

# Acronis

#CyberFit

## **Proteggi Microsoft 365 con Acronis Cyber Protect Cloud**

Gianluca Gravino – Senior Solution Engineer

# Acronis Cyber Protect Cloud

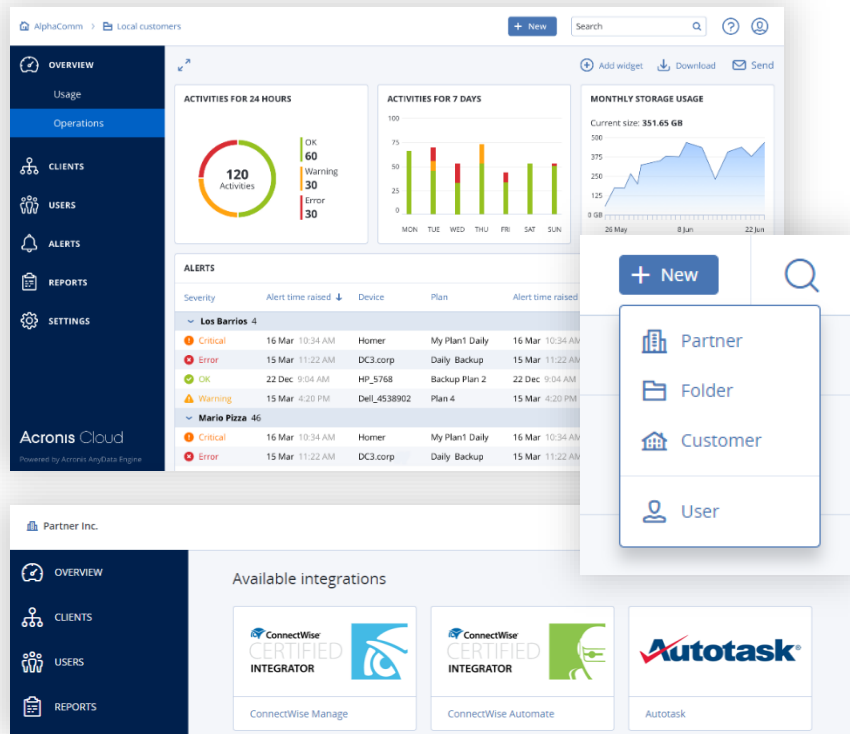


Optimize for every workload

Easy to upsell

Vendor consolidation

# Built for Service Providers



Easy, scalable management of customers' accounts via an easy-to-use web console



Integration with Autotask, ConnectWise Automate, and ConnectWise Manage



Integration with custom provisioning systems via RESTful management API



Comprehensive white-labelling

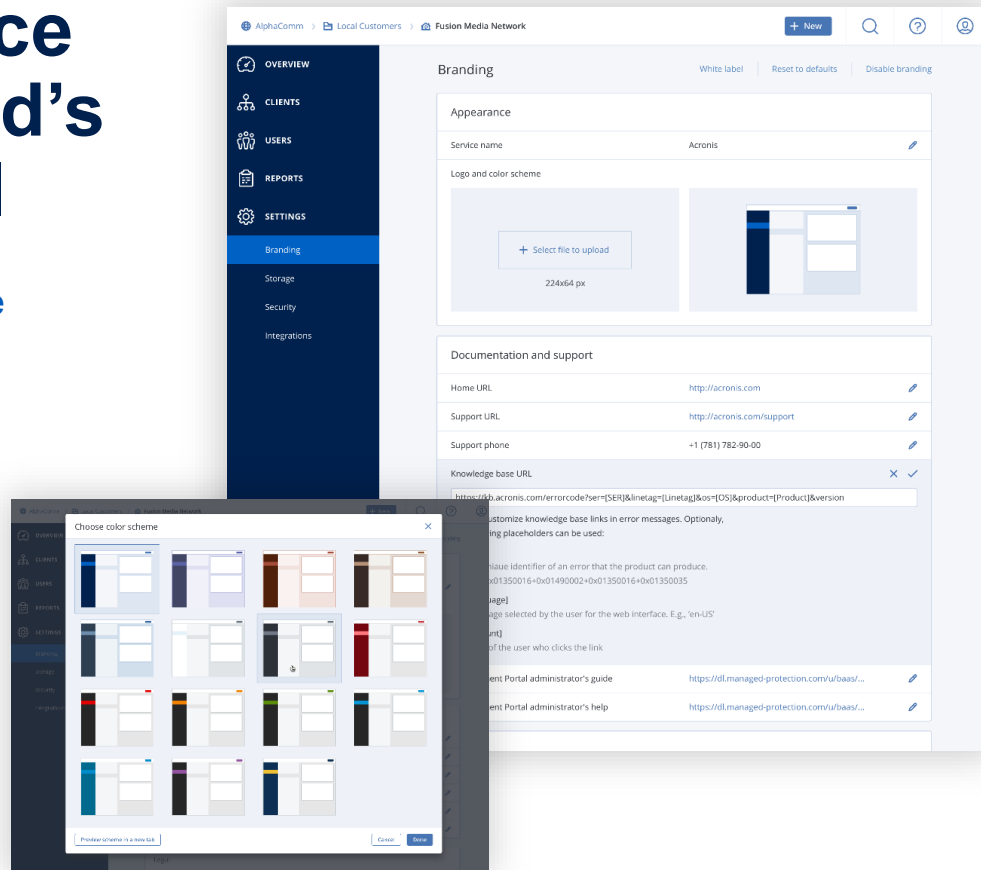


Straightforward pay-as-you-go pricing

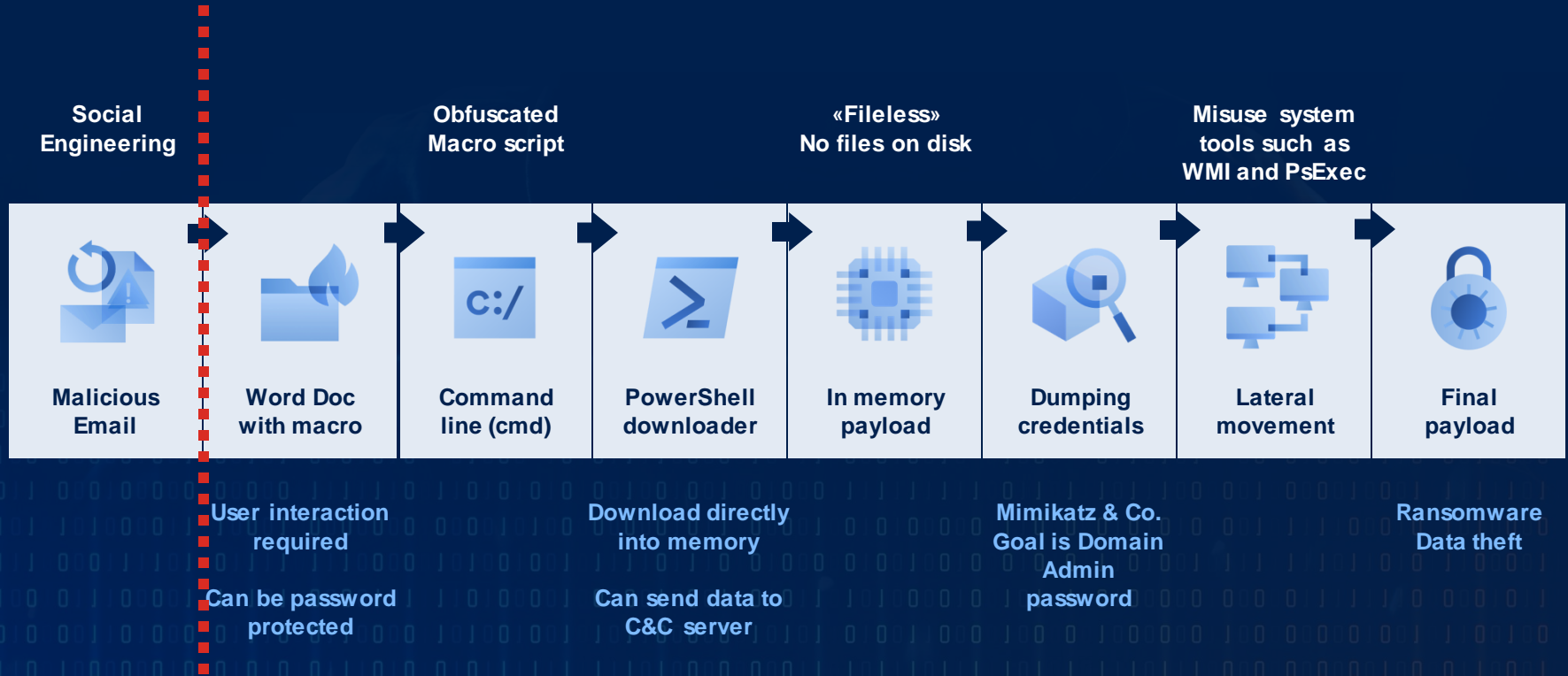
# White-Label the Service to Maintain Your Brand's Unique Look and Feel

Design the management portal's user interface and your backup and disaster recovery services as desired. You can remove any association with Acronis or higher-level partners. Nearly 20 branding items offer key flexibility, such as:

- Web-console color scheme
- Logos
- Company and service names
- Customizable email settings



# Typical Infection Chain



# Statistics from CPOC

Q4 2021



**3.14 M**

of malicious URLs  
on average per month  
were blocked



**94%**

of malicious content  
was prevented by  
anti-phishing and threat  
intelligence



**1%**

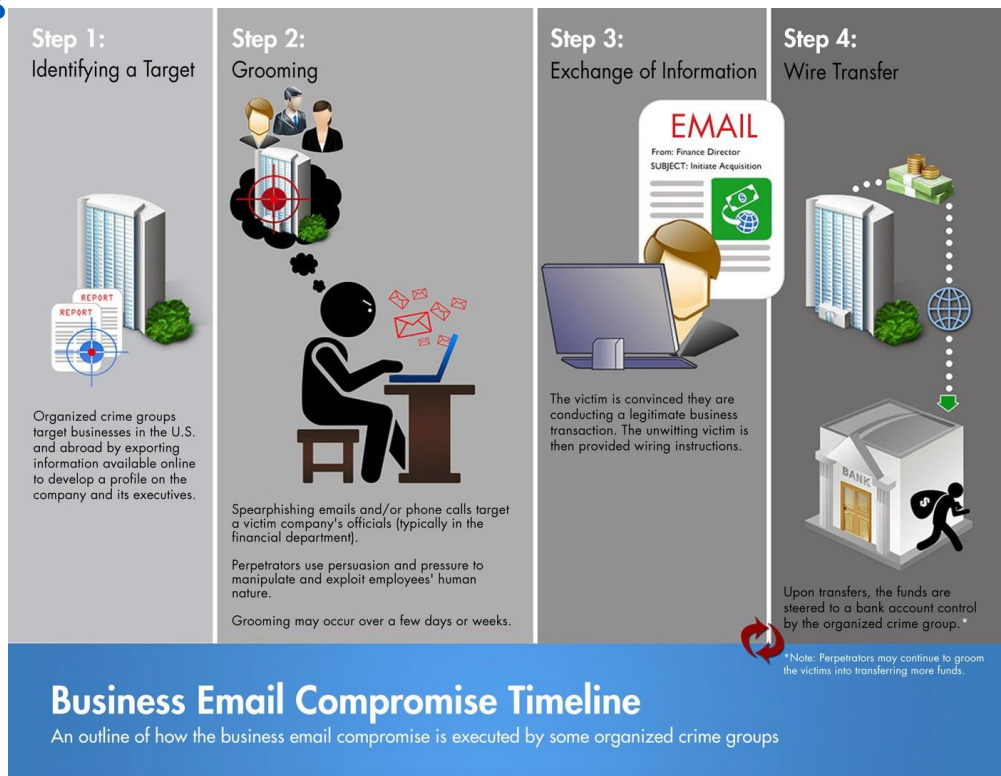
of the blocked  
emails was identified  
as BEC/CEO fraud

# Business Email Compromise

## How Criminals Carry Out BEC Scams

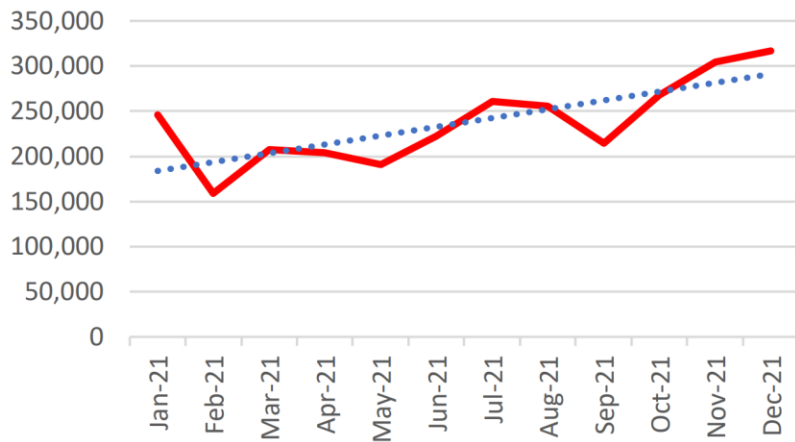
### A scammer might:

- **Spoof an email account or website.** Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic
- **Send spearphishing emails.** These messages look like they're from a trusted sender to trick victims into revealing confidential information.
- **Use malware.** Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices.



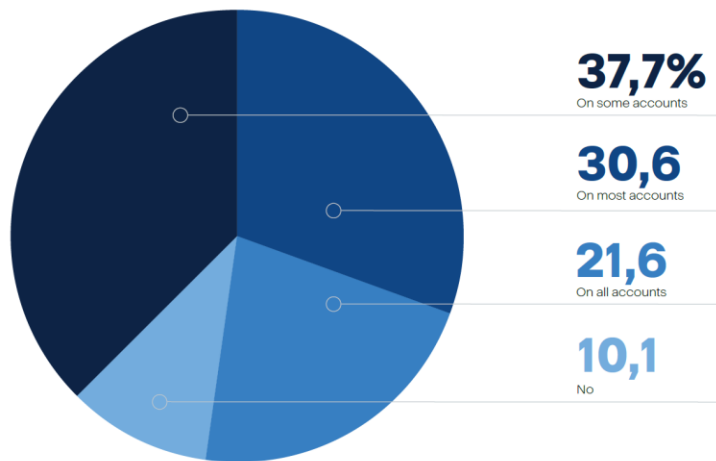
# Phishing Still Works

## Phishing Attacks in 2021



Source: APWG Phishing Trend Reports 2021

## 47% of IT managers don't commonly use MFA



Source: Acronis Cyber Readiness Report 2021



# Evolution of Email Threats

## Massmailing Worms

- I LOVE YOU.VBS (2000)
- MY DOOM (2004) – fastest Email worm
- NETSKY & Sasser Co. (2004)

## Techniques

- Social engineering & bad spelling
- Domain spoofing & font tricks
- Send to all in address book with scripts
- Hoax, chain letters, ads, adult content
- Beginning of spear phishing



LOVE-LETTER-FOR-Y  
OU.TXT.vbs



AnnaKournik...  
(2KB)

2000 - 2005

## Phishing & Malicious Attachments

- EMOTET (2014)
- QBOT → Infostealer & Ransomware
- Romance scam & fake extortion scams

## Techniques

- Office documents + macros
- Reply to existing emails
- Personalized spam from data breaches
- Password protected archives
- Bait'n'Switch links & CAPTCHAs



File Home Insert Design Layout Re



PROTECTED VIEW Be careful Enable Editing

2005 - 2015

## Targeted Context

- TRICKBOT (2016)
- AGENT TESLA
- Business Email Compromise (BEC)

## Techniques


- Account takeover & insider attacks
- ML optimized phishing lure improvement
- Misuse of trusted Cloud and SaaS
- Individual malware per campaign
- 2FA & OAuth phishing

New message


Please transfer 100K now!  
Your CFO


Today


# Phishing Emails



A secured document has been shared with you through  
Microsoft OneDrive.

**Financial Reports & Cash Flow Sta...**


 This link only works for the direct recipients of this message.  
Sign in Microsoft OneDrive for bussiness to get access.

 Microsoft  
Privacy statement

Sign in to your account

← → ↺ ⚠ Dangerous | asetricom.com/well-known/Onedrive/offc.php

☆ Incognito



laczyC

Connecte

Connect

Verbinden


Yixidat

powezas

つなぐ

لواصل

Ligue


 Office 365

Work or school account

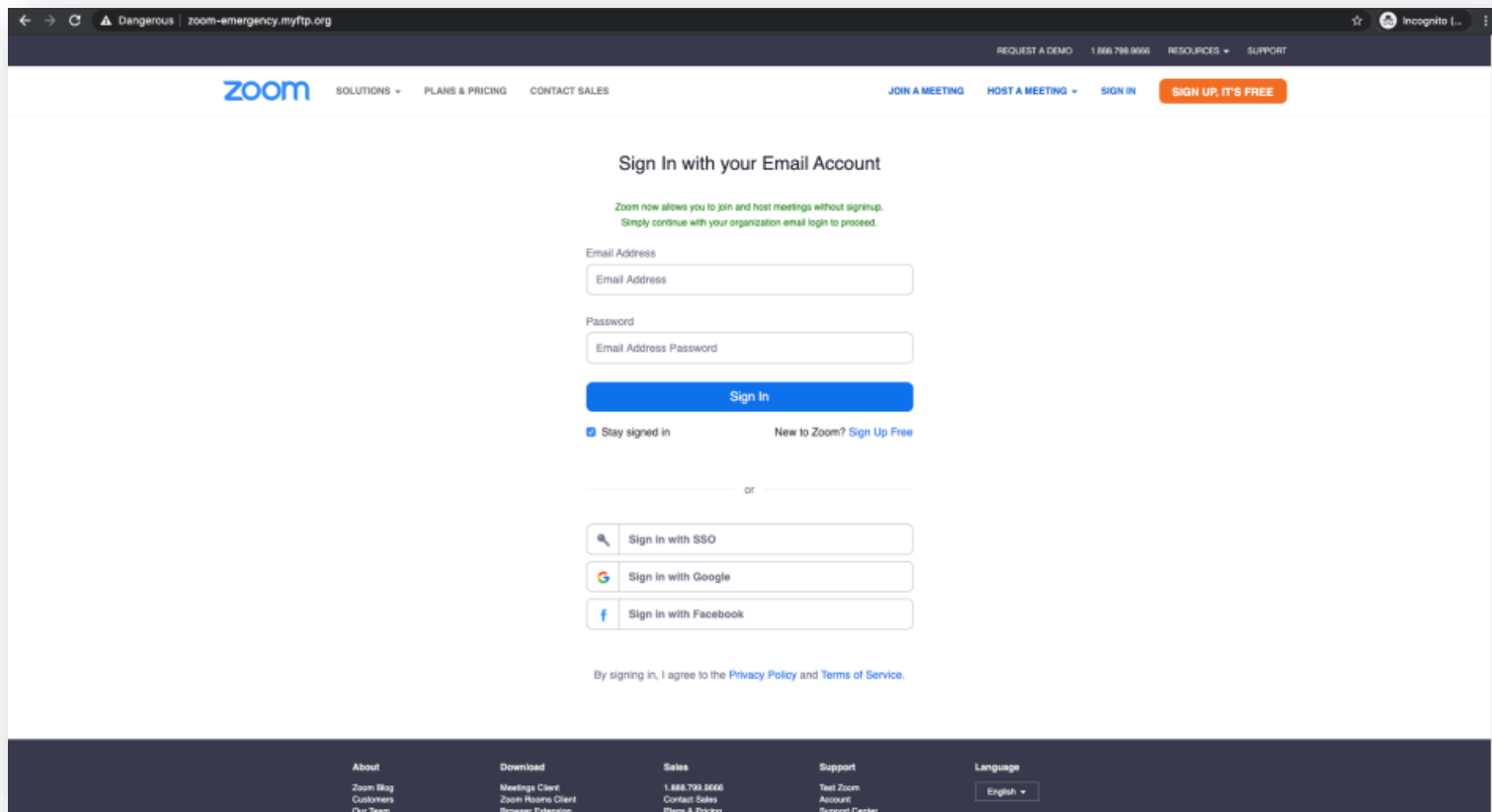
☐ Keep me signed in

[Can't access your account?](#)

© 2018 Microsoft  
[Terms of use](#) [Privacy & Cookies](#)

 Microsoft

# Zoom phishing site



The image shows a screenshot of a phishing website designed to look like the Zoom login page. The browser's address bar shows the URL 'zoom-emergency.myftp.org' with a 'Dangerous' warning. The page features a dark blue header with the Zoom logo and navigation links. The main content area is white and contains a 'Sign In with your Email Account' form. The form includes fields for 'Email Address' and 'Password', a 'Sign In' button, and a checkbox for 'Stay signed in'. Below the form are links for 'Sign in with SSO', 'Sign in with Google', and 'Sign in with Facebook'. At the bottom, there is a footer with links for 'About', 'Download', 'Sales', 'Support', and 'Language'.

← → ↻ ⚠ Dangerous | zoom-emergency.myftp.org

REQUEST A DEMO 1.888.799.9666 RESOURCES + SUPPORT

zoom SOLUTIONS + PLANS & PRICING CONTACT SALES JOIN A MEETING HOST A MEETING + SIGN IN SIGN UP, IT'S FREE

### Sign In with your Email Account

Zoom now allows you to join and host meetings without signing up.  
Simply continue with your organization email login to proceed.


Email Address


Password


Sign In

☒ Stay signed in New to Zoom? [Sign Up Free](#)

or

 Sign in with SSO

 Sign in with Google

 Sign in with Facebook

By signing in, I agree to the [Privacy Policy](#) and [Terms of Service](#).

About  
Zoom Blog  
Customers  
Our Team

Download  
Meetings Client  
Zoom Rooms Client  
Browser Extension

Sales  
1.888.799.9666  
Contact Sales  
Plans & Pricing

Support  
Test Zoom  
Account  
Support Center

Language  
English

# Acronis Cyber Protect Cloud

Microsoft  
Partner

Gold Application Integration  
Gold Data Analytics  
Gold Application Development  
Silver Datacenter  
Gold Windows and Devices

Protect clients' Microsoft 365 applications and data with comprehensive cyber protection that unifies data protection, cybersecurity, and endpoint protection management in one



## Data protection

Ensure your clients' Microsoft 365 data is backed up and recoverable with best-in-class, cloud-to-cloud backup and disaster recovery technologies.



## Email security

Intercept and stop all email threats, including zero-day malware and advanced persistent threats (APTs), before they reach clients' Microsoft 365 mailboxes



## Patch management

Monitor all Microsoft products for vulnerabilities and promptly close security gaps with automated patch management prioritized by vulnerability criticality.



## Exploit prevention for Microsoft Teams

Protect remote workers and prevent any exploitation attempts against the collaboration apps they use, such as Microsoft Teams.

# Protect your Microsoft 365

with Advanced Email Security

# Acronis Cyber Protect Cloud with Advanced Email Security

Improve client security by detecting any email-borne threat before it reaches end-users



## Stop phishing and spoofing attempts

Minimize client risk with powerful threat intelligence, signature-based detection, URL reputation checks, unique image-recognition algorithms, and machine learning with DMARC, DKIM, and SPF record checks.



## Catch advanced evasion techniques

Detect hidden malicious content by recursively unpacking embedded files and URLs and separately analyzing them with dynamic and static detection engines.



## Prevent APTs and zero-day attacks

Prevent advanced email threats that evade conventional defenses with Perception Point's unique CPU-level technology, which acts earlier in the attack chain to block exploits before the malware is released, delivering a clear verdict within seconds.

**\*Product UI supports English only**

# What makes Advanced Email Security unique?

Leverage a single, multi-layered email security solution for lightning-fast detection that's easy to deploy and manage



## Scan 100% of traffic in real-time

Ensure every bit of content (emails, files, and URLs) is analyzed at any scale and a clear verdict is delivered in seconds before the content reaches end users.



## Prevent APTs and zero-day attacks

Block sophisticated threats that evade conventional defenses with a unique CPU-level analysis that acts earlier in the attack chain than other technologies to block threats at the exploit stage, prior to malware release.



## Effortless rapid deployment

Within minutes, the cloud-native deployment integrates the solution directly in the email system without requiring additional configurations, reducing the administrative burden associated with standard secure email gateway (SEG) solutions.



## Incident response services

Empower your service delivery team with direct access to cyber analysts and email security experts that monitor all customer traffic, analyze malicious intent, and provide ongoing reporting and support, including handling FPs, remediating and releasing as required.

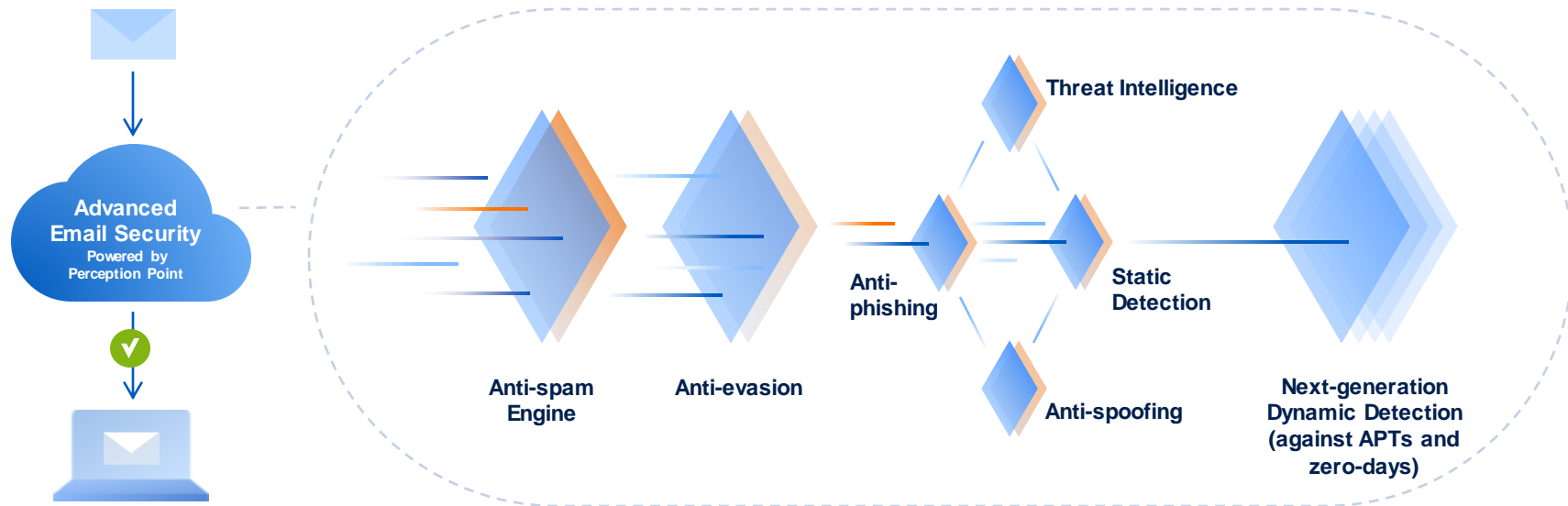


## Unmatched detection speed

Leverage an unmatched detection speed that enables you to prevent all threats before they reach all end-users – which is better than the reactive approach of standard email security technologies.

# Multi-layered protection

7 layers of protection against any email-borne threat



**Why?** Block any email-borne threat before it reaches end-users

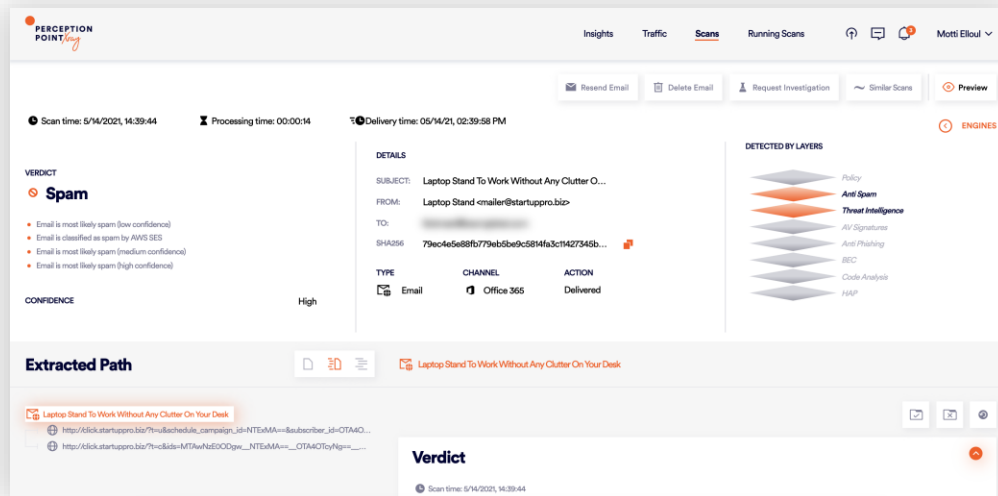


# Anti-spam engine

Stop the unwanted spam emails once and for all

Receives the email and applies anti-spam and reputation-based filters, including IP reputation checks, to block malicious or unwanted communication

- Block malicious attempts
- Quickly flag emails
- Clear the clutter in emails due to spam



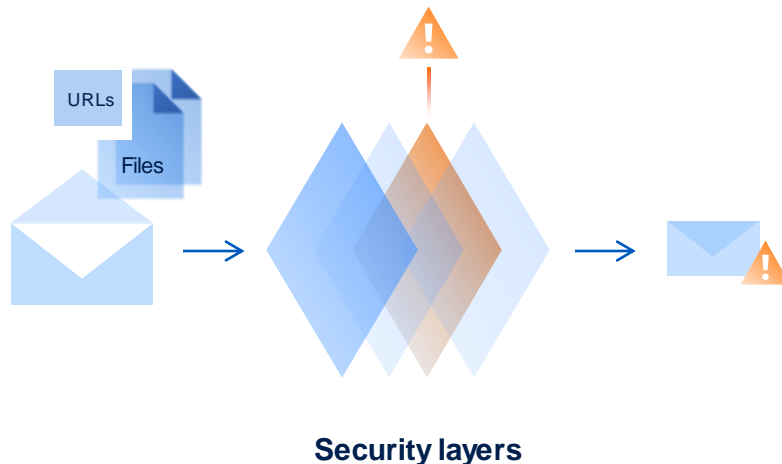
**Why?** Reduce risks for clients by preventing unwanted spam

# Anti-evasion

Detect malicious content hidden within clean one

**Separates embedded files and URLs into their individual components to identify hidden malicious content**

- Recursively extracts embedded URLs and files – unpacking files and following URLs at any nesting level.
- All of the extracted components go separately through the next security layers.
- Unique algorithms run the same files and URLs in multiple versions and patterns to make sure the attack is not leveraging unseen evasion mechanisms



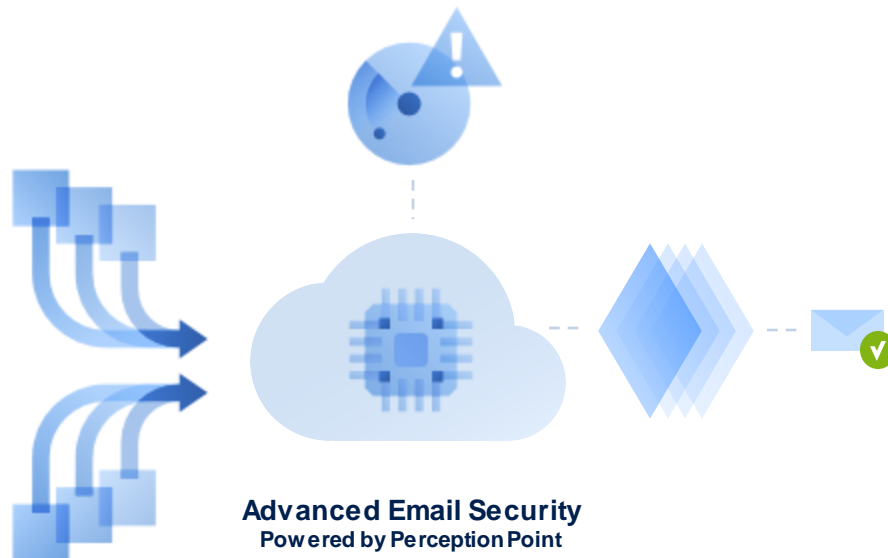
**Why?** Prevent advanced evasion techniques with lightning-fast speed

# Threat intelligence

## Stay ahead of emerging threats

Leverage powerful threat intelligence to stop potential or current attacks

- Threat intelligence from multiple market-leading sources
- Combined with Perception Point's custom engine that collects information on URLs and files from protected customers and from the wild
- Increase reactivity to threats
- Don't miss any threat that appears in the wild – leverage the combined knowledge of external security vendors and the cyber community



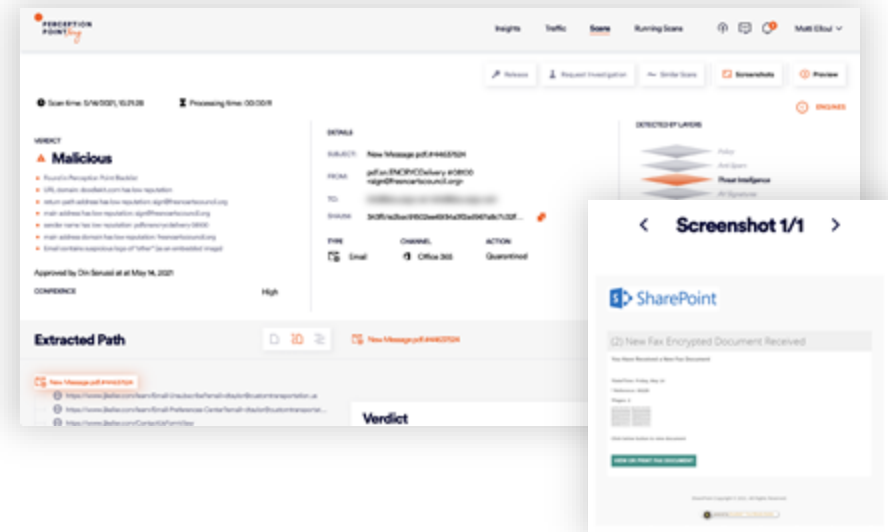
**Why?** Prevent emerging threats from infiltrating clients' emails

# Anti-phishing engines

## Keep phishing attacks from tormenting end-users

Catches phishing attacks and impersonation techniques based on content analysis with multiple phishing filters:

- URL reputation engines from market-leading sources
  - Unique image recognition technology catches malicious URLs based on the images and logos used on the web page.
  - Lexical analysis of the URL
  - Reputation vector of various parameters of the sender and the recipient
- 
- Block known and unknown malicious URLs



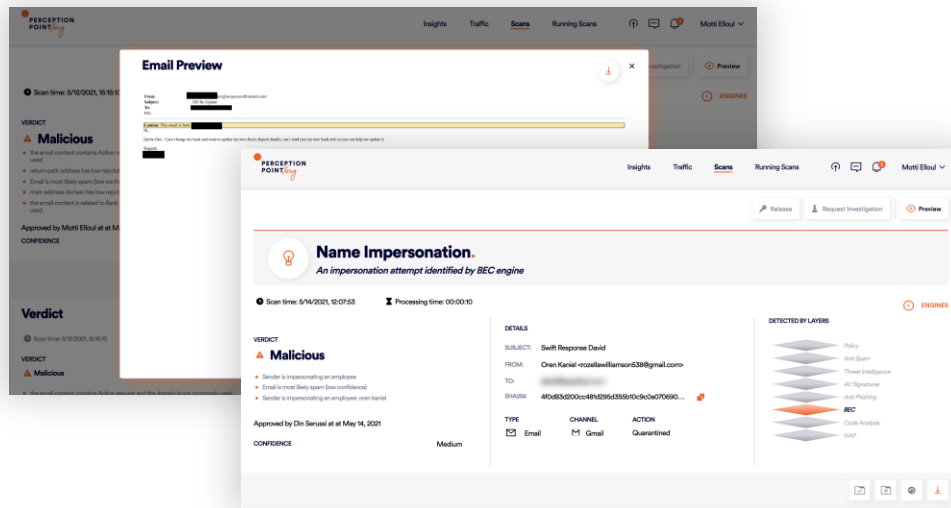
**Why?** Prevent any type of phishing attack before it reaches end-users

# Anti-spoofing

Prevent business email compromise (BEC), including look-alike domain, and display-name deception

Machine Learning-based technology inspects all relevant data and metadata to identify any deviation from standard operations and to detect suspicious content well ahead it reaches the end-user

- IP reputation, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-Based Message Authentication Reporting and Conformance) record checks
- Machine learning, text and metadata analysis, scoring of senders, and other algorithms
- Catch any impersonation attempt



**Why?** Keep clients protected against social engineering based on payload-less attacks.

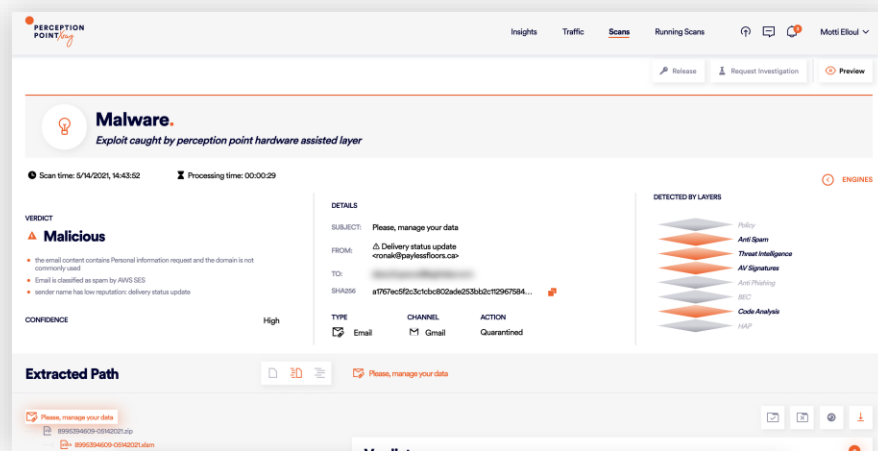
# Antivirus for emails (signature-based detection)

Stop any known email-borne malware in seconds

Strengthen your local anti-malware solution with another layer of protection that's specifically developed for preventing email-borne threats.

Applies best-in-class signature-based detection to emails and files to identify malicious attacks based on a traditional approach to detection in combination with modern technologies.

- Combines multiple signature-based, antivirus engines
- Perception Point's custom technology identifies highly complicated signatures and applies additional static analysis methods



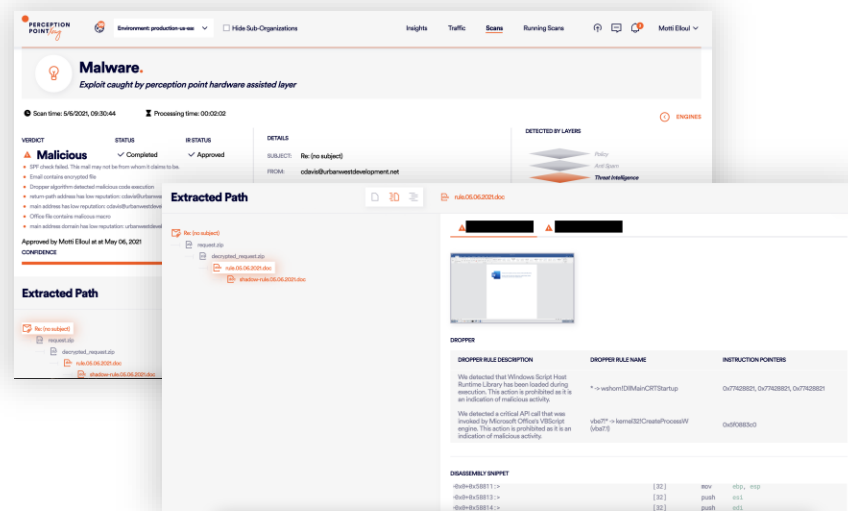
**Why?** Minimize the risks for clients being infected by malware through email

# Next-generation dynamic detection for APTs and zero-days

## Prevent advanced attacks that evade conventional defenses

Unique CPU-level technology acts earlier in the kill chain than any other solution. It blocks attacks at the exploit phase by analyzing the applications' execution flow during runtime to identify deviations from standard flow based on the assembly code.

- True APT prevention – analysis at the exploit stage (pre-malware release)
- Clear verdict within 10 seconds on average – much quicker than sandboxing solutions
- No compromising on content functionality – unlike CDR (content disarm and reconstruction) solutions



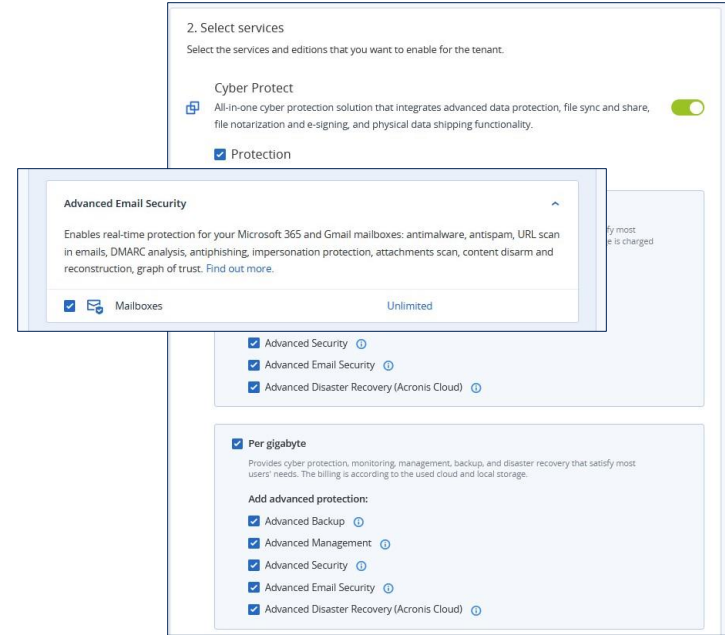
**Why?** Prevent advanced attacks such as APTs and zero-days that conventional defenses miss

# Advanced Email Security Licensing



# Advanced Email Security: Licensing and SKU

- Advanced Email Security is powered by Perception Point's next-generation technology
- Advanced Email Security is applicable to both per-GB and per-workload licensing models
- The pack can be added either to the free core cyber protection functionality or used along with the pay-as-you-go features
- Advanced Email Security is priced per unique user (shared and group mailboxes are not charged separately) as it's independent of the storage used



# Prevent Data Loss

with Advanced Backup

# Acronis Cyber Protect Cloud

Microsoft  
Partner

Gold Application Integration  
Gold Data Analytics  
Gold Application Development  
Silver Datacenter  
Gold Windows and Devices

Protect clients' Microsoft 365 applications and data with comprehensive cyber protection that unifies data protection, cybersecurity, and endpoint protection management in one



## Data protection

Ensure your clients' Microsoft 365 data is backed up and recoverable with best-in-class, cloud-to-cloud backup and disaster recovery technologies.



## Email security

Intercept and stop all email threats, including zero-day malware and advanced persistent threats (APTs), before they reach clients' Microsoft 365 mailboxes



## Patch management

Monitor all Microsoft products for vulnerabilities and promptly close security gaps with automated patch management prioritized by vulnerability criticality.



## Exploit prevention for Microsoft Teams

Protect remote workers and prevent any exploitation attempts against the collaboration apps they use, such as Microsoft Teams.

# Keep clients worry-free with an easy, efficient, and secure Microsoft 365 backup



## Convenient agentless backup

Gain simplified configuration and maintenance of the solution with no need to install an agent on the client's local premises. The agent runs in the secure Acronis Cloud.



## Granular restore in seconds

Recover client systems in seconds to avoid downtime and ensure their business continuity. Granularly back up and restore required data such as emails, files, websites, contacts, attachments, and more.

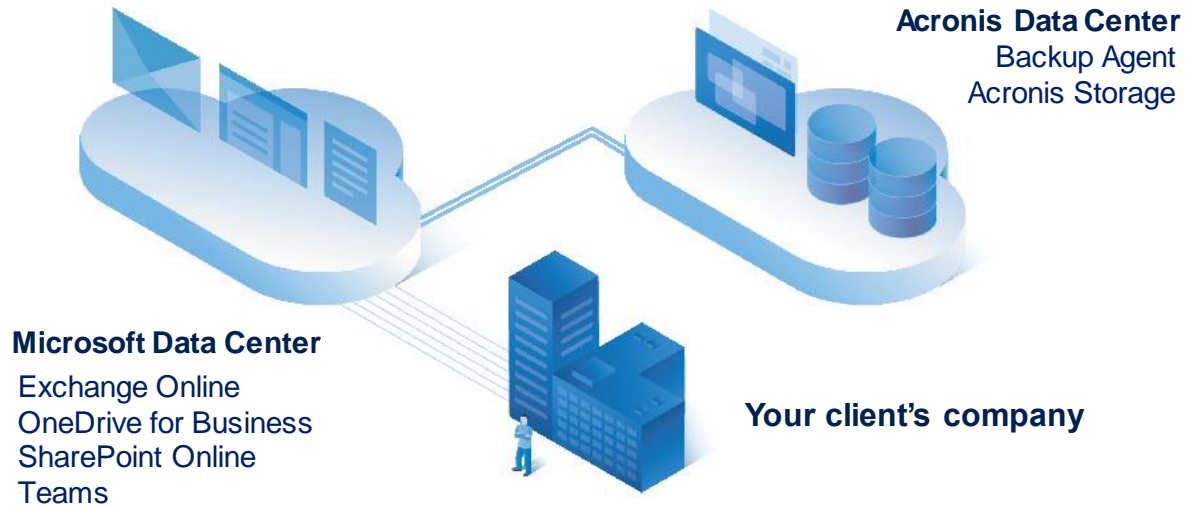


## Quick backup search

Ensure access to your clients' backed up data. Search for specific Microsoft 365 items and use them immediately, before recovering. Download the critical file or attachment, or send the email right from the backup.

# Effortless cloud-to-cloud backup

Start quickly with no upfront costs and save on training and maintenance.  
With Acronis Cyber Protect Cloud, you can directly back up client data from Microsoft data centers to our highly secure Acronis data centers.



# Complete Microsoft 365 protection



**Backup for  
Microsoft  
Exchange Online**



**Backup for  
Microsoft OneDrive  
for Business**



**Backup  
for Microsoft  
SharePoint Online**



**Backup for  
Microsoft Teams**  
Including call protection

- ✓ Back up from Microsoft data centers directly to cloud storage
- ✓ Automatically protect new Microsoft 365 users, groups, and sites
- ✓ Search through Microsoft 365 backups to quickly access backed-up data

New

**Unlimited Acronis Hosted Cloud Storage for Microsoft 365 data  
at no additional cost for per-seat licensing**



# Microsoft Exchange Online backup

Emails, attachments, contacts, tasks, events, group mailboxes, archived mailboxes, and calendars

## Flexible recovery

- Granular point-in-time recovery
- Search for emails in backups
- Cross-user and cross-organization recovery
- Restore to custom folders via live browsing of mailbox content
- Preview email content
- Download email attachments
- Send email from backup

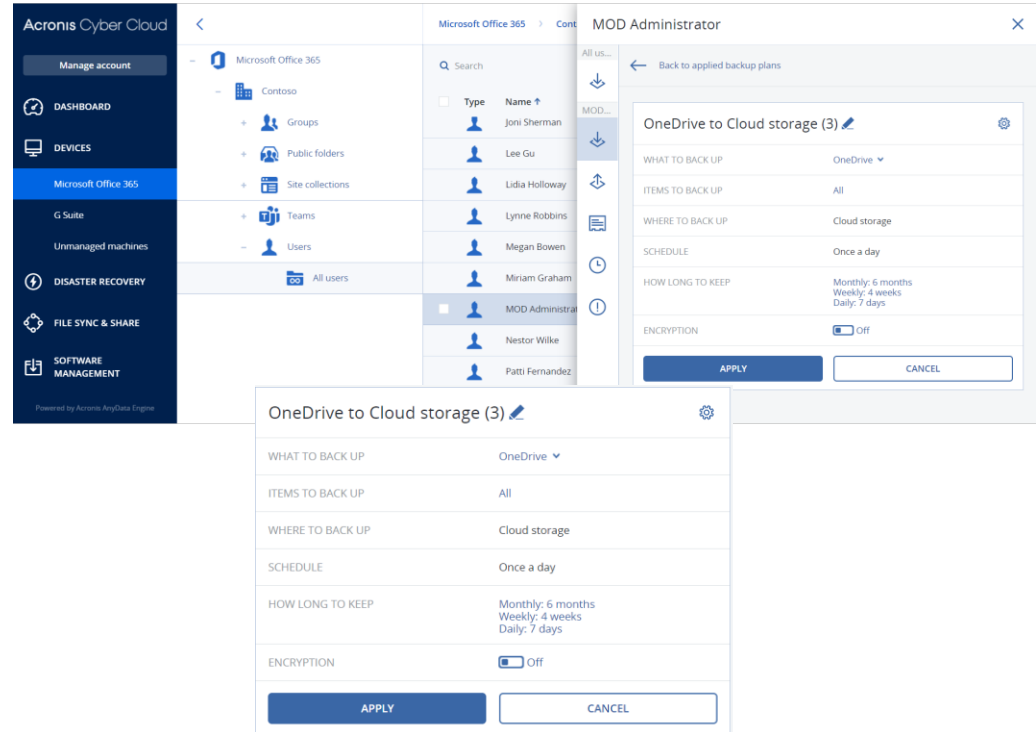
The screenshot displays the Acronis Cyber Cloud interface for configuring a Microsoft Office 365 backup. The left sidebar shows navigation options: Manage account, DASHBOARD, DEVICES, Microsoft Office 365 (selected), G Suite, Unmanaged machines, DISASTER RECOVERY, FILE SYNC & SHARE, and SOFTWARE MANAGEMENT. The main area shows the 'Microsoft Office 365' section with a list of entities: Contoso, Groups, Public folders, Site collections, Teams, and Users. A table lists users: Joni Sherman, Lee Gu, Lidia Holloway, Lynne Robbins, Megan Bowen, Miriam Graham, MOD Administrator, Nestor Wilke, and Patti Esmundson. A modal window titled 'Office 365 mailboxes to Cloud storage (3)' is open, showing backup settings: WHAT TO BACK UP (Office 365 mailboxes), WHERE TO BACK UP (Cloud storage), SCHEDULE (Once a day), HOW LONG TO KEEP (Monthly: 6 months, Weekly: 4 weeks, Daily: 7 days), ARCHIVE MAILBOX (On), and ENCRYPTION (Off). Buttons for APPLY and CANCEL are at the bottom.

# Microsoft OneDrive for Business backup

Files, folders, file filters, and support (e.g. “back up \*.docx”)

## Flexible recovery

- Granular point-in-time recovery
- Search files through backup
- Cross-user and cross-organization recovery
- Restore to custom folders via live browsing of OneDrive content
- Download a file from backup
- Sharing permissions recovery



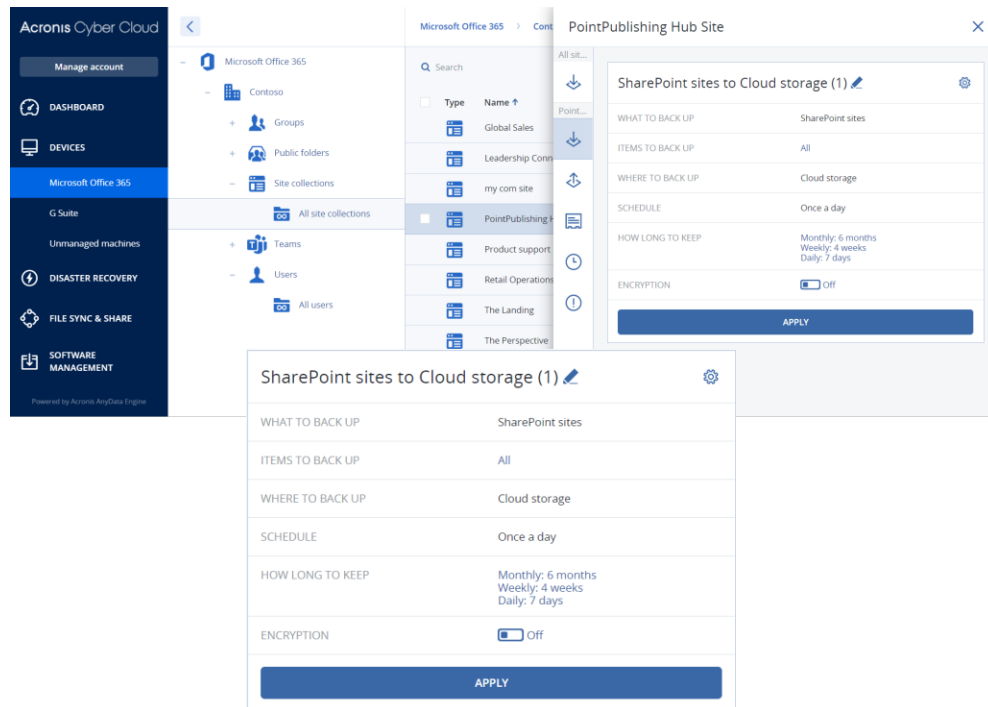


# Microsoft SharePoint Online backup

Site collections, team sites, and communication sites

## Flexible recovery

- Granular point-in-time recovery for entire sites, document libraries, single documents, etc.
- Search for items in backups
- Cross-organization recovery: recovery to another Microsoft 365 organization
- Download a file from backup
- Sharing permissions recovery

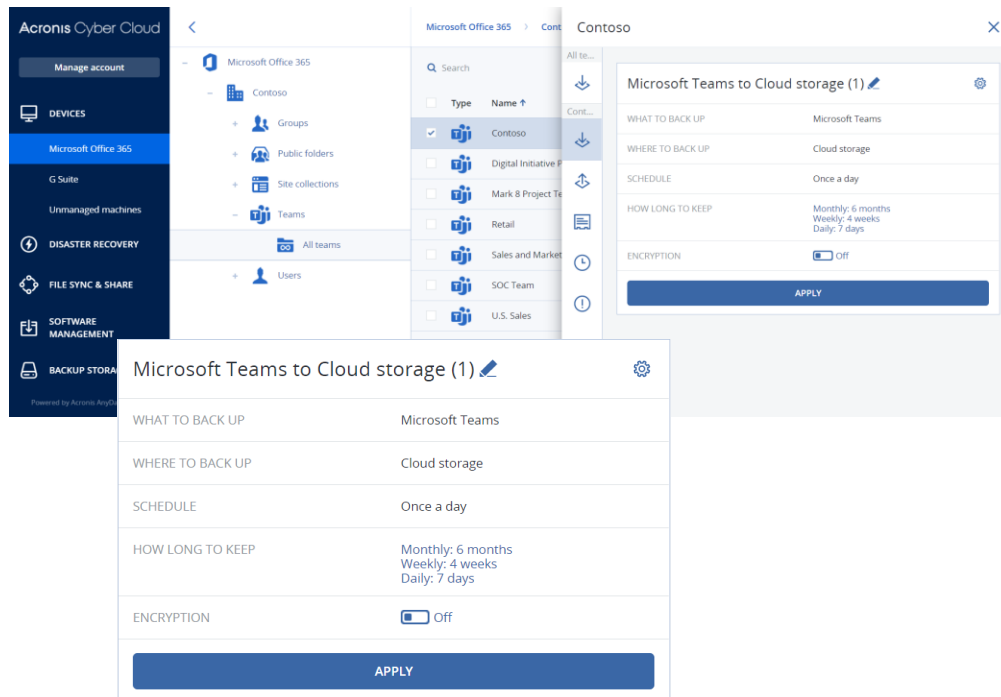


# Microsoft Teams backup

Entire team, channels, files, mailbox, email folders and messages, meetings, and team sites

## Flexible recovery

- Granular point-in-time recovery for entire teams, channels, mailboxes, etc.
- File-name search and full-text search for text in the chat messages
- Download a file from backup
- Download file conversations and attachments



# Key features to protect your clients' Microsoft 365 data

## Automatic protection for new Microsoft 365 items

Reduce headaches by streamlining backup management for Microsoft 365. New users, groups, and sites are automatically protected.

## Quick backup search

Find any file your client needs in seconds. Enhanced search for mailboxes allows you to search by email subject, recipient, sender, and date.

## Simplified administration

Administer the solution and perform backup tasks using an easy-to-use management portal. Reduce costs and time spent learning the solution and implementing it.

## Multi-level encryption

Safeguard your clients' data with additional security. At-source, enterprise-grade AES-256 encryption protects backups with irreversibly encrypted passwords.

## Powerful status monitoring

Achieve higher levels of transparency and security through advanced reporting capabilities and backup status monitoring, including widgets, notifications, and alerts for critical events.

## Multi-factor authentication support

Add additional security with Microsoft's multi-factor authentication (MFA). Authentication is enabled via a trusted device or fingerprint.

# Acronis Cyber Protect Cloud for M365 Licensing

# Acronis Cyber Protect Cloud: Pay-as-you-go features

Ensure further protection of your clients' data, systems and applications with Acronis Cyber Protect Cloud pay-as-you-go features. Choose a licensing model and apply it on a client level. Both per-GB and per-workload are available.

Features		Acronis Cyber Protect Cloud
Backup	Workstations, Servers (Windows, Linux, Mac) backup	PAYG
	Virtual machine backup	PAYG
	File backup	PAYG
	Image backup	PAYG
	Immutable backups	PAYG
	Standard applications backup (Microsoft 365, Google Workspace, Microsoft Exchange, Microsoft SQL)	PAYG
	Network shares backup	PAYG
	Backup to local storage	PAYG
	Backup to cloud storage	PAYG
Disaster Recovery	Test failover in isolated network environment	32 compute points / month*
	Cloud-only VPN Connection	PAYG
	Firewall policies management	PAYG
File Sync and Share	File Sync and Share functionality	PAYG
Notary	Notarization, e-signature, document templates	PAYG

\* Partners get 32 compute points for test failover that can be used to run several virtual machines of the same or different type. Fewer VMs or less powerful VM types will run for longer.

# All-in-one cyber protection and management solution

Cover all of your clients' Microsoft environments with a single solution

