

Suite completa per la gestione di 365

Email Security/Dati/Compliance



Luca Bin
Senior EMEA Solution Architect
Lbin@barracuda.com



Barracuda Solution Framework

Managed Services / XDR

Deployment Choices / Flexible Consumption

Email Protection

Spam, Malware, Threats

Phishing & Impersonation

Account Takeover

Incident Response

Security Awareness

Data Protection

Backup

Archiving

Data Classification

Network Protection

Secure Access Service Edge

Zero Trust Security

Secure SD-WAN

Network Firewalls

IoT/OT Security

Application Protection

OWASP Top 10

Bot Protection

DDoS Protection

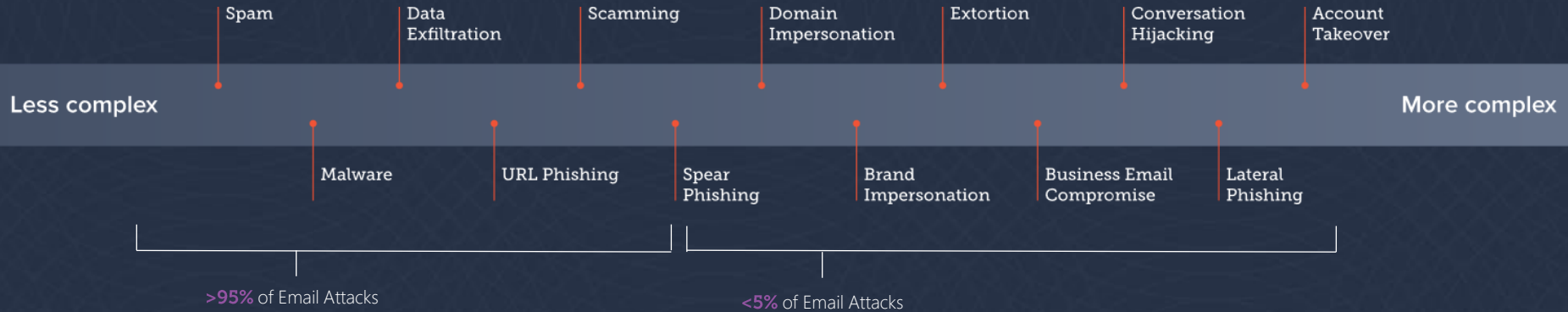
Client-side Protection

API Security

Product Platforms

Threat Intelligence Platform

13 Tipi di minacce e-mail



Esempi di tipi di attacchi

Data exfiltration

Your iCloud Storage is almost full

Help (small fontline),

Your iCloud storage is almost full. You have **772.7 MB** remaining of **50 GB** total storage.

Upgrade to 200 GB for \$2.99/Month

Your iCloud storage is used for iCloud Photos, iCloud Mail and to keep the most important things on your iPhone, iPad, and iPod touch safe and available, even if you lose your device. iCloud Drive, and apps like Keynotes, Pages, and Numbers also use iCloud storage to keep your files up-to-date everywhere.

To continue to use iCloud and to back up your photos, documents, contacts, mail, and more, you need to [upgrade your iCloud storage plan](#) or reduce the amount of storage you are using.

The iCloud Team


Do you even have an iCloud account? Scammers will often make claims like this to get you to react.

If you're not sure if this is the case, check your storage by visiting the actual source, not by clicking the link.

Copy is designed to create anxiety over losing important files and get you to act.

Overall, this is a sophisticated phish, but being skeptical and keeping your emotions in check can help you avoid falling for it.

URL phishing

**ALERT: VERIFICATION REQUIRED**
USPS is in possession of an item intended for you.

PACKAGES

PACKAGE DETAILS:
COMPANY: AMAZON.COM
TRACKING NO: 7140138402048-24
FROM: HICKSVILLE, TENNESSEE 37011
WEIGHT: 4.67 LBS

In order for the USPS to complete this delivery, we need you to **verify your information**. Once we've received confirmation on the missing details, we will release this from our shipping center for delivery.

VERIFY INFORMATION

You may have more mail or packages than are shown in your Daily Digest. To check, go to your **Dashboard** »

An email that looks official and asks you to verify account details or personal information is likely a savvy scam.

Do you have a package coming? If so, be wary and verify delivery method with sender. If not, this is a scam.

Legitimate organizations rarely ask for verification by email. Positioning this as a hold further indicates a possible scam.

Clicking this button will take you to a fake page or site designed to steal the information you provide.

Scamming

Greetings (Name:Full Name),

My name is Mike Johnson and I am an investment broker. I want to inform you that I represent an investment Group called Pillar Five Investments. We are expanding our global presence by investing in viable projects across the globe, as well as assisting businesses to grow in this trying time of the covid 19 pandemic. We are willing to inject \$1 million to \$300 million or more in a viable project.

We grant our funding at a 4% ROI per annum for 10 years and 12 months maturities. If you have a viable project that needs funding, kindly get back to us with your business plan and executive summary for our review and possible funding.

Regards,





Mike Johnson
Chief Executive/Broker

▶ An email that arrives unsolicited offering financial rewards is always some form of scam.

▶ Don't be fooled by highly technical or sophisticated content that's designed to entice you to act.

▶ The highly designed logo, header and 'personalized' sign-off look convincing, but a web search of the company and sender would reveal they don't exist.

Extortion

Vulnerability Scan Required

Attention User:

To ensure the integrity of our corporate network, we operate firewall technology that protects us from external threats.

Recent internet activity from workstation has caused a breach in our firewall security. To prevent further issues, your network connection has been disabled until the activity can be reviewed and analyzed.

For more details on this breach, please see the link below.

Thank you for your support on this matter.

[Corporate Systems Group]

Scan your system now

Extortionists use alarming content and graphics to catch targets off guard and create fear.

The email content creates anxiety in an effort to elicit a response, in this case clicking the button below.

Clicking this button would likely launch or further some type of attack.

Spear Phishing

You've been nominated!

Dear [email:firstName][email:lastName],

We are pleased to inform you that a colleague of yours has nominated you to be a feature profile in our [online magazine](#) on most influential thought leader of the year!

We carefully select our nominees based on a number of factors including professional accomplishments and industry achievements – and we are happy to say that based on our research, our editorial staff truly your combination of business skills and leadership make you more worthy of our nomination.

Our readers are achievers, and a profile in our publication will put you in touch with some of the most successful and well connected professionals in your industry. It would also give us the opportunity to share your story as well as insights into the life of a successful executive.

Simply [click here](#) to learn more about it for your time and consideration.

Sincerely,
Professionals Org. Editorial Staff



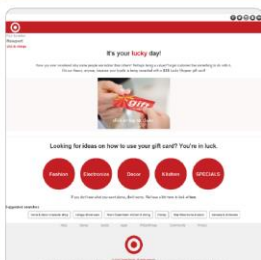
- Nominations of any kind are an appeal to ego used by spear phishers designed to get you to engage.
- A personalized email with flattering copy is an attempt to create an emotional connection.
- Spear phishers use personal information freely available online to craft targeted content.
- The highly designed logo and email look convincing, but a web search of the organization would reveal it doesn't exist.

Domain Impersonation

[illegible]

Esempi di tipi di attacchi

Brand impersonation



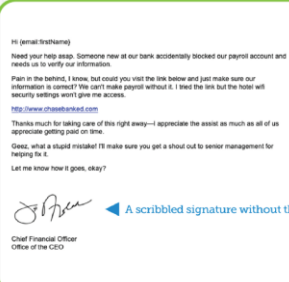
Effective brand impersonation is difficult to detect when logos and branding are mimicked properly.

Be skeptical of any offers that promise rewards or gift cards, even if the email looks convincing.

Multiple opportunities to click are common in phishing emails.

Sometimes details, or a lack of them, indicate that something's not right. Study the entire email, as well as the domain name, for irregularities.

Business Email Compromise



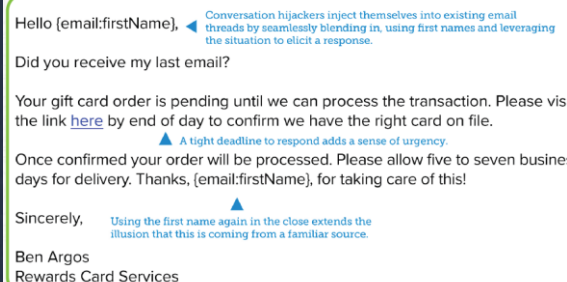
Business email compromise scams usually involve urgent requests from 'higher-ups' in an effort to get targets to respond to authority.

A fake domain name, easily overlooked, leads to a fake website that will track and keep account details.

The promise of recognition by senior management is a strong incentive to engage.

A scribbled signature without the printed counterpart is an attempt to look authentic.

Conversation hijacking



Conversation hijackers inject themselves into existing email threads by seamlessly blending in, using first names and leveraging the situation to elicit a response.

Did you receive my last email?

Your gift card order is pending until we can process the transaction. Please visit the link [here](#) by end of day to confirm we have the right card on file.

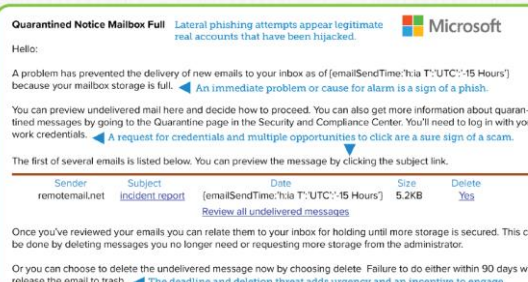
A tight deadline to respond adds a sense of urgency.

Once confirmed your order will be processed. Please allow five to seven business days for delivery. Thanks, (email:firstName), for taking care of this!

Sincerely, Using the first name again in the close extends the illusion that this is coming from a familiar source.

Ben Argos
Rewards Card Services

Lateral Phishing



Quarantined Notice Mailbox Full Lateral phishing attempts appear legitimate real accounts that have been hijacked.

Hello:

A problem has prevented the delivery of new emails to your inbox as of (emailSendTime:'t:ia T:UTC':-15 Hours) because your mailbox storage is full. An immediate problem or cause for alarm is a sign of a phishing.

You can preview undelivered mail here and decide how to proceed. You can also get more information about quarantined messages by going to the Quarantine page in the Security and Compliance Center. You'll need to log in with your work credentials. A request for credentials and multiple opportunities to click are a sure sign of a scam.

The first of several emails is listed below. You can preview the message by clicking the subject link.

Sender	Subject	Date	Size	Delete
remotemail.net	incident report	(emailSendTime:'t:ia T:UTC':-15 Hours)	5.2KB	Yes

[Review all undelivered messages](#)

Once you've reviewed your emails you can relate them to your inbox for holding until more storage is secured. This can be done by deleting messages you no longer need or requesting more storage from the administrator.

Or you can choose to delete the undelivered message now by choosing delete. Failure to do either within 90 days will release the email to trash. The deadline and deletion threat adds urgency and an incentive to engage.

Account Takeover



Brand impersonation lends a sense of authenticity to the email. Pay close attention to irregularities in logos, brand colors and copy tone to detect fakes.

This is a mandatory service verification

We detected something unusual about a recent unsuccessful multiple login attempt on (email:address)

Account takeover can begin with a phishing attempt to gain login credentials and other sensitive information.

For your safety, an additional security step is required. Click on the verify button below to authenticate your account.

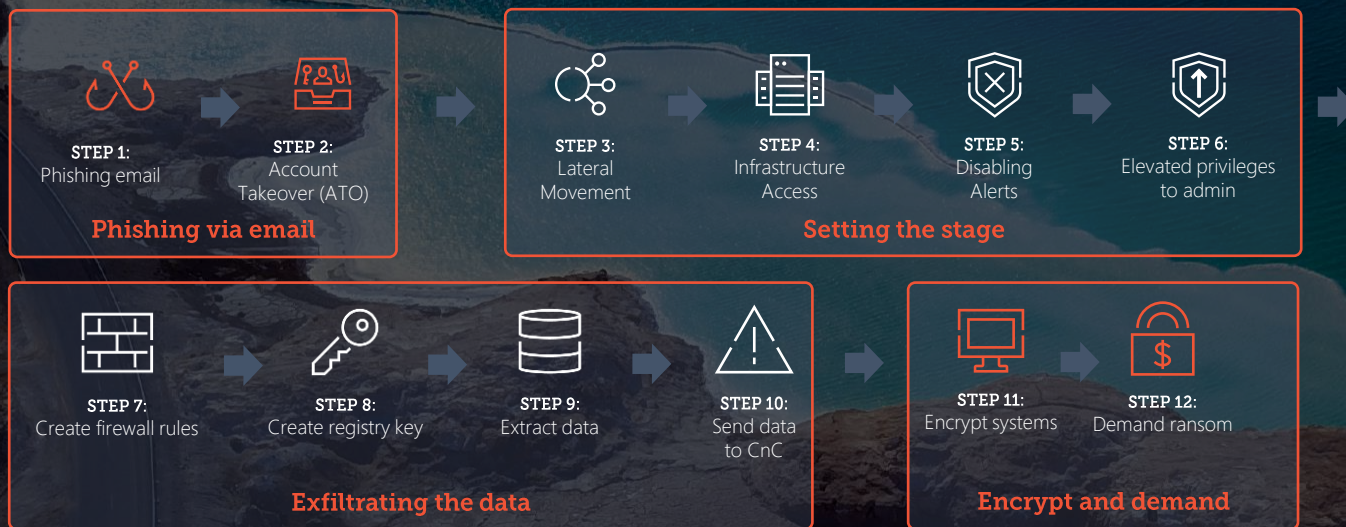
Verify (email:address) Any request to verify information should be greeted with skepticism.

If this wasn't you, we'll help you secure your account. If this was you, we'll boost online activity in the future.

By recognizing the signs of phishing emails like this one, you can stop account takeover from happening before it starts.



Exempio di ransomware attack chain



Barracuda's integrated approach to securing Microsoft 365

THREAT PREVENTION

Spam, Malware, and ATP
Phishing and Impersonation Protection
Account Takeover Protection
Domain Fraud Protection

DETECTION AND RESPONSE

Incident Response
Security Awareness Training

DATA PROTECTION AND COMPLIANCE

Email Encryption and DLP
Cloud-to-Cloud Backup
Cloud Archiving Service
Data Inspector™



Barracuda
Email Protection™



Impersonation Protection

Come agisce?

Machine Learning: best for targeted attacks



Inbox Tecnologia di difesa

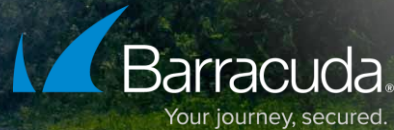


multiple classifiers



Avere Evidenza

Apriamo la scatola nera.....



Email Threat Scanner

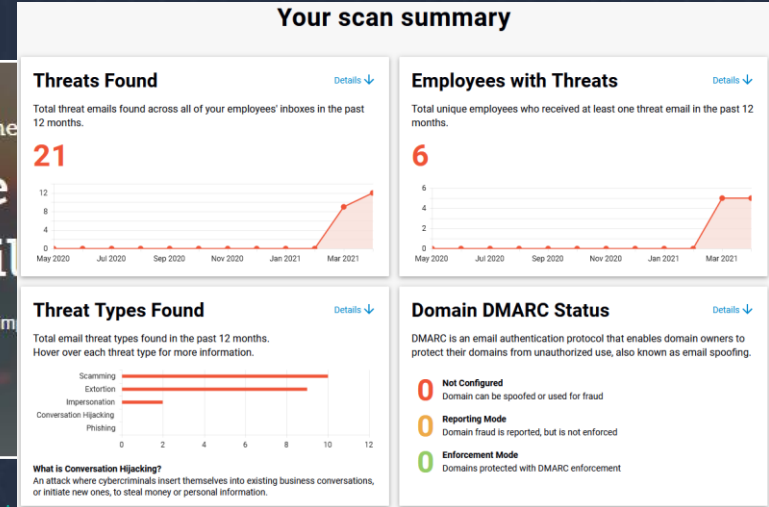
Barracuda Email Threat Scanner

Serious threats may be in your Office 365 mailbox

Scan your Office 365 environment. It's fast, free and safe—with no impact on your mailbox.

[SCAN YOUR EMAIL NOW](#)

<https://scan.barracudanetworks.com>



Domain Fraud Protection

SPF versus DKIM versus DMARC



Requirements for senders to Google recipients

All sender domains

Over 5k messages

- SPF for email authentication
- OR**
- DKIM for message integrity
 - Valid PTR records for each sending IP
 - TLS encryption required
 - Spam rate < 0.1%; never to reach 0.3%+
 - Cannot impersonate Gmail

- SPF for email authentication
- AND**
- DKIM for message integrity
 - Valid PTR records for each sending IP
 - TLS encryption required
 - Spam rate < 0.1%; never to reach 0.3%+
 - Cannot impersonate Gmail
 - Must have DMARC policy
 - Messages must pass DMARC alignment
 - One-click unsubscribe

Incident Response

Controllo e Rimedio dopo la consegna.....



Threat hunting:

Enable proactive threat discovery based on new and shared intelligence

Remediation:

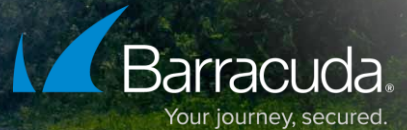
Simplify the process of removing unwanted email post-delivery.

Automation:

Automate the process of threat discovery and clean-up and continuously improve your security

Monitoraggio h24

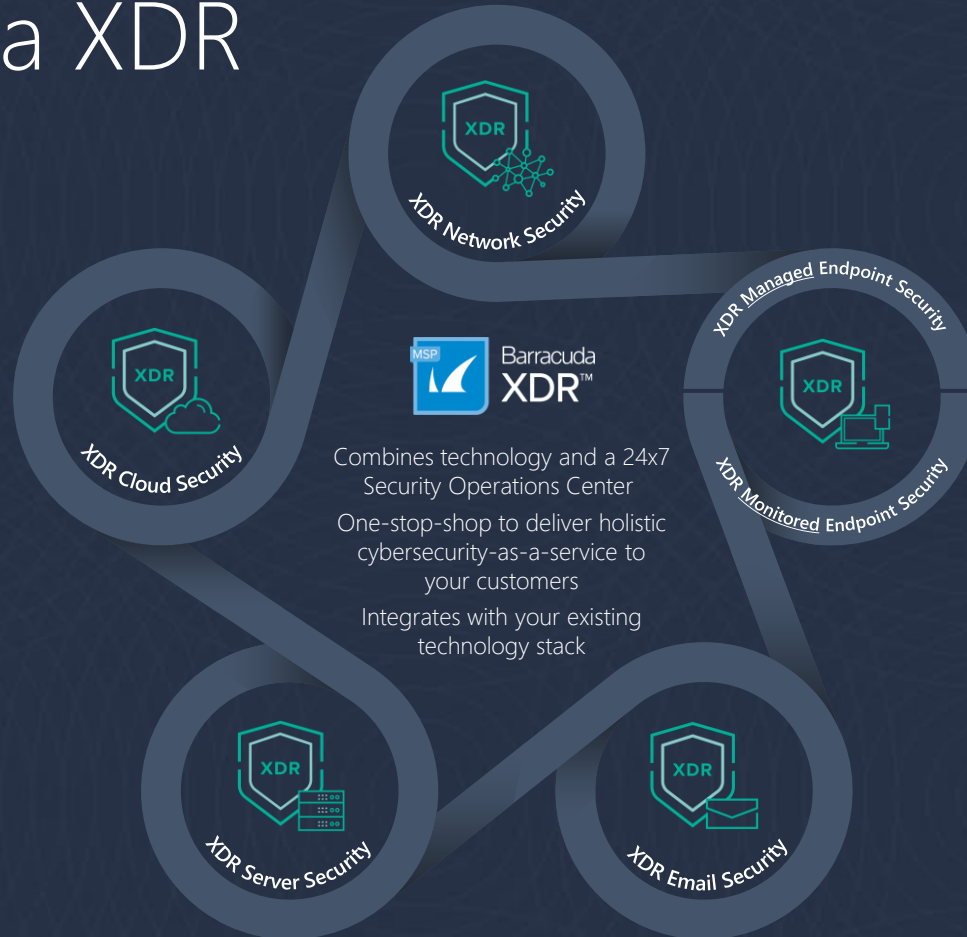
Il Lavoro dell' IT aziendale



Come ci vedono gli utenti....e come siamo



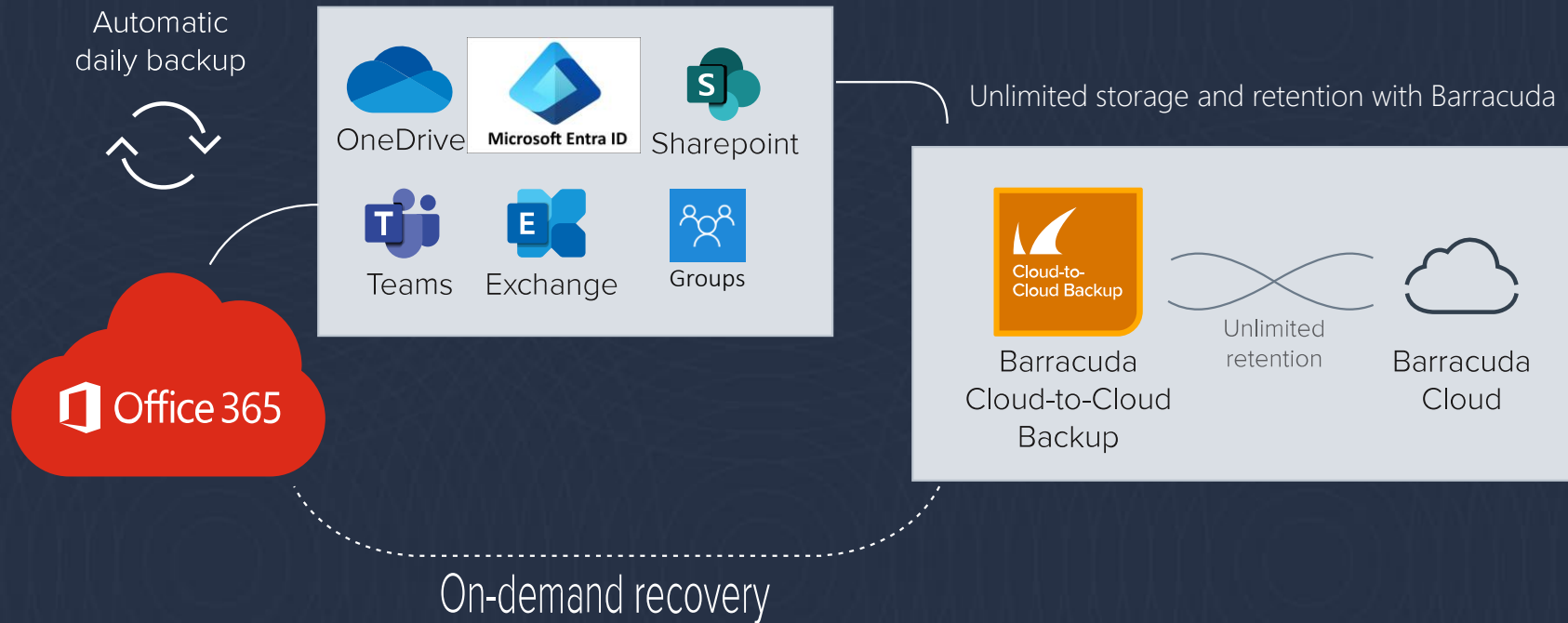
Barracuda XDR



Backup and Archiving

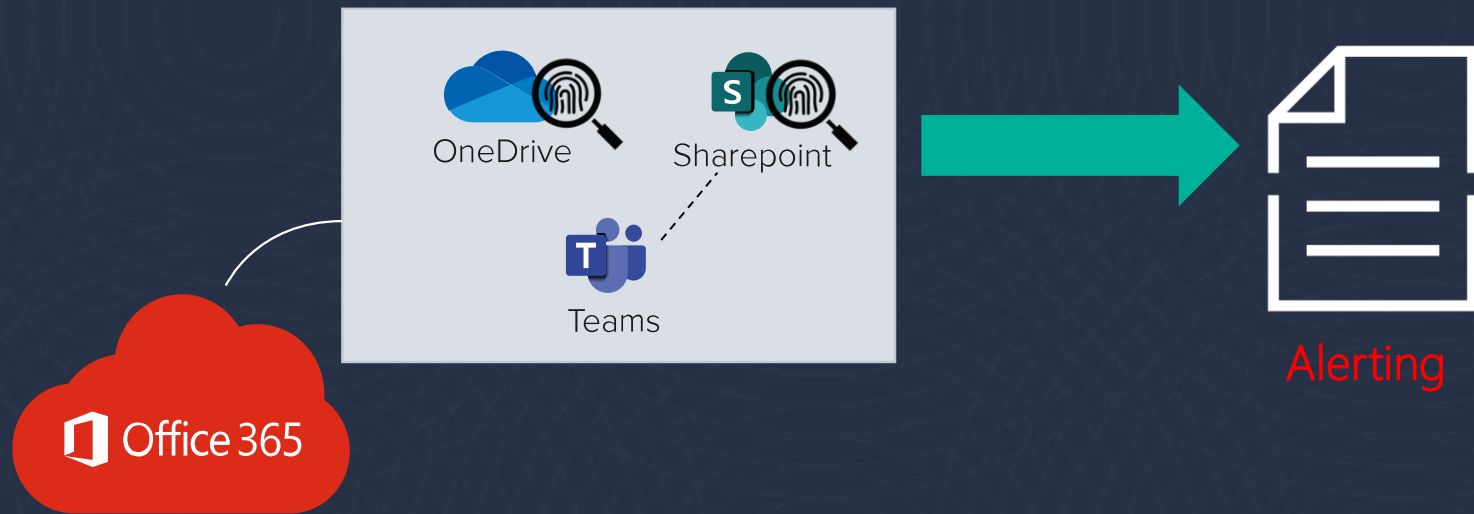
Backup Vs Archiving

Office 365 data backup



Data inspector

Office 365 data Inspector



Servizi e Piani

Advanced

- Email Gateway Defence
- Domain Fraud Protection
- Impers./Phish. Protection
- Incident Response



Premium

- Email Gateway Defence
- Domain Fraud Protection
- Data Inspector
- Impers./Phish. Protection
- Incident Response
- Cloud to Cloud Backup



Premium Plus

- Email Gateway Defence
- Domain Fraud Protection
- Data Inspector
- Security Awareness Training
- Impers./Phish. Protection
- Incident Response
- Cloud to Cloud Backup
- Cloud Archiving



Thank You



Email Protection

Capabilities	Advanced	Premium	Premium Plus
★ Flexible deployment	X	X	X
★ AI-powered detection and response	X	X	X
★ Spam, Malware, and Ransomware protection	X	X	X
★ Phishing and BEC protection	X	X	X
★ Account Takeover protection	X	X	X
★ QR-code attack protection	X	X	X
★ Link protection	X	X	X
★ Attachment sandboxing	X	X	X
★ Dynamic warning banners	X	X	X
★ DMARC reporting	X	X	X
★ Automated Incident Response	X	X	X
★ SIEM/SOAR/XDR integrations	X	X	X
★ Email encryption	X	X	X
★ Email continuity	X	X	X
★ Data loss prevention	X	X	X
★ Unlimited Microsoft 365 backup		X	X
★ Point-in-time data recovery		X	X
★ File scanning for PII and malware		X	X
★ Remediation of improper file shares		X	X
★ Cloud archiving			X
★ Security awareness training*			X
★ Attack simulation*			X

