# VM BACKUP
## RELIABLE. POWERFUL. IMMUTABLE.

Colin Wright



HORNETSECURITY

# Why AVMB V9? Ransomware

## Today's Highwayman?

- Ransomware attacks increased 105% in 2021. (TechTarget)

- Ransomware has risen 232% since 2019. (TechTarget)

- There are 20 ransomware attacks attempted every second. (TechTarget)

- Ransomware is now responsible for 10% of global breaches (up from 2% in 2016). (Verizon)

- 78% of organisations experienced email-based ransomware attacks in 2021. (Proofpoint)

- 68% of organisations were infected by ransomware in 2021, up from 66% in 2020. Nearly two-thirds of those organisations were hit by three separate ransomware infections, while nearly 15% of those experienced more than 10 separate ransomware infections. (Proofpoint)

- Operating systems targeted most targeted by ransomware: Windows (85%), MacOS (7%), Android (5%), iOS (3%). (SafetyDetectives)

- Most common methods of ransomware infection: phishing emails (67%), lack of cyber awareness training (36%), weak passwords/access management (30%), poor user practices (25%), malicious websites or ads (16%), other (16%). Some were targeted by multiple methods. (SafetyDetectives)

- Since 2020, more than 130 different strains of ransomware have been detected. (VirusTotal)

- Average Ransomware cost 2022 $4.54M! (IBM Jan 2023)

https://www.blackfog.com/the-true-cost-of-ransomware-attacks/

HORNETSECURITY

# THREAT SITUATION: RANSOMWARE ON THE RISE

Nearly **6 in 10** ransomware attacks originated from malicious email or phishing attacks

**15%** of ransomware attacks targeted specifically backup storage

Costs for downtime and data loss can amount to **millions of €**

HORNETSECURITY

HORNETSECURITY

# Ransomware

**HORNETSECURITY**



What we think a hacker looks like?



The new reality of Threat Actors/Hackers!

# BACKUP IS THE LAST LINE OF DEFENCE

## From

- ❯ Users
- ❯ The Outside world
- ❯ Ransomware
- ❯ Data loss
- ❯ System issues
- ❯ Mishaps
- ❯ Etc. Etc. Etc

# NEW: VM BACKUP V9

**HORNETSECURITY**

**VM Backup V9 leverages Immutable Cloud Storage** which assures data cannot be erased, modified, or deleted by anyone for a set duration

- Tamper-proof backup data whilst under the defined immutable policy

- Peace of mind from ransomware attacks

- Extra layer of security above the existing offsite storage functionality

- No need for retaining unnecessary data and incurring high costs as retention operates seamlessly on the cloud repository

IMMUTABLE CLOUD STORAGE WITH
**VM BACKUP V9**

Amazon S3
Wasabi
Azure (coming soon)
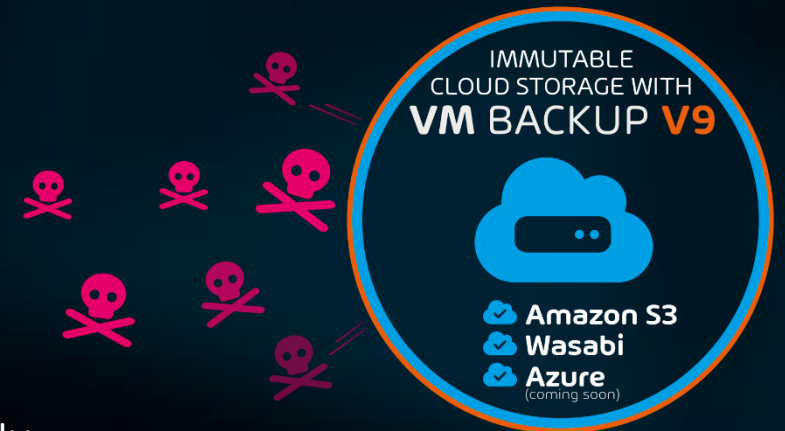
# KEY FEATURES OF VM BACKUP V9

## IMMUTABILITY OF BACKUPS

- Protection against ransomware attacks and rogue admins
- Available for Wasabi and Amazon S3
- Maintain use of augmented in-line deduplication for cost savings

**HORNETSECURITY**

## SCALABILITY & ROBUSTNESS ENHANCEMENTS

- VM Backup installations can now handle larger infrastractures
- Designed with the growing needs of our customers in mind

# KEY FEATURES OF VM BACKUP V9

## SUPPORT FOR THE LATEST VERSIONS OF HYPER-V and VMWARE

- VMware, vCenter & vSphere 8
- Windows Server 2022, Azure Stack HCI 22H2

## OTHER PERFORMANCE IMPROVEMENTS

- Retention operations now run in parallel with backup operations
- Disk space is utilised more efficiently

# BACKUP FUNCTIONS

- **Hot/Live Backups:** Perform backups at any time needed at the push of a button without requiring any downtime

- **WAN-optimized replication:** Continuous replication of virtual machines to another site

- **Continuous Data Protection (CDP) & Flexible backup scheduling:** fully automatic backup at individual time settings (as frequently as every 5 min)

- **Concurrency:** Simultaneous backup of multiple virtual machines

- **Retention policies:** Define and change retention times for onsite backups and offsite copies

- **Grandfather-Father-Son Archiving (GFS):** Set up dedicated hierarchical backup intervals for years, months, and weeks.

- **Direct Cloud Storage Integration:** Directly integrates with Microsoft Azure, Amazon S3 and Wasabi Cloud Storage

HORNETSECURITY

# RECOVERY FEATURES

**HORNETSECURITY**

- ◉ **Boot from Backup:** Boot directly from the backup location

- ◉ **Instant Business Continuity:** Optimized time to boot of replicated virtual machines

- ◉ **Recovery as clone:** restore of virtual machines of the same or other hypervisors

- ◉ **Exchange item-level restore:** restore individual mailboxes or emails from a backed up Exchange VM

- ◉ **Sandbox Restoring & Backup Verification:** Set up a recovery and test scenario for the backup database

- ◉ **Granular Restore:** File-based recovery of files or folders from backed up Windows VMs
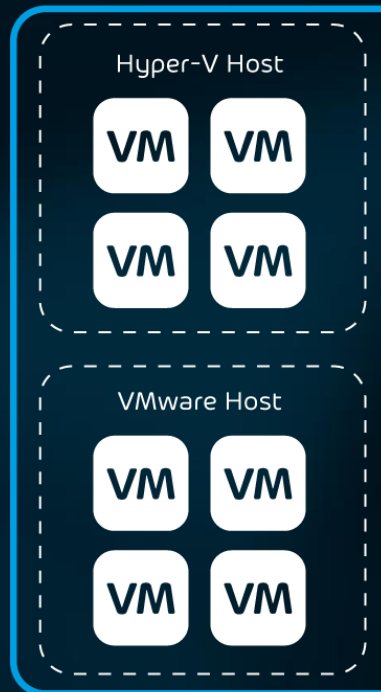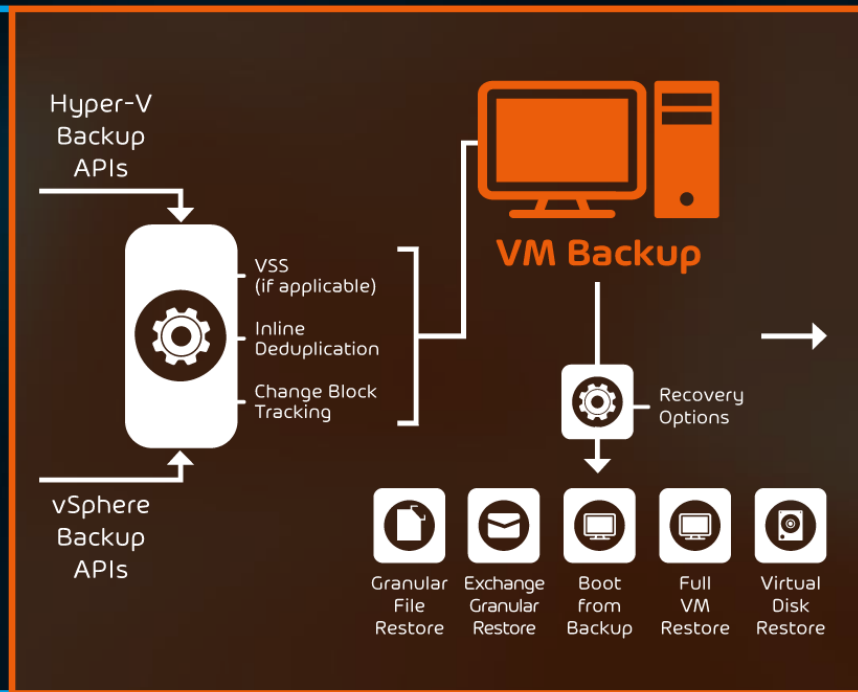
# BACKUP & RECOVERY FOR VMWARE & HYPER-V
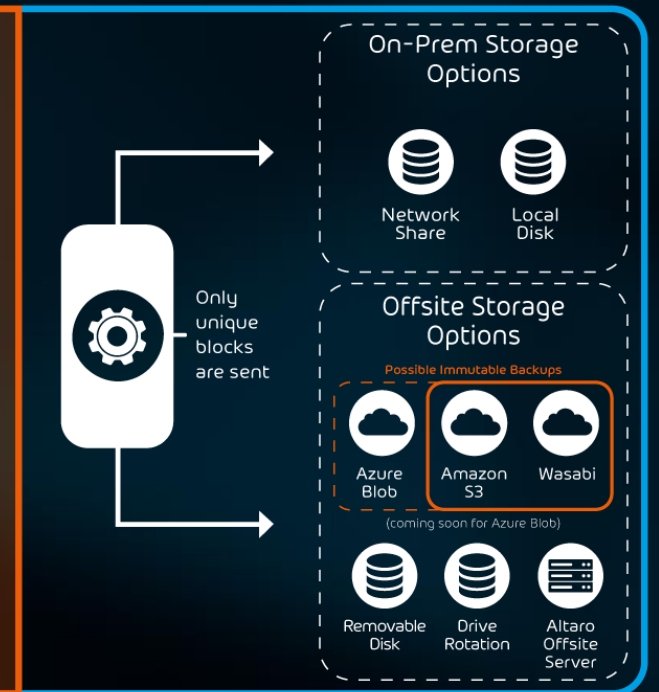
HORNETSECURITY

HORNETSECURITY

### Virtualization Infrastructure

**Hyper-V Host**

VM VM
VM VM

**VMware Host**

VM VM
VM VM

### Backup Process

Hyper-V Backup APIs

VSS (if applicable)

Inline Deduplication

Change Block Tracking

vSphere Backup APIs

**VM Backup**

Recovery Options

Granular File Restore

Exchange Granular Restore

Boot from Backup

Full VM Restore

Virtual Disk Restore

### Storage Options

Only unique blocks are sent

**On-Prem Storage Options**

Network Share

Local Disk

**Offsite Storage Options**

Possible Immutable Backups

Azure Blob

Amazon S3

Wasabi

(coming soon for Azure Blob)

Removable Disk

Drive Rotation

Altaro Offsite Server

# AUGMENTED INLINE DEDUPLICATION

- Dramatically reduced storage requirements for backups
- Much faster backups
- Less data transferred, thus loads of bandwidth saved
- Common data is only transfered to the backup or offsite location ONCE, without the need for Post-Process Deduplication
- Use of variable block size Deduplication for the best efficiency
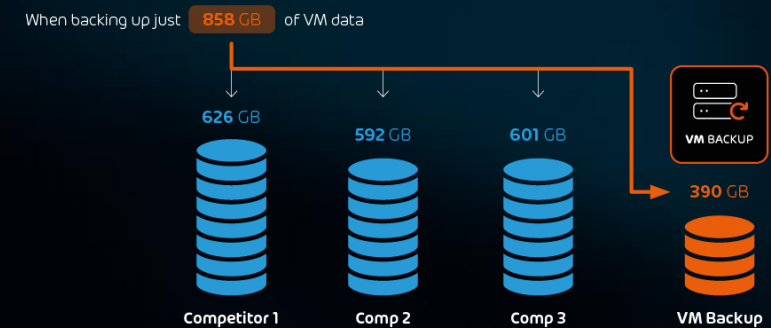- Deduplication is not taxing on server performance

When backing up just **858** GB of VM data

**626** GB     **592** GB     **601** GB

VM BACKUP

**390** GB

Competitor 1    Comp 2    Comp 3    VM Backup

**Figure 1:** When compared to other vendors, the Augmented Inline Deduplication results in smaller backup size saving massive storage space.

*May vary depending on environment and data.

HORNETSECURITY

HORNETSECURITY

# STATS ON DEDUPLICATION

> Sample of 100 customers' data



Data backed up:
**450 TB**

**AVERAGE CUSTOMER**
**SAVES 63%**
in backup storage thanks to our
Augmented Inline Deduplication

Backup storage required:
**120 TB**
OF DATA
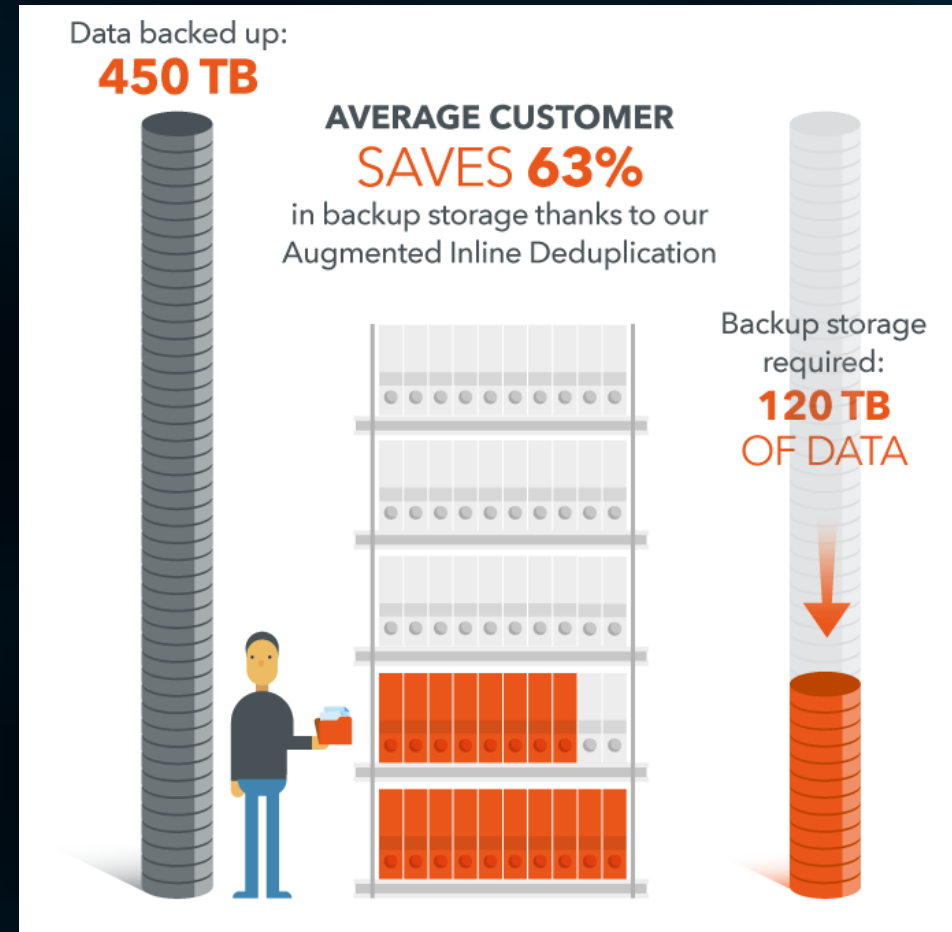
# RESTORING YOUR VMS

- Full VM Restore

  - Restore clone
  - Restore different versions
  - Restore to different host
  - Boot from Backup Drive

- Granular Restore

  - **File level restore** – Instantly browse the contents of the VHD/VMDK files of the VM, choose which files/folders you would like, and restore just these files/folders to a specified location on disk

  - **Exchange item level restore** – Instantly browse the contents of a Microsoft Exchange (2007 or later) database inside the VM you have backed up, and restore individual items from the Microsoft Exchange Database to a PST.

# RESTORING YOUR VMS

Boot from Backup

Instant **Boot from Backup**
Enables users to instantly boot any VM version directly from the backup location, thus drastically <u>reducing RTOs</u> (Recovery Time Objectives)

**Verification mode:** Instantly boot up your backed up VMs for verification

**Recovery Mode:** If disaster strikes, the VM can be booted up instantly from the backup drive with minimal downtime, while the VM is restored back to the Hypervisor in the background.

A simple VM reboot completes the recovery process and preserves any changes done while the VM was booted.

09.05.2023
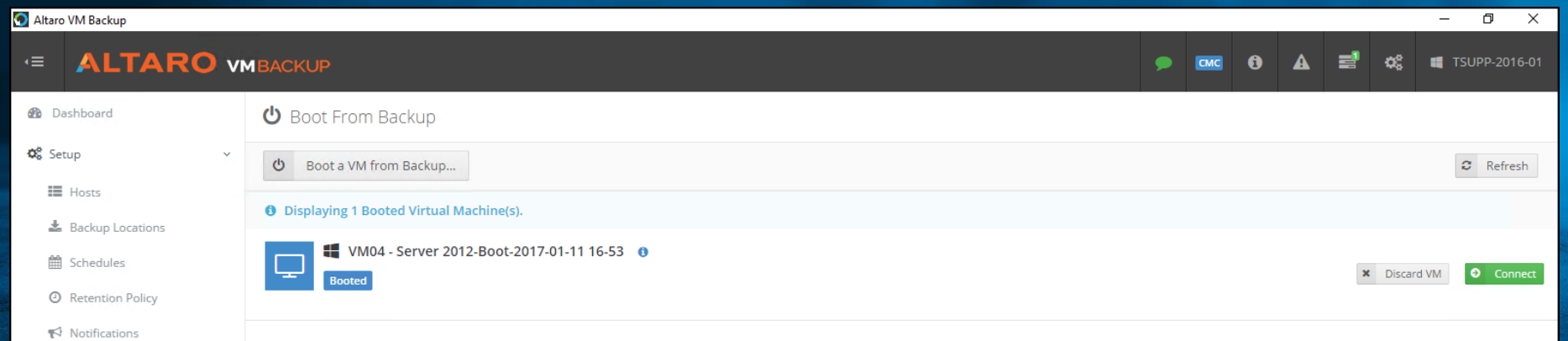
# RESTORING YOUR VMS

- Sandbox Restore & Verification

- Run manual or automated integrity checks of your backup data

  - **Verify Backup Folders** – Verify backup data checksums without requiring additional disk space or attaching the VM to the hypervisor

  - **Full Test Restore** – Fully restore a VM and attach to the hypervisor while in a sandbox environment to ensure that it boots, without affecting the production environment



09.05.2023

# CLOUD MANAGEMENT CONSOLE (CMC)

- Monitor, configure & manage all your Altaro VM Backup installations from a single Cloud console

- Access Portal from anywhere

- Remotely assign Configuration Templates

- Trigger backups/restores from an online portal

- Remote Management

- Multi-tenancy

- Real-time status updates

- Saved Searches & Alerts

- Subscription Licensing for Partners

- Available right now for Partners & MSPs,

# PRODUCT INSIGHTS - IMMUTABILITY

# VM BACKUP KEY POINTS

**Easily back up and replicate** virtual machine hosted on Microsoft Hyper-V and Vmware, as well as physical Microsoft servers

**Ransomware Protection** leveraging Immutable Cloud Storage

**Ease of use** through intuitive interface and minimal maintenance

**Scalable** for any company size

**Optimized performance**: fast, small backups, resource-saving

# EDITIONS & LICENSING

Feature comparison:

| Edition: | Standard | Unlimited | Unlimited Plus |
|---|---|---|---|
| Features | • Basic Backup<br>• Scheduling<br>• Basic Restore<br>• Offsite Backups<br>• Encryption<br>• File Level Restore<br>• Restore to different host<br>• Priority Tech Support | Standard Edition features<br><br>+<br><br>• Augmented Inline Deduplication<br>• Boot from Backup<br>• Support for Clusters & vCenter<br>• Exchange Level Restore | Unlimited Edition features<br><br>+<br><br>• WAN-Optimized Replication<br>• CDP<br>• Back up to Azure, Amazon S3, Wasabi<br>• Immutable Backups on Amazon S3 and Wasabi<br>• Control Panel (CP) |

HORNETSECURITY

# EDITIONS & LICENSING

## Monthly Subscription

- Most flexible option: no upfront cost, pay per use – per backed up VM per month
- One edition: Unlimited Plus
- Support, updates and version upgrades included in monthly fee

## Perpetual & SMA

- Perpetual license: per host (unlimited sockets and VMs)
- Choose your edition: Unlimited Plus, Unlimited or Standard
- SMA necessary to receive support, updates and version upgrades

HORNETSECURITY

# THREATS

## 2022 trends

- Lockdown and home usage drove more attacks

- Growth of 365, WFH and Teams
  - Use of any machine to access data and continue to work

- 82% increase Ransomware attacks

- CEO Fraud

- 170+ new adversaries

- 45% increase in intrusion campaigns

- PaaS
  - Phishing as a Service
  - Dark web
  - Great tech support!!

- Business email compromise

- Social engineering

- Account takeover attacks – Linkedin new starters

HORNETSECURITY


THE PHISHING MAIL OCEAN

# RECENT "HITS"
## RANSOMWARE..WHEN…NOT IF!

- Rackspace - January 2023
- Australia Fire Rescue – January 2023
- Royal Mail UK – January 2023
- Yum Brands, (KFC, Taco Bell) – January 2023
- B&G Foods – February 2023
- Argentina Oil & Gas – February 2023
- Washington State – February 2023
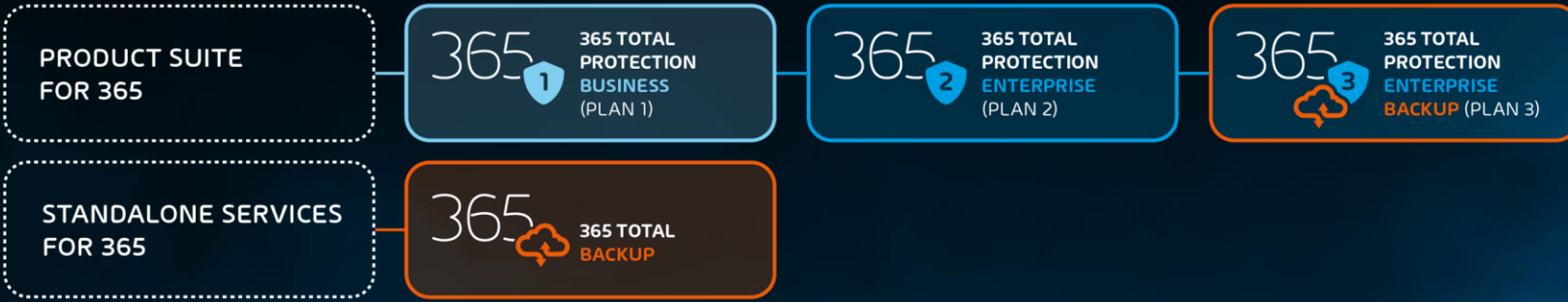
HORNETSECURITY

# WE CAN'T ALWAYS RELY ON HUMANS

**HORNETSECURITY**

| 365 TOTAL PROTECTION BUSINESS | 365 TOTAL PROTECTION ENTERPRISE | 365 TOTAL PROTECTION ENTERPRISE BACKUP |
|---|---|---|
| NEXT-LEVEL MICROSOFT 365 SECURITY | PREMIUM NEXT-LEVEL MICROSOFT 365 SECURITY | COMPLETE EMAIL SECURITY AND BACKUP FOR MICROSOFT 365 |
| SPAM & MALWARE PROTECTION · EMAIL ENCRYPTION · EMAIL SIGNATURES & DISCLAIMERS | SPAM & MALWARE PROTECTION · EMAIL ENCRYPTION · EMAIL SIGNATURES & DISCLAIMERS | SPAM & MALWARE PROTECTION · EMAIL ENCRYPTION · EMAIL SIGNATURES & DISCLAIMERS |
| | + ADVANCED THREAT PROTECTION · EMAIL ARCHIVING · EMAIL CONTINUITY | ADVANCED THREAT PROTECTION · EMAIL ARCHIVING · EMAIL CONTINUITY |
| | | + BACKUP & RECOVERY OF MAILBOXES & TEAMS · BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT · BACKUP & RECOVERY OF ENDPOINTS |

**OPTIONAL ADD-ONS**

⊕ HORNET.EMAIL
HOSTED MAILBOX WITH FULL SECURITY

⊕ 365 TOTAL ENCRYPTION (EXCLUSIVELY FOR 365 TOTAL PROTECTION ENTERPRISE)
FULLY SECURED MAILBOX EMAIL ENCRYPTION

# OUR BRAIN STRUGGLES?

## BECAUSE IT ADAPTS – MAKES IT EASIER TO TARGET
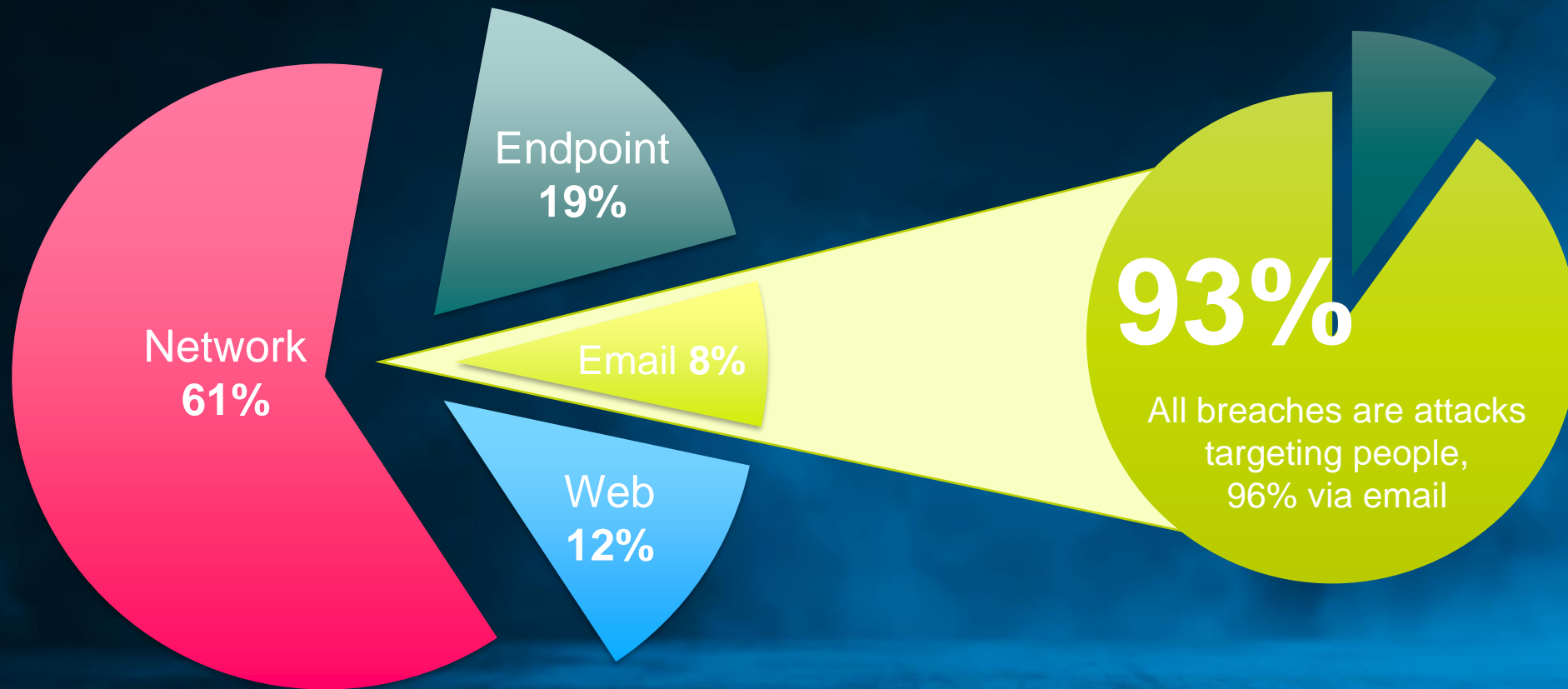
HORNETSECURITY

Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoetnt tihng is taht the frist and lsat ltteer be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe.

> info@westmoreland.org.ac
> info@westmoerland.org.ac

Spot the Difference?

maybank2u.com is not the same as
maybank2u.com

citibank.com is not the same as
citibank.com
(the first one is correct, the second one is from hackers)

The "a" in the later url is a cyrillic alphabet.

An average internet user can easily fall for this. Be careful for every mail requiring you to click on a link.

Please Stay Alert

# SOCIAL ENGINEERING ATTACKS ON COMPANIES

**HORNETSECURITY**

- **Social engineering** is all about manipulating individuals on an interpersonal level. It involves the hacker trying to gain their victim's trust and persuade them to reveal confidential information, for example, or to share credit card details and passwords.
  - Won't happen to me?

- Hackers will usually target an employee who is authorized to carry out financial transactions, sending them an urgent message from a fake email address that looks like it has come from the boss.

Hi Sharon

When you have a moment kindly let me know what details will be required to process a wire transfer payment from our operating business account to a new vendor today.

Thanks

Chris

File    Message    Help    💡 Tell me what you want to do

Ignore    Delete    Archive    Reply    Reply All    Forward    More    📧 Car Insurance -...    Team Email    Reply & Delete    → To Manage...    Done    Create New    Meeting

Junk

Delete    Respond    Quick Steps

We've Updated Your Email    12/04/2022 10:08:15

**C**    colinjwright@btconnect.com
To    colinjwright@btconnect.com

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

0.92 GB

We are closing all old ve...

CLIC

Please do not reply to th

12/04/2022 10:08:15

---

# Your latest bill is ready

Hello,
Your latest bill is now ready to view in My BT. Go to **bt.com/mybt** or click the button below:

**View your bill in My BT**

You don't need to do anything to pay it. We'll take your Direct Debit as normal. To find out when, take a look at the bill.

# Need some help?

BT STATUS: ***Active***

**Call 0800 800 150**    **Read our FAQs**

## The legal stuff

Please don't reply to this email - we won't see it.

# PHISHING TEST

https://phishingquiz.withgoogle.com/

HORNETSECURITY

Let's start with this Google Doc email

Make s

**Sharon Mosley** <sharon.mosley@westmountdayschool.org>
to me ▾

Good day colin,

Please find attached the 2022 financial a

Thanks and regards,

Ms. Sharon Mosley
Westmount Day School

Luke Joh
to me ▾

PDF

PDF 2022 F.A.R.pdf

Good effort, colin!
You got 4/8 correct.

Practice makes perfect and the more you understand what to look for, the safer you are from phishing attacks.

You can also take a few simple steps to protect your online accounts better. Learn more at g.co/2SV.

Share the quiz:

# NEXT STEPS

- Download V9 from https://www.altaro.com/downloads.php

- Until 30th June 2023

- Buy V9 with first year SMA get 2nd year FREE
- Buy V9 with additional year SMA get 3rd year FREE


- colin.wright@hornetsecurity.com
- carsten.haak@hornetsecurity.com

**HORNETSECURITY**

THANK YOU!

HORNETSECURITY