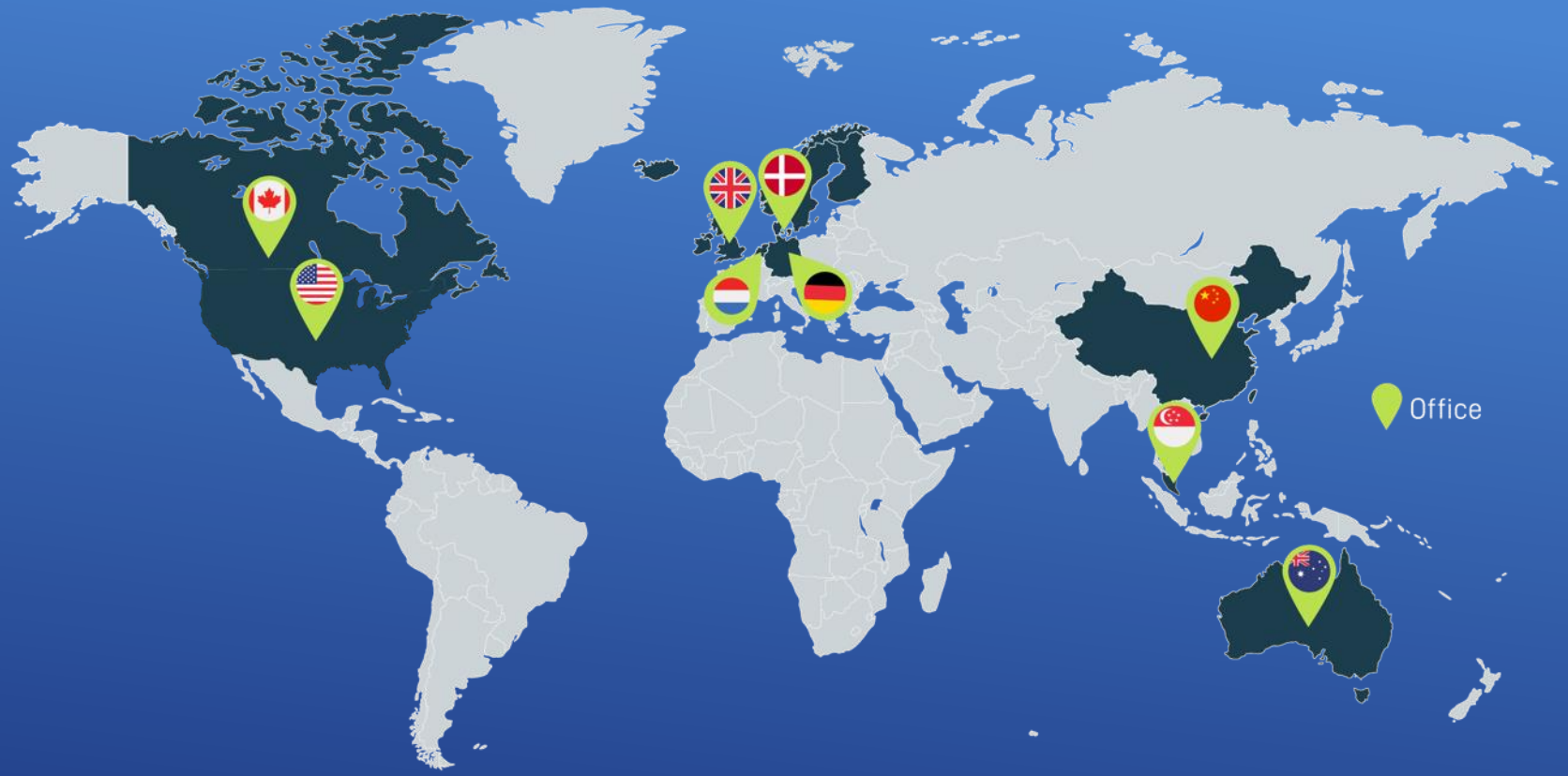
A Futuristic Look at Cyber Threats & Protection

Taylor Thorson
Channel Development Manager

Kaseya®

Kaseya®

The world's leading provider of Business Continuity solutions



Founded in 2007

23 Offices Globally
9 Private Data Centers

800,000+ SMB's protected

4,000+ Employees worldwide & growing

Kaseya®


CYBER THREATS
DISRUPTING
BUSINESS
OPERATIONS
Kaseya®

WHAT IS CYBER RESILIENCE?

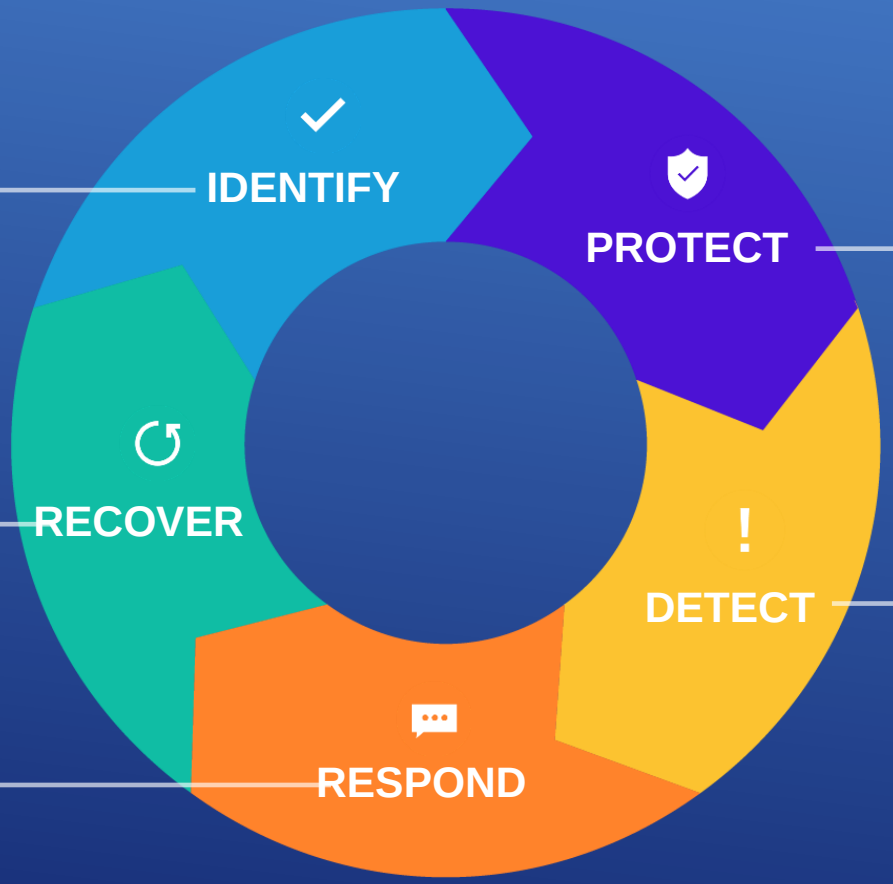
Kaseya®

Cyber Resilience is a measure of business strength in preparing for, operating through, and recovering from the eventuality of a cyber attack.

Cyber resilience relies on the successful ability to **identify, protect, detect, respond** and **recover** quickly from an adverse cyber event and combines cybersecurity, business continuity, and incident response.

Kaseya®

NIST Cyber Security Framework



- Asset Management
- Business Environment
- Risk Management & Strategy
- Governance
- Risk Assessment
- Supply Chain Risk Management

- Identity Management, Authentication, & Access Control
- Awareness & Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance
- Protective Technology

- Anomalies & Events
- Security Continuous Monitoring
- Detection Processes

- Communications
- Mitigations
- Improvements
- Response Planning
- Analysis

- Recovery Planning
- Improvements
- Communications

Kaseya®


WE ARE UNDER ATTACK!!

ALL OF US

TOP INDUSTRIES TARGETED BY CYBER CRIMINALS

Healthcare

Government & Municipalities

Education

Technology Providers

Professional Services

Financial Institutions

WHY ARE YOU BEING TARGETED

Kaseya®

WHY CYBER CRIMINALS ARE TARGETING YOUR ORGANIZATIONS

- Targets that provide a cache of useful data
- Host sensitive information for multiple organizations
- SMB’s often lack strong cybersecurity defenses
- Data is hosted / stored in many locations
- Compliance obligations (HIPAA, PII, PHI, PCI)

Kaseya®

HOW OFTEN IS A BUSINESS HIT WITH RANSOMWARE?

Kaseya®

- **46%** Of All Cyber Attacks Are Aimed At Small And Medium Sized Businesses.

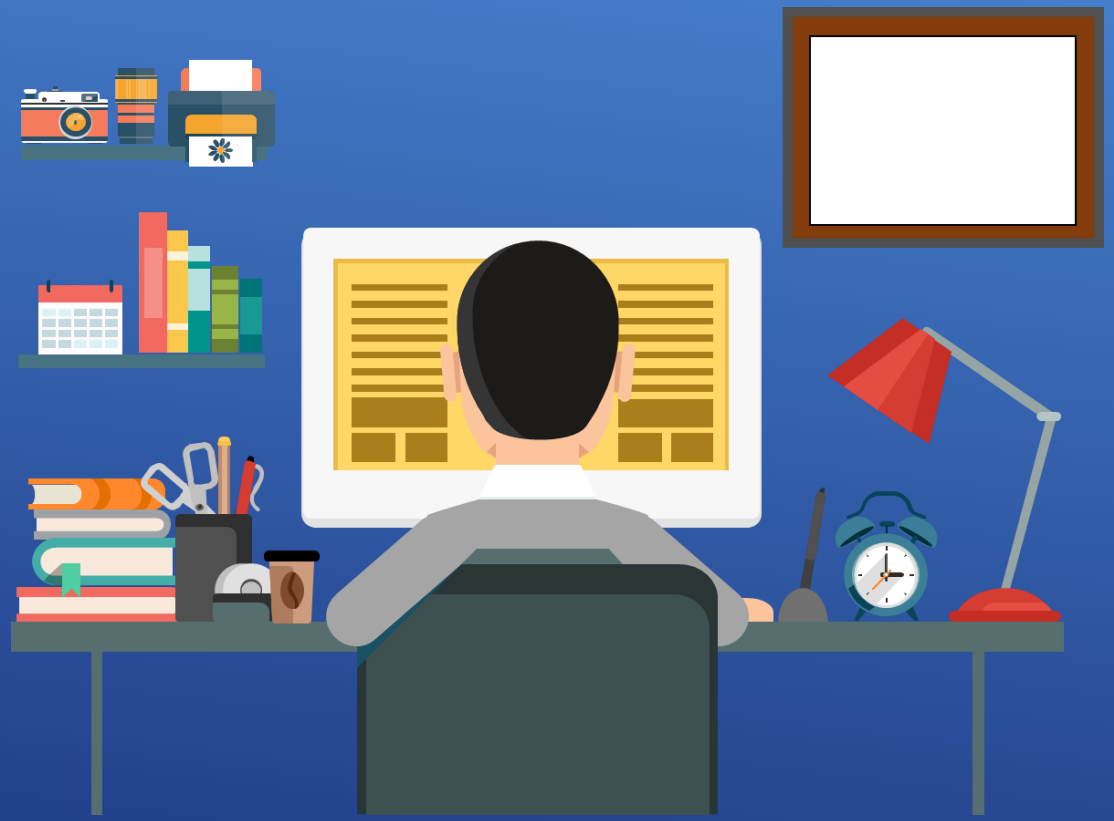
- **85%** Of **All** Email Attachments Are Harmful.

- **91%** Of Attacks Are Launched From A Phishing Attack.

- Cyber Crime Will Cost **$8** Trillion in 2023.

- **24,000** New Malicious Apps Are Removed From The App Store Daily.

- **A Business Is Hit With Ransomware Every 11 Seconds.**



Kaseya®

“Lincoln College has been serving students from across the globe for more than 157 years,” said David Gerlach, president of Lincoln College. “The loss of history, careers, and a community of students and alumni is immense.”

CHI Health: System outages due to ransomware attack

Since the attack, CHI Health workers and nurses have been forced to go back to doing everything by hand, including charting patient information.

City of Wayne falls victim to ransomware cyber attack

WHAT CAN WE DO ABOUT IT

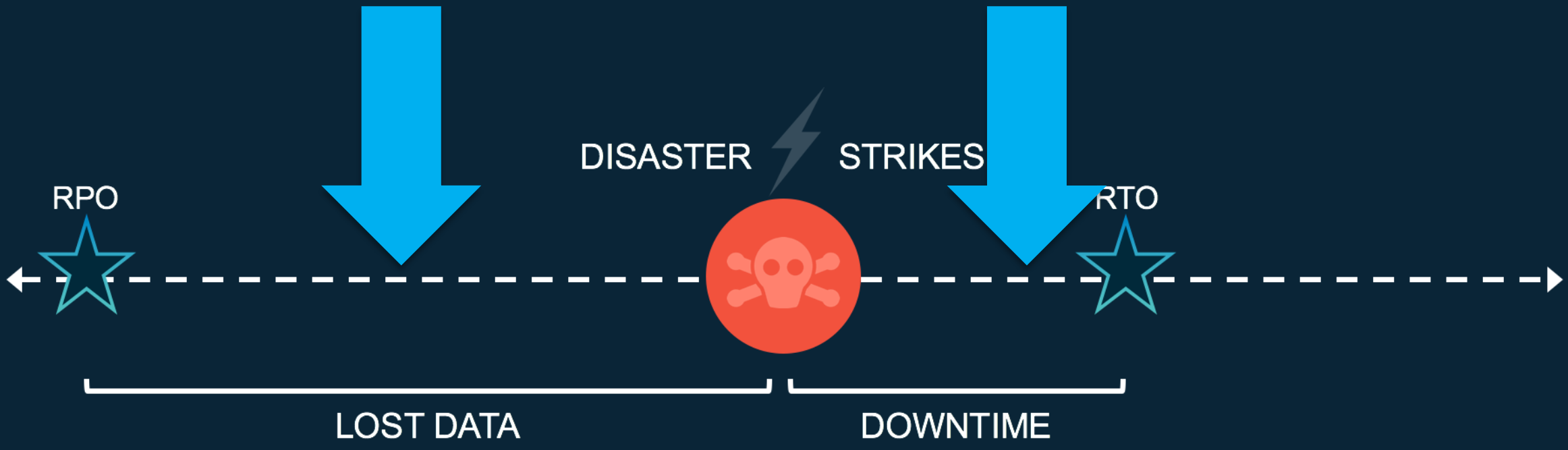
Kaseya®

CYBER RESILIENCE TODAY STARTS WITH BUSINESS CONTINUITY

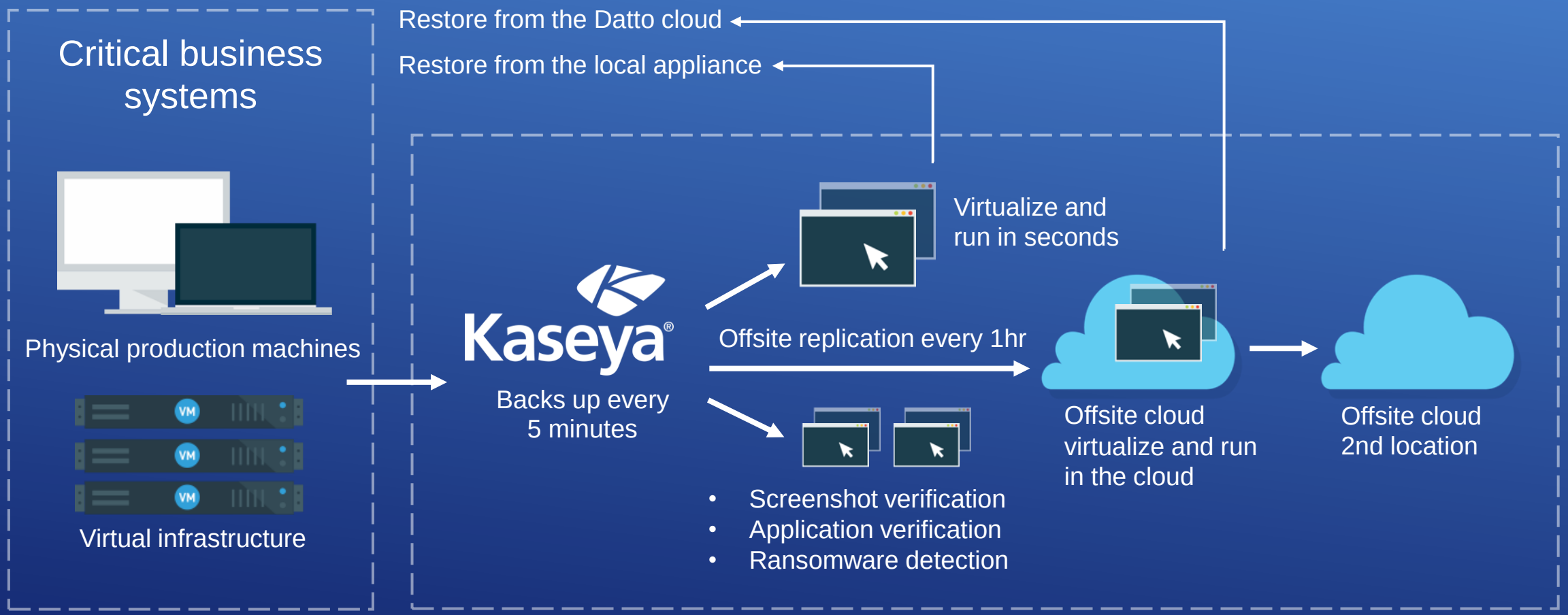
Kaseya®

Business continuity is the ability to keep running through a disaster or data loss.

Kaseya®

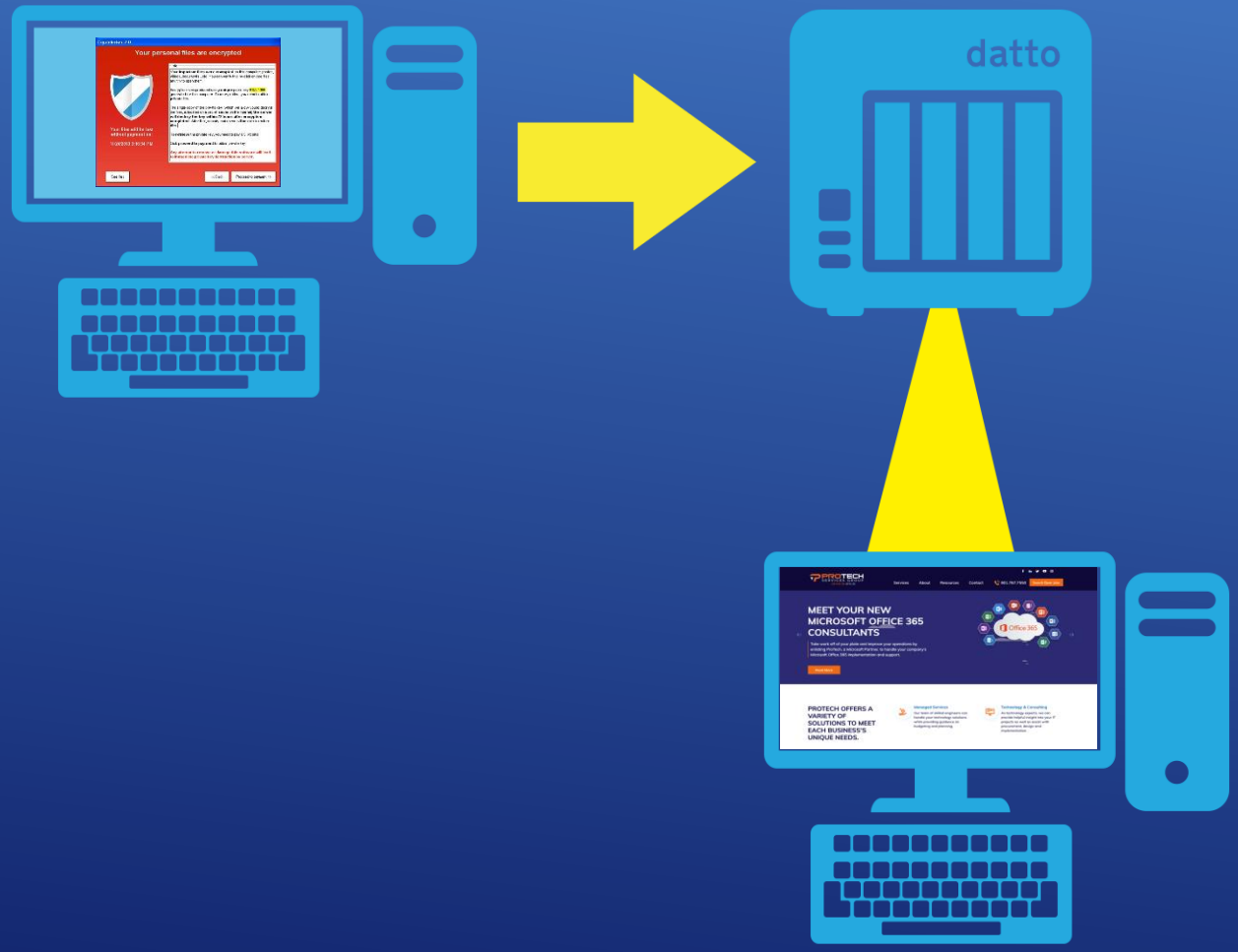

DISASTER
STRIKES
RPO
RTO
LOST DATA
DOWNTIME

CONTINUITY IN ACTION



Kaseya®

CONTINUITY IN ACTION



Benefits of Virtualization

- Reduces downtime
- Local and cloud
- Helps your RTO/RPO

Kaseya®

ON-PREM PLATFORMS ARE SLOWLY MOVING TO CLOUD HOSTED INFRASTRUCTURE

Kaseya®

BUSINESS CONTINUITY TOMORROW WILL INCLUDE SaaS PROTECTION

Kaseya®

In 2022, the market for software-as-a-service (SaaS) was

$250 billion

— by 2029 that number will be $**883 billion**.

78% of businesses

will be run almost entirely on SaaS and SaaS application

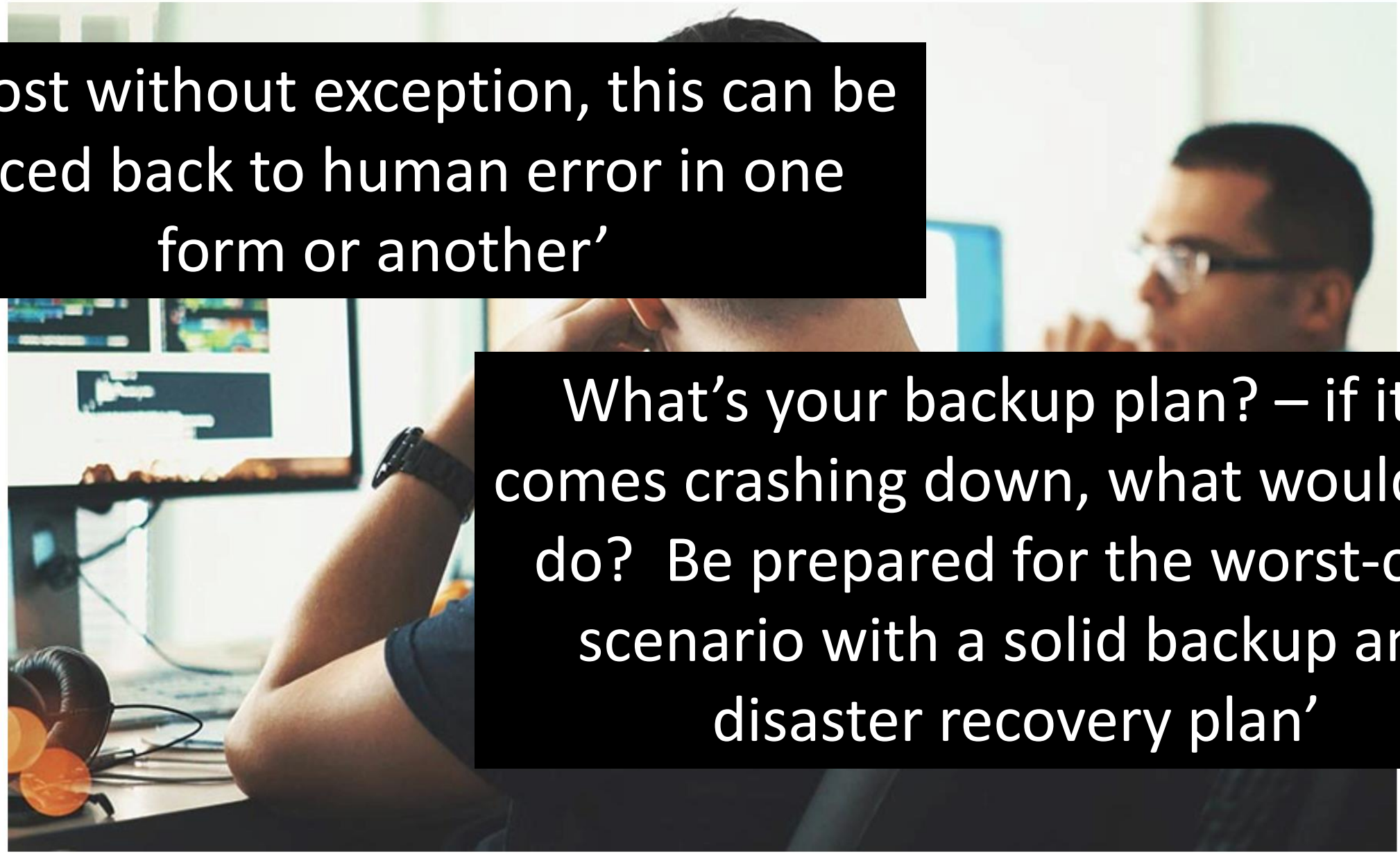
Source: BetterCloud Report and Gartner

Google Workspace

Microsoft 365

Kaseya®

Microsoft Office 365 – convenience in the cloud or an open invitation to hackers?



Almost without exception, this can be traced back to human error in one form or another’

What’s your backup plan? – if it all comes crashing down, what would you do? Be prepared for the worst-case scenario with a solid backup and disaster recovery plan’

THE SHARED RESPONSIBILITY MODEL

Microsoft/G-Suite provides for the security of the cloud, and the tenant (partner) provides the security in their cloud.

Microsoft 365

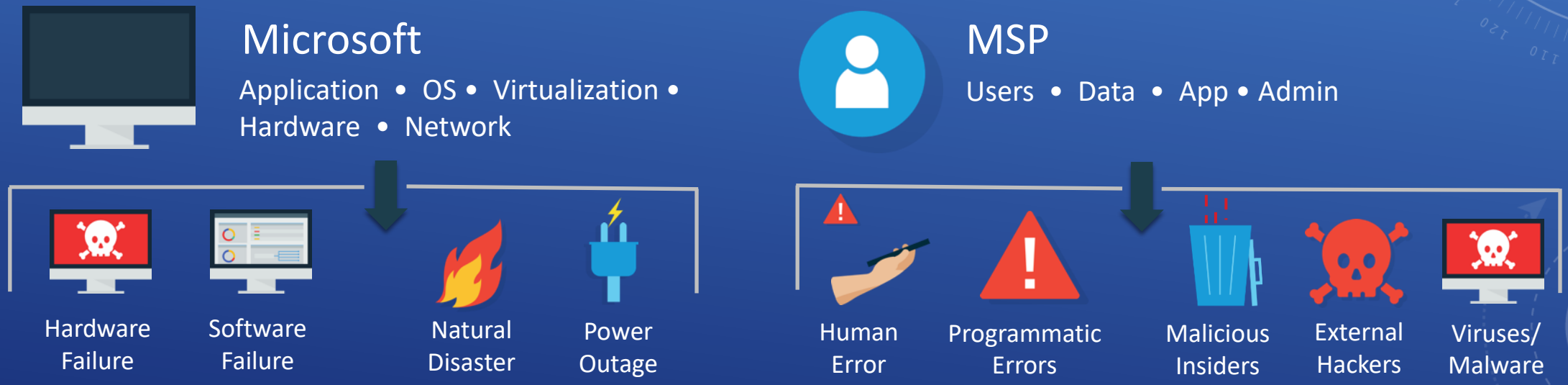
DATA RETENTION AND DELETION

MICROSOFT WILL RETAIN CUSTOMER DATA THAT REMAINS STORED IN ONLINE SERVICES IN A LIMITED FUNCTION ACCOUNT FOR 90 DAYS AFTER EXPIRATION OR TERMINATION OF CUSTOMER'S SUBSCRIPTION SO THAT CUSTOMER MAY EXTRACT THE DATA. AFTER THE 90-DAY RETENTION PERIOD ENDS, MICROSOFT WILL DISABLE CUSTOMER'S ACCOUNT AND DELETE THE CUSTOMER DATA AND PERSONAL DATA WITHIN AN ADDITIONAL 90 DAYS, UNLESS MICROSOFT IS PERMITTED OR REQUIRED BY APPLICABLE LAW TO RETAIN SUCH DATA OR AUTHORIZED IN THIS AGREEMENT.

MICROSOFT HAS NO LIABILITY FOR THE DELETION OF CUSTOMER DATA OR PERSONAL DATA AS DESCRIBED IN THIS SECTION.

Cloud data protection: a shared responsibility

The message is simple - Microsoft is responsible for their cloud, end users and their MSPs are responsible for what's in it.



1 IN 3

COMPANIES USING SAAS LOSE DATA

ABERDEEN: “SAAS DATA LOSS: THE PROBLEM YOU DIDN’T KNOW YOU HAD”

47%

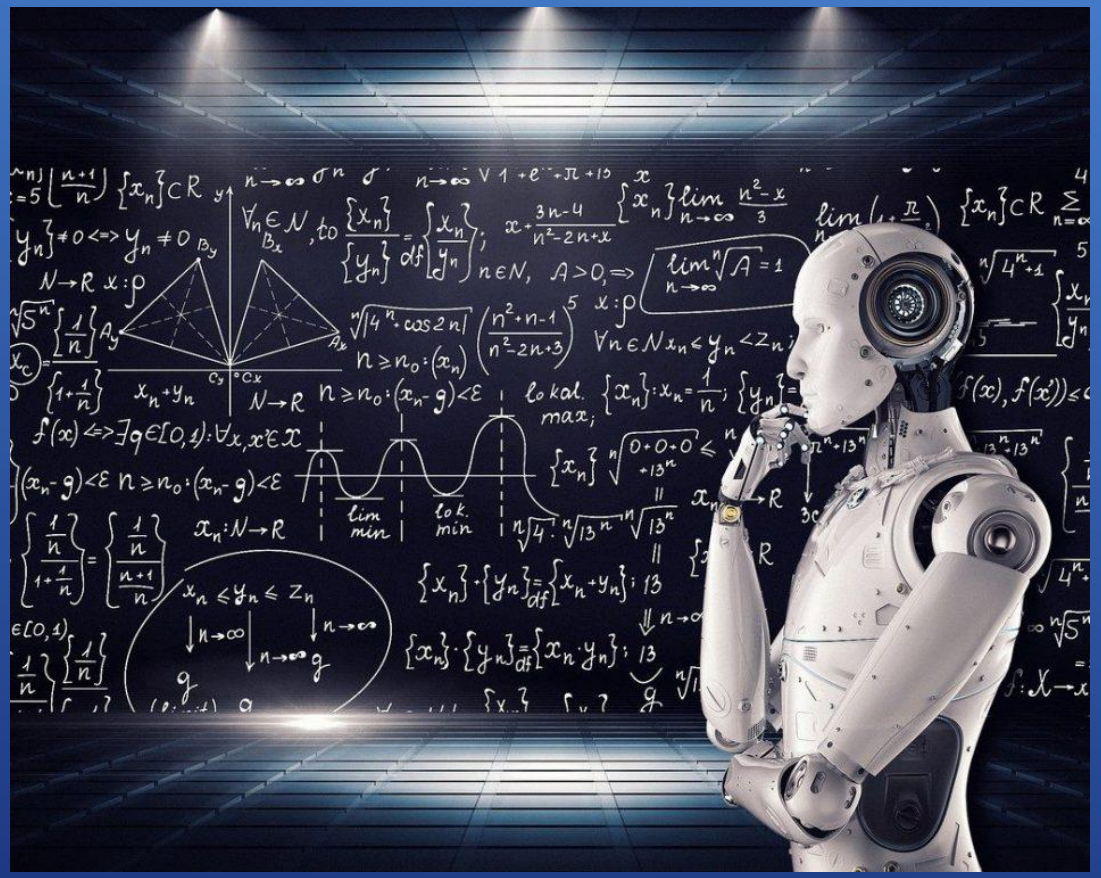
OF DATA LOSS IS CAUSED BY END-USER DELETIONS

datto

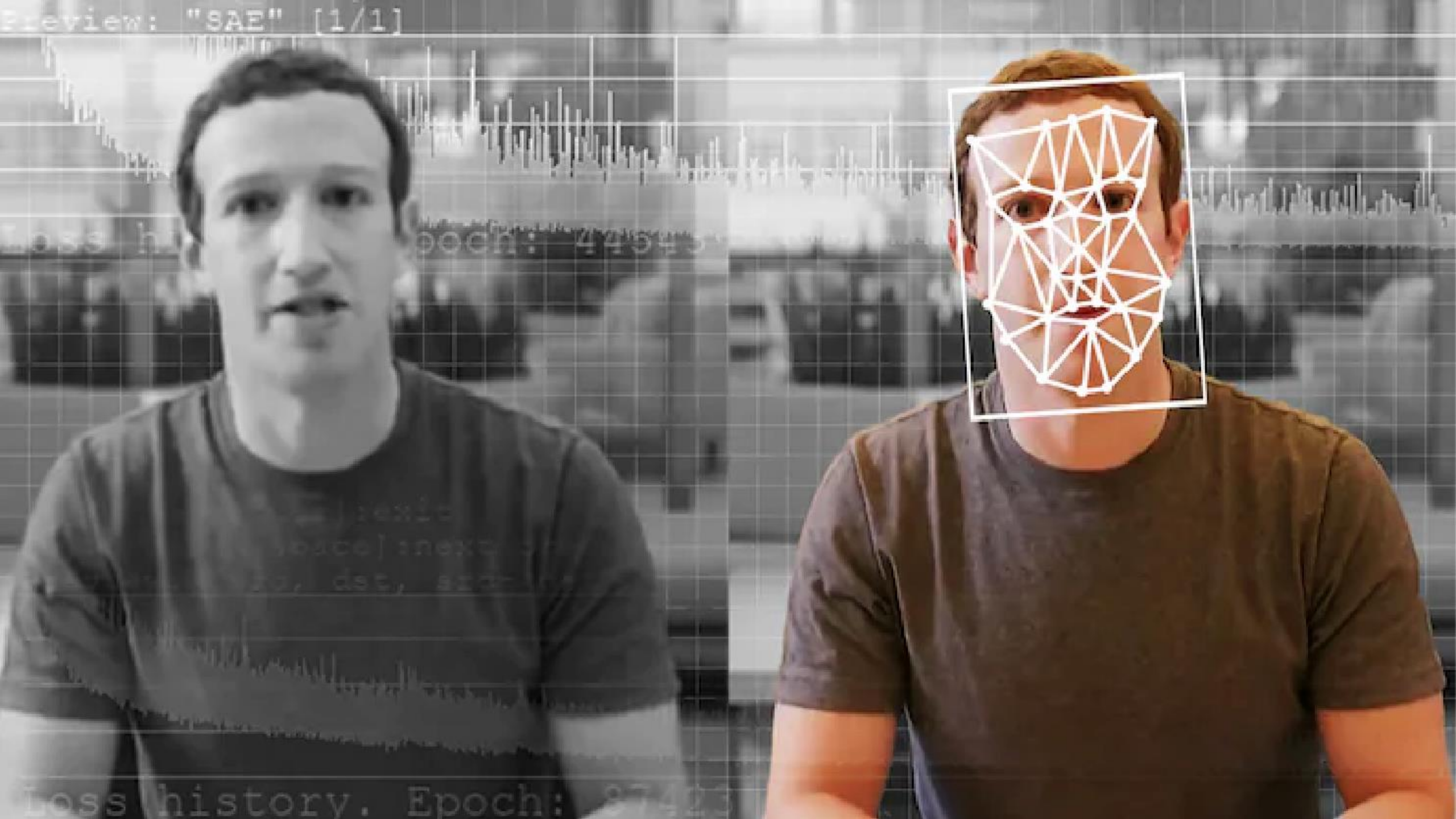
20%

OF DATA LOSS IS CAUSED BY A MALICIOUS ACT

WHAT ELSE SHOULD WE BE THINKING ABOUT?




DEEPFAKE TECHNOLOGY


Preview: "SAE" [1/1]
ss history. Epoch:


MADE WITH
Revive


DEEPFAKE VOICE
TECHNOLOGY

Deepfake Phishing: Is That Actually Your Boss Calling?

Deepfake technology is outpacing our ability to spot it. That could be bad news for cybersecurity.

Tatum Hunter

November 10, 2020 · Updated: April 19, 2021

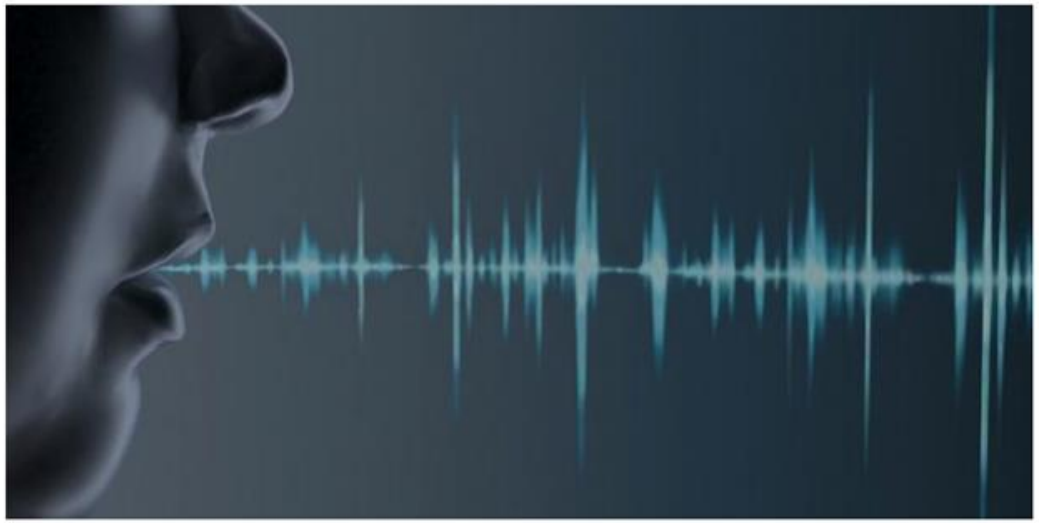
When you hear the term "deepfake," you probably think of synthetic reproductions of politicians or celebrities. But, starting now, you should also think about your boss.

Remote work is putting companies at greater risk of deepfake phishing attacks, executives at Technologent warned during a cybersecurity webinar last week. In a deepfake attack, criminals use synthetic audio to mimic the tone, inflection and idiosyncrasies of an executive or other employee. Then, they ask for a money transfer or access to sensitive data.

Concern about deepfakes — or technology that uses machine learning to realistically recreate the face, body or voice of a real person — has been on the rise as open-source tools like DeepFaceLab and Avatarify gain traction.

These Bank Robbers Used Deepfake To Imitate Boss' Voice And Siphon Off $35 Million

Armeen Khan October 18, 2021 0



Excess of everything is bad…

Not long ago, Justin Bieber fell prey to a deepfake version of Tom Cruise and now it seems like the technology is even being used to commit heists. A bank in the United Arab Emirates was fooled by criminals using AI voice cloning which ended with them stealing $35 million dollars. Deepfake technology is getting more advanced day by day and dangerous as well…

According to court documents in Forbes' custody, the robbers used a deepfaked voice of the company executive to fool the bank manager to transfer millions of dollars to their possession in early 2020. The

Recent Posts

The U.S Has Strongly Criticised A Russian Anti-Satellite Test That Created A Dangerous Debris Field In Space

Chile Wants To Export Solar Energy To Asia – Using A 15,000km Submarine Cable

This New Defense Drone Can Carry 16 Hellfire Missiles In-Flight – More Than Ever Before

This New Earthgazing VR Experience Will Help Astronauts Cope With Loneliness In Space

Researchers Have Come Up With A New Way To Quickly Turn Plastic Waste Into Graphene

MUST READ: Workplace monitoring is everywhere. Here's how to stop algorithms ruling your office

Forget email: Scammers use CEO voice 'deepfakes' to con workers into wiring cash

AI-generated audio was used to trick a CEO into wiring $243,000 to a scammer's bank account.

By Liam Tung | September 4, 2019 | Topic: CXO

Criminals are using AI-generated audio to impersonate a CEO's voice and con subordinates into transferring funds to a scammer's account.

RELATED


Yahoo pulls plug on services in China: Report


An Apple executive said something extraordinary. You may think about this for days


As technology skills demand grows, so does attention to low-code and no-code solutions

AI-DRIVEN MALWARE

Kaseya®

WHAT IS AI-DRIVEN MALWARE?

Kaseya®

AI-DRIVEN MALWARE

AI-driven malware is conventional malware altered via AI to make it **more effective**. It can use its intelligence to infect computers faster or make attacks more efficient.

Conventional malware in a sense is dumb. It is a set of pre-created, fixed code that tries to sneak past defenses. In contrast AI-driven malware can **think for itself**, to an extent.

Kaseya®

HOW DOES IT THINK FOR ITSELF?

AI uses deep learning via an algorithm of data and creates its own rules. For example, facial recognition in photos. Applied to malware AI can perform tasks that are impossible with traditional software structures.

This means it is very difficult for contemporary endpoint security to identify malware that doesn’t conform to these traditional rules.

Kaseya®

POSSIBLE CRIMINAL USES OF AI-DRIVEN MALWARE

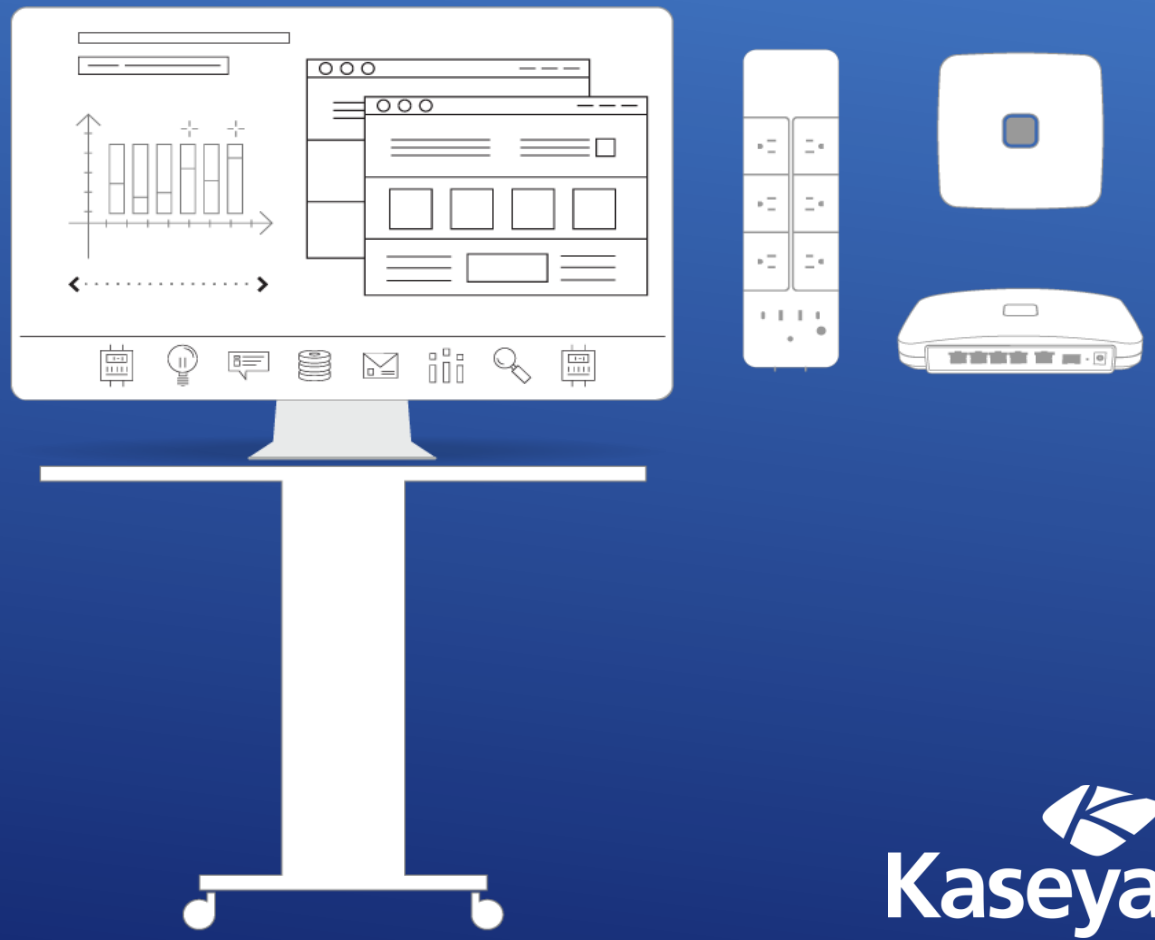
- Solving CAPTCHAs to sneak past authentication
- Scan social media to find contacts to bolster phishing attacks
- Create more convincing, customized and targeted spam

Kaseya®

CYBER RESILIENCE BEYOND

Kaseya®

THE WORKFORCE WILL INCLUDE MORE FLUID WORKSPACES



Kaseya®


CONNECTED DEVICES TODAY
~ 11.2 BILLION


CONNECTED DEVICES TOMORROW
~ 20+ BILLION

WHERE DO WE GO FROM HERE?

Kaseya®

YOU ARE A TARGET ONLINE AND OFFLINE

Don't ever say "It won't happen to me". We are all at risk and the stakes are high - to your personal and financial well-being.

Kaseya®

POLICY AND PROCEDURES

Have written Policies and Procedures in place to protect your organization can help!

Kaseya®

ON-GOING EMPLOYEE TRAINING

Conduct User Awareness Training at twice a year if not every quarter. 90% Of Network Breaches Are Caused By User Error. REGULARLY Train Employees To Avoid Risks.

Your MSP can help!

Kaseya®

PASSWORD MANAGEMENT

Use Password Policies for your organization.

Kaseya®

- 65% of people reuse passwords across multiple sites
- 95% claim to understand risk of reusing passwords across multiple site, 59%
- do it anyway
- 49% of employees change or add a digit or character to their password when updating company password every 90 days.

Kaseya®

USE MULTIFACTOR IDENTIFICATION

Implementing multi-factor authentication is one of the most effective ways to prevent unauthorized access to sensitive data.

Kaseya®

NEVER LEAVE DEVICES UNATTENDED

The physical security of your devices is just as important as their technical security.

Kaseya®

BE CAREFUL ON WHAT YOU CLICK

Avoid visiting unknown websites or downloading software from untrusted sources

Kaseya®


EPSON
OLYMPUS
Haier
HYUNDAI

PEOPLE ARE YOUR GREATEST RISK

Kaseya®

ANTI-VIRUS AND MALWARE PROTECTION

Only install an anti-virus program from a known and trusted source. Keep virus definitions, engines and software up to date to ensure your anti-virus program remains effective.

Kaseya®

SECURITY TESTING | CONFIGURATIONS

Work with your managed service provider to set this in place

Kaseya®

ESTABLISH AN INCIDENT RESPONSE PLAN

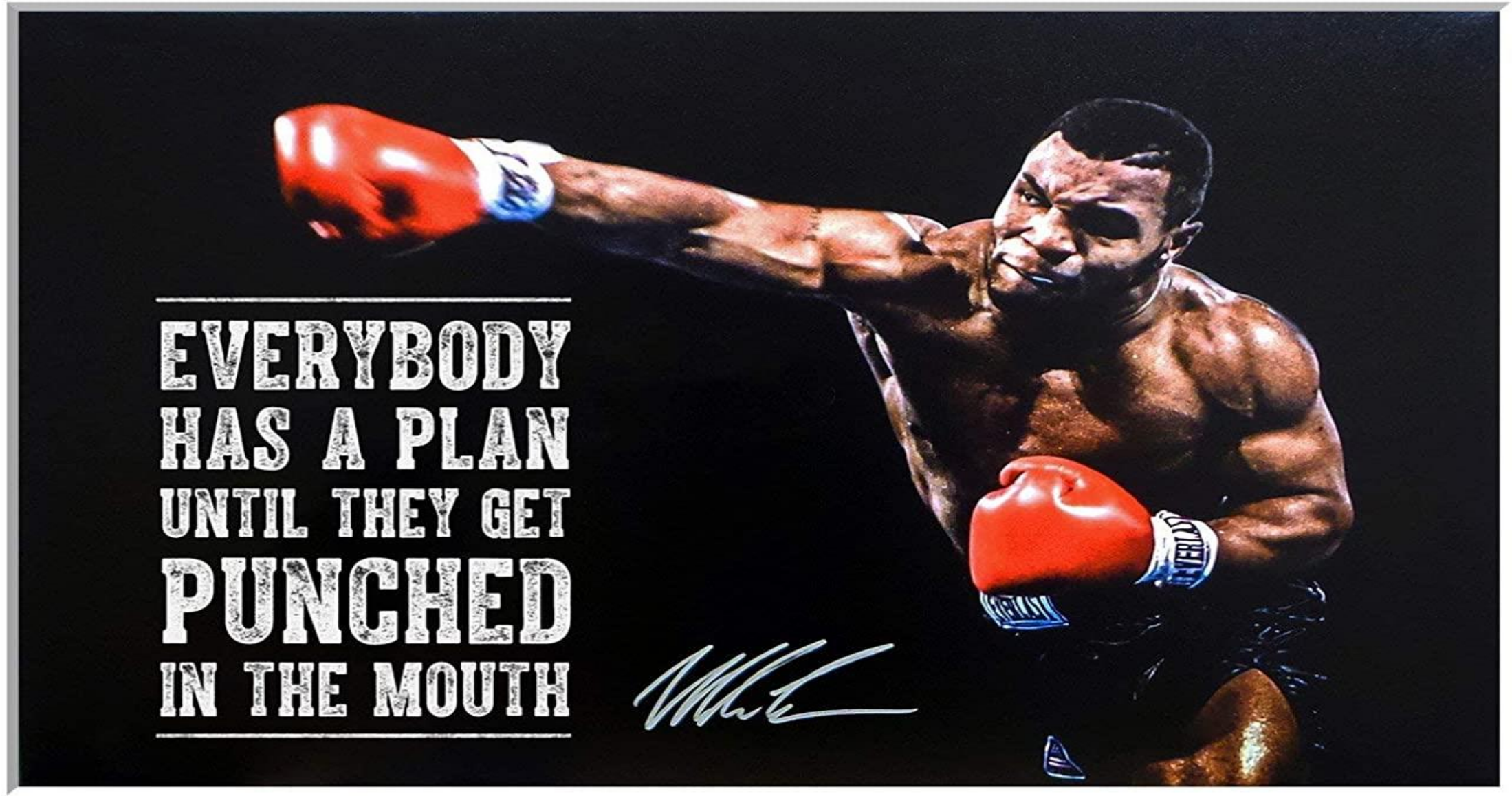
24% of businesses with 1-19 employees aren't prepared for the top threats to their network.

Kaseya®

CONTINUITY!!!!!! MUST HAVE

Back up regularly - if you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install the system.

Kaseya®


EVERYBODY
HAS A PLAN
UNTIL THEY GET
PUNCHED
IN THE MOUTH

THANK YOU!

Kaseya®