HOW THE REMOTE WORKFORCE CREATES A PERFECT STORM OF INSIDER THREAT RISK

BRINGING REMOTE WORKFORCE RISKS INTO CLEAR FOCUS

As businesses in every sector shift agility and business continuity to the top of their priority list, security teams are being forced to accept the added risks of remote employees in order to enable the business to adapt quickly, work freely and collaborate effectively. Security teams know they can't impede the cloud-based productivity that powers the WFH world of work. But accepting risk does not mean ignoring it, and here's the troubling reality many security teams are missing: The data portability and user agility of the WFH world, combined with the acute pressures of the post-COVID business climate, combine to create a perfect storm of insider threat risks.

Empower Agility — Ensure Business Continuity

Facing converging — and rapidly evolving — market pressures, businesses in every sector are making business agility and business continuity their top priorities.

THE GOAL

Make sure we have the tools we need to...

CONNECT TO INTERNAL RESOURCES → **COLLABORATE (INTERNALLY AND WITH 3RD PARTIES)** → **GET OUR JOBS DONE** → **SERVE OUR CUSTOMERS**

IN THE FACE OF...

EVOLVING CUSTOMER DEMAND

Rapidly rising & shifting consumer expectations

INCREASING MARKET COMPETITION

Urgent need to gain/ sustain an edge

UNCERTAIN WORKPLACE CONDITIONS

Sudden shift to work from home

ENABLE CLOUD COLLABORATION

Businesses increasingly recognize cloud-based productivity and collaboration as the key to unlocking the agility and business continuity needed to succeed in the new world of work. They're willingly trading the increased risk of cloud-based work for the competitive advantages it delivers.

50% growth in the adoption of cloud services across all industries in early 2020*

REMOTE CONNECTIVITY

Connecting from beyond the perimeter, personal devices, etc.

ANYTIME-ANYWHERE PRODUCTIVITY

Using cloud- and web-based apps

FRICTIONLESS COLLABORATION

Easily sharing files and data via the web and cloud

*https://www.csoonline.com/article/3545775/use-of-cloud-collaboration-tools-surges-and-so-do-the-attacks-report-shows.html

Off-Network Activity

Security teams know they have to come to terms with tolerating more risk in an increasingly decentralized work environment. But as collaboration culture collides with the sudden shift to WFH in most organizations, Security teams are recognizing a blind spot in the typical security stack: Conventional security tools were built to work within an LAN and/or VPN—and they're blind to the rapidly growing off-network activity of the remote workforce.

Decentralized Work = More Off-Network Activity

NON-VPN ACTIVITY

Only 10% consistently use VPN

CLOUD-BASED APPS

Legacy tools can't see web/ cloud activity

SHADOW IT

1 in 3 use unsanctioned apps daily

THE POST-COVID BUSINESS WORLD

The technological infrastructure of the cloud-based remote workforce creates the perfect *conditions* for insider threat going undetected. But it's the unique pressures of the post-COVID business world that whip those conditions into a perfect storm for insider threat risk.

> "**THE MOMENTUM OF** digital transformation projects will outpace the ability of organizations to accommodate the changes, introducing additional complex threats. Neither the pace of change, nor the evolving risk landscape will wait for business continuity management and organizational resilience strategies to evolve and catch up."
>
> **–Gartner 2020 Strategic Road Map for Business Continuity Management**

STRESSED USERS

Uncertain business climate and work conditions push users to behave less consistently/predictably

DISGRUNTLED USERS

Frustrations over pay cuts, furloughs, WFH conditions, etc. lead to more risky user behaviors

ISOLATED USERS

Workforce changes may disrupt employee satisfaction/loyalty, leading to less responsible behaviors

How do you see, understand and manage this risk?

The acute pressures around the COVID crisis won't last forever, but it's clear that this situation has accelerated a transformation in the way we work. More remote workers and more flexible work arrangements. More collaborative and iterative workflows. More cloud- and web-based technologies. Security teams know they need to get comfortable tolerating risk to promote agility and protect continuity. But to tolerate risk, you need to see it—otherwise you're just flying blind. It's time that security tools designed for the way we work now—tools that consider all users, all files, and all the ways we connect, collaborate and move files today.

CODE42

Check out Incydr:

→ code42.com/product