SaaS MSP
Simple to configure and manage backup and recovery—on-premises and to the cloud

Cloud-to-Cloud Backup ☁ SaaS
Cloud-based Office 365 Backup and Recovery—protect Office 365 including email, OneDrive and SharePoint

Deployments

▬	Hardware
▣	Virtual
☁	Cloud
SaaS	Software-as-a-Service
MSP	Managed Service Provider

To learn more about our solutions, contact your Barracuda partner.

Subscription Services

Barracuda Energize Updates
Real-time threat intelligence and firmware updates protect against evolving Internet threats. Also provides access to Tech Support.

Barracuda Instant Replacement
Replacements for failed equipment ship within one business day, and all subscribers get a hardware refresh every four years.

Barracuda
Your journey, secured.

Thank you

Barracuda.

SKO FY20

The journey