

Backup is No Longer Enough:

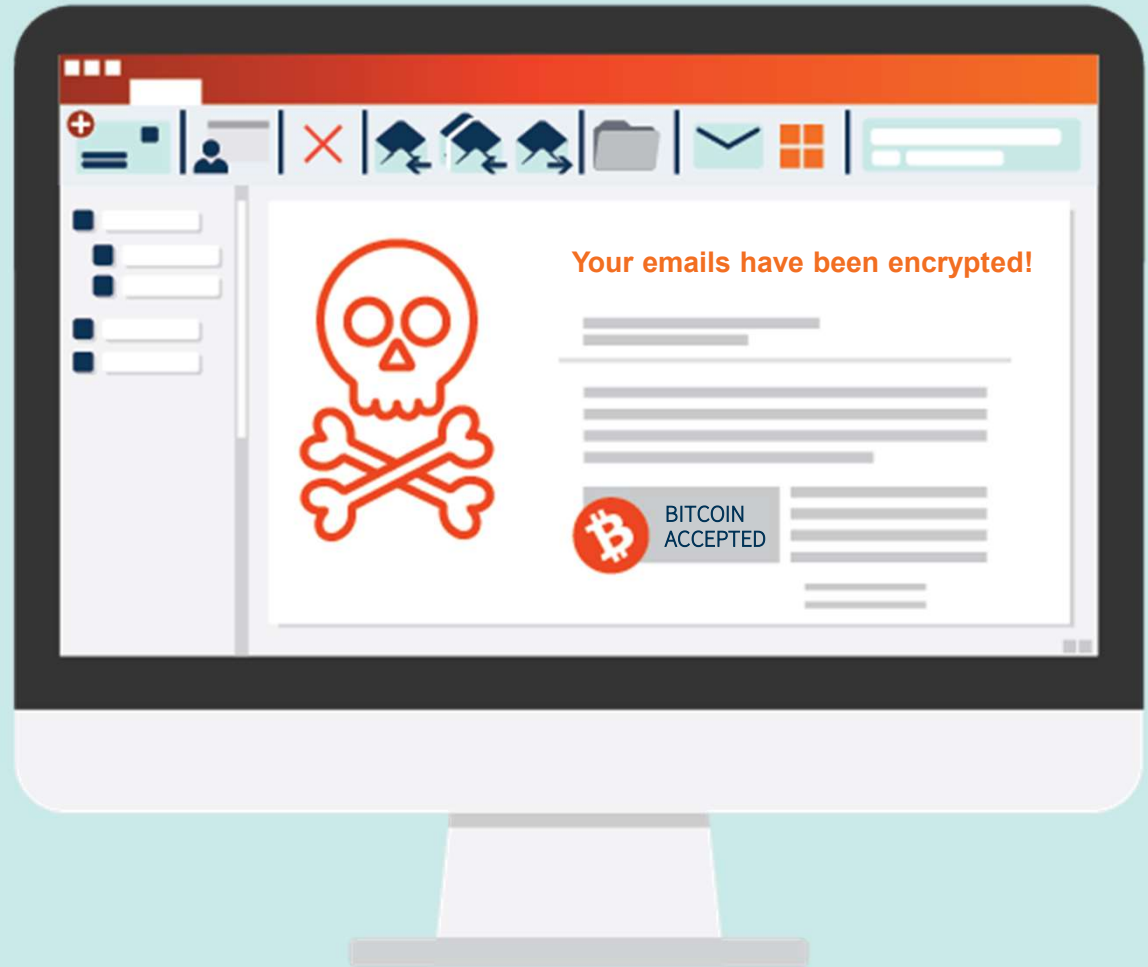
How to Protect Your Business from the #1 Cause of Data Loss

Sean Lawless- National Account Manager
Cory Hintz- Sales Engineering Manager
Adam Ward- Business Development Manager

CURE DATA LOSS

Keep business running.

This
could be
your
reality



Axcient

Threats are Escalating



The New York Times

Uber Investigating Breach of Its Computer Systems

The company said on Thursday that it was looking into the scope of the apparent hack.

Omaha World-Herald

CHI Health's parent acknowledges ransomware attack



HELPNET
SECURITY

**SMBs increasingly
vulnerable to ransomware,
despite the perception they
are too small to target**

The Growing Threat of Ransomware in 2023



RANSOMWARE

85% of MSPs report SMB ransomware attacks

50% had demands exceeding \$50,000

40% required more than 8 hours to address (\$100 to \$250 per hour)

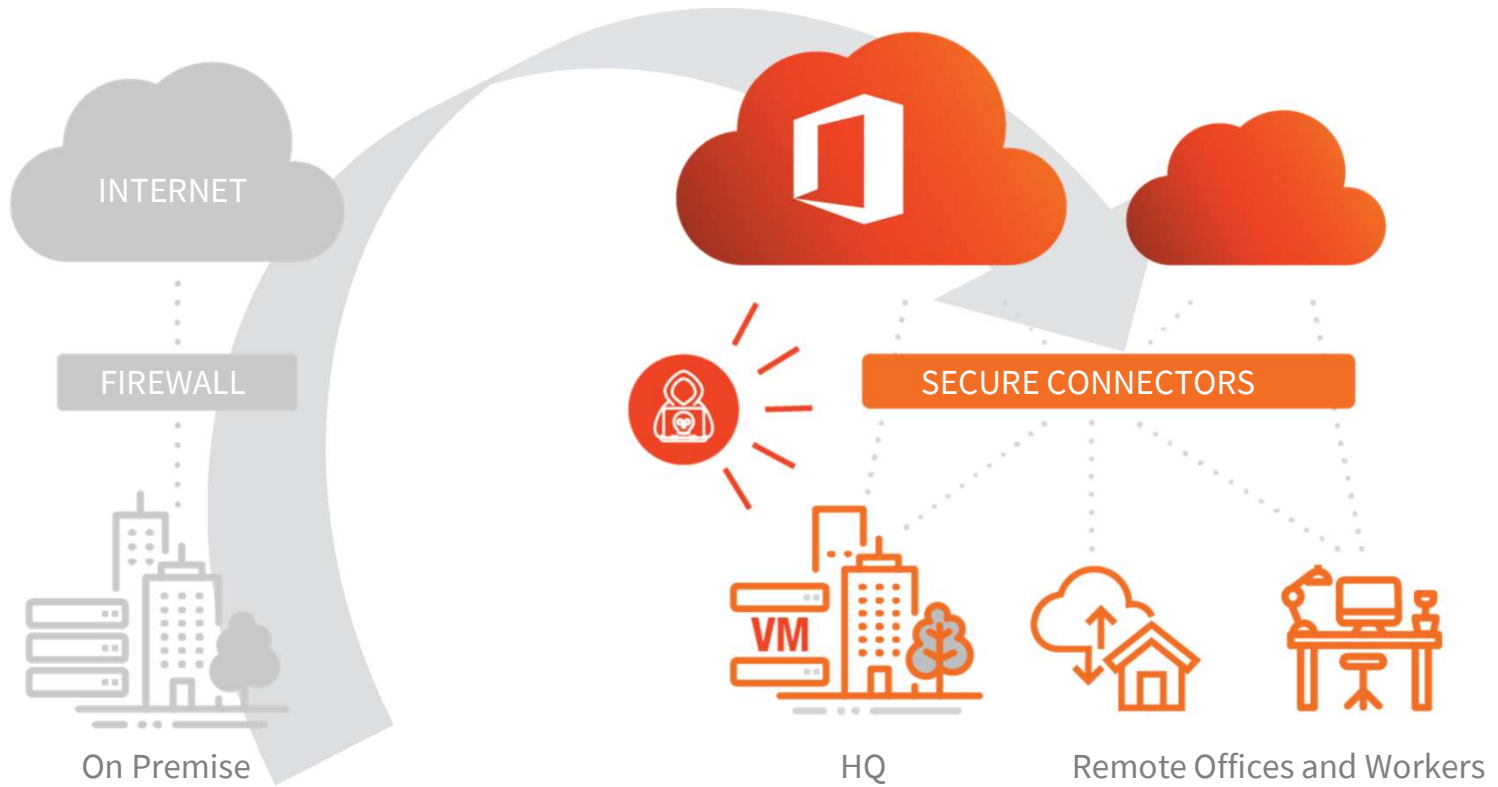
15% of people successfully phished will be phished again with 1 year



Sources: Webroot, 2021 Threat Report; CSO, Why are SMBs Under Attack by Ransomware, 2021

Axcient

Data Sprawl Due to Digital Transformation



Are You Protecting All Your Data? Everywhere?



33%

SaaS users believe applications do not need backup

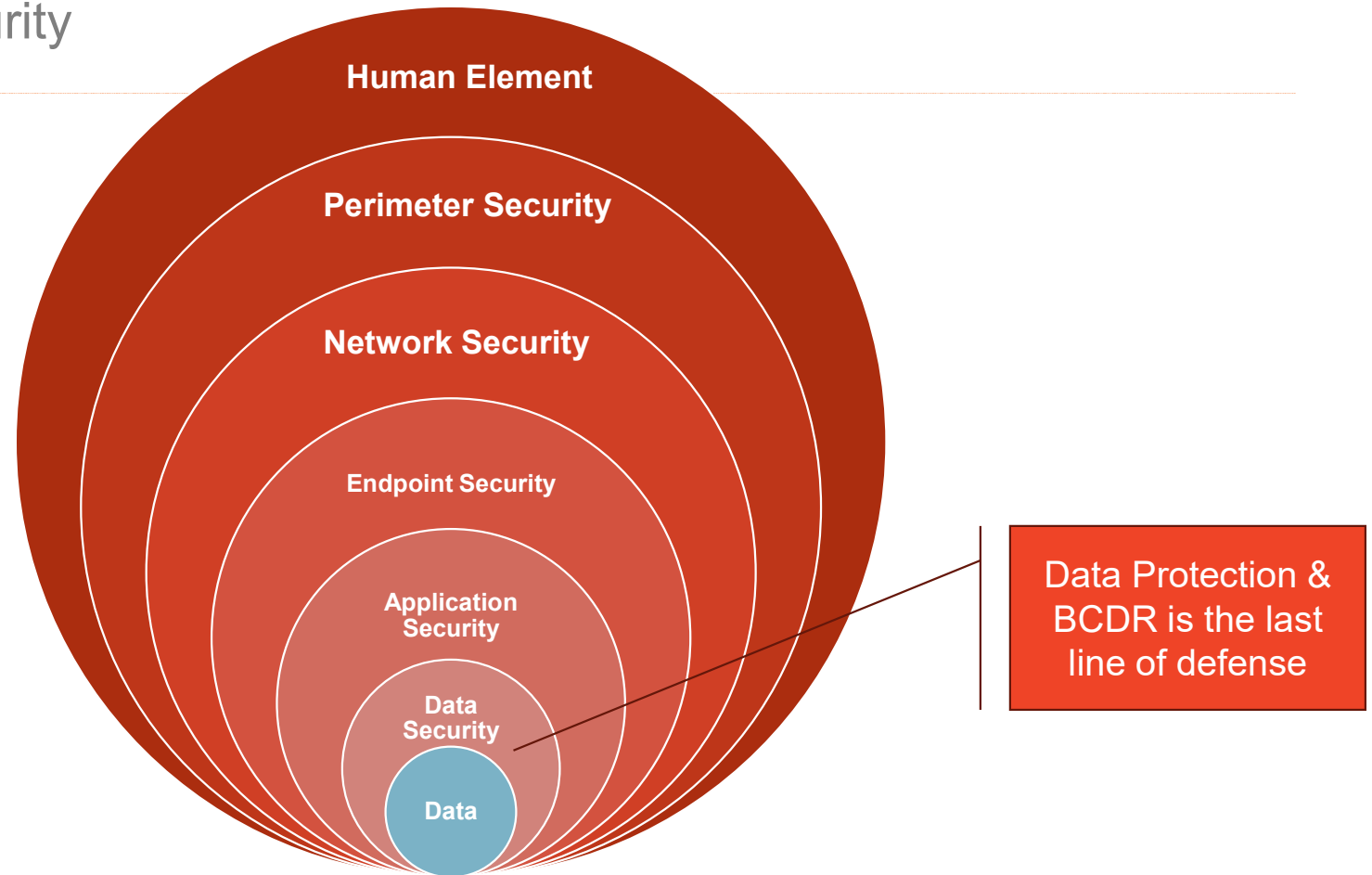


37%

believe SaaS provider is responsible for protecting data

Source: ESG, *Data Protection Cloud Strategies*, Christophe Bertrand, 2019

7 Layers of Security



The Cost of Down Time

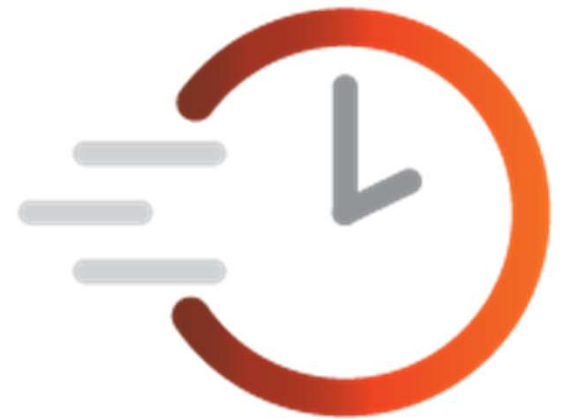
Best-in-class recovery speed and responsiveness to cyberthreats

RPO – Recovery Point Objective 15 Minutes

- The point in time before the event at which data can be successfully recovered -- that is, the time elapsed since the most recent reliable backup.
- We take image backups as often as every 15 minutes so that we can recover the data to the time a disaster strikes.

RTO – Recovery Time Objective less than 1 Hour

- The maximum acceptable amount of time for restoring a network or application and regaining access to your data after an unplanned disruption.
- We can do fast local virtualization and restores to keep your business running.



AirGap

from Axcient

Immutable Data

Requests to delete data are separated from the mechanics of data deletion.



AutoVerify

from Axcient

AutoVerify for Peace of Mind

AutoVerify is an always-on data backup check feature, which checks ALL drives with a deep check of data integrity, validates the recoverability of backups, and captures a screenshot of the protected system.

AutoVerify automatically virtualizes recent backup recovery points for each system to make sure it is recovery ready.

Then it runs numerous tests to check for:

- Bootability
- Operating system health
- Data corruption, and
- File system and application integrity

Virtual Office

from **Axcient**

Trust Your Business Continuity Plan with Virtual Office Cloud Failover






- Quickly spin up of production servers and workstations in the Axcient Cloud.
- A tool for regular full-office recovery tests to ensure backups are recoverable and your MSP is ready.
- Easily configure secure access to Virtual Office instance using VPN, Site-to-Site OpenVPN, and port forwarding.
- Data is securely encrypted in transit and at rest in our offsite SOC II Type II certified datacenters.
- Customized Runbooks enable automated spin up of your systems for disaster recovery plan testing
- Helps maintain compliance for regulations and cyber insurance requirements







Microsoft 365 and Google Workspace Data and Productivity Protection . . .

Service-level protection
for Microsoft 365

100% Backup

Service-level protection
for Google Workspace

-  **Calendar**
-  **Contact**
-  **Mail**
-  **OneDrive**
-  **Sharepoint**

-  **Calendar**
-  **Contact**
-  **Gmail**
-  **Drive**
-  **Shared drives**
-  **Sites**

Axcient

Why Protect This Data? Because Microsoft is Not Liable for Data Loss . . .

Microsoft is Not Liable for Data Loss

We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. **We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.**

Microsoft Services Agreement, Section 6b



Why Protect This Data? Google Isn't Liable for Data Loss, either

“ The only commitments we make about our services (...) are (1) described in the Warranty section, (2) stated in the service-specific additional terms, or (3) provided under applicable laws. We don't make any other commitments about our services.



[Google's Terms of Service](#)

Complete Data Protection with BCDR, Not Just Backup



Endpoint Backup

Protect data for remote employees and satellite offices



No-Appliance BCDR

Advanced server backup directly to cloud



Appliance BCDR

Backup to appliance and cloud, with immutable backups



Public Cloud Backup

Protect servers in public clouds with long-term retention



Cloud-to-Cloud

Backup, and restore Exchange, OneDrive, SharePoint and Teams

Comprehensive data protection, business continuity, and ransomware recovery

CURE DATA LOSS

Keep business running.

Questions?

