Zero Trust Workplace Solution

Matthew Raida

Workplace Engineer

Abel Molina

Workplace Leader

September 2021

Softchoice

Agenda

Softchoice

- Who Are We?
- The Progress and Advancements
- The Softchoice ROI

Zero Trust

- The need for a Zero-Trust Solution
- Things to Know About Zero Trust Adoption
- Old World vs. Current World
- Zero Trust Principals and Holistic Security Strategy

Softchoice Offerings: Overview

- Zero Trust Workplace Solution
- Overview and Direction
- The Breakdown

Questions & Answers

Softchoice

31 years in business	**10,000+** customers	**1,400+** cloud customers and growing
1,800+ team members across North America	**500+** successful cloud migrations	**5,000+** technical assessments delivered annually
3,000+ enterprise agreements managed	**85% growth** in our engineering and solutions architect headcount	**700** managed services customers
15 straight years as a Best Workplace in Canada	**10,000+** paid volunteer days taken	**400+** technical resources

Cloud

Workplace

Modern technology

- Collaboration, messaging, calling and meetings
- Virtual desktop
- Enabling devices: headsets, conferencing, laptops, digital whiteboards, device and application management, meeting rooms

Optimize technology

- Workplace Accelerator
- Managed Workplace
- Adoption Services
- Security Services

Innovate business

- Workplace Automation

Reduce cost

- Enterprise Lifecycle Management
- Software Rationalization

The Softchoice ROI

Powered by data, anchored in customer success

I nnovate

Advanced professional services for application modernization, modern data estates and intelligent workplace analytics

Transformation

O ptimize

Get the most out of your technology and build agility with cloud and engagement with digital workplace with powerful assessments, advanced and managed services

Agility

Engagement

R educe

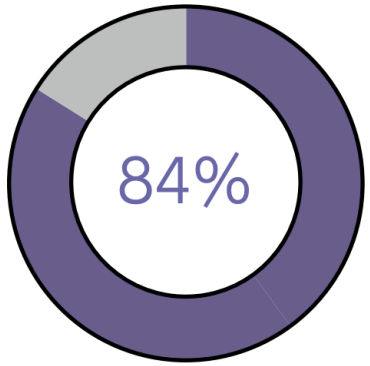
Rationalize your technology spend and drive ongoing optimization through lifecycle management

Efficiency

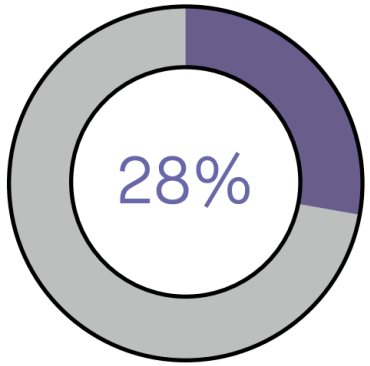
Why the need for a Zero-Trust Solution

The State of Cloud Security 2020 Report

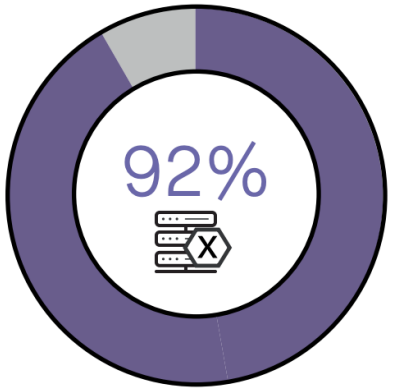
ARE CONCERNED THEY'VE BEEN HACKED AND DON'T KNOW IT



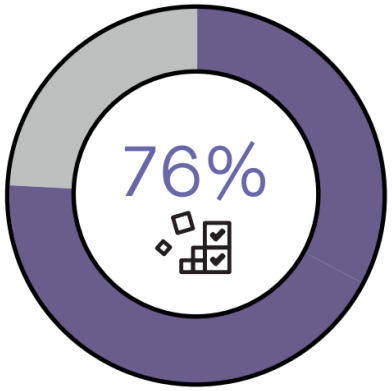
HAVE ALREADY BEEN HACKED AND KNOW IT



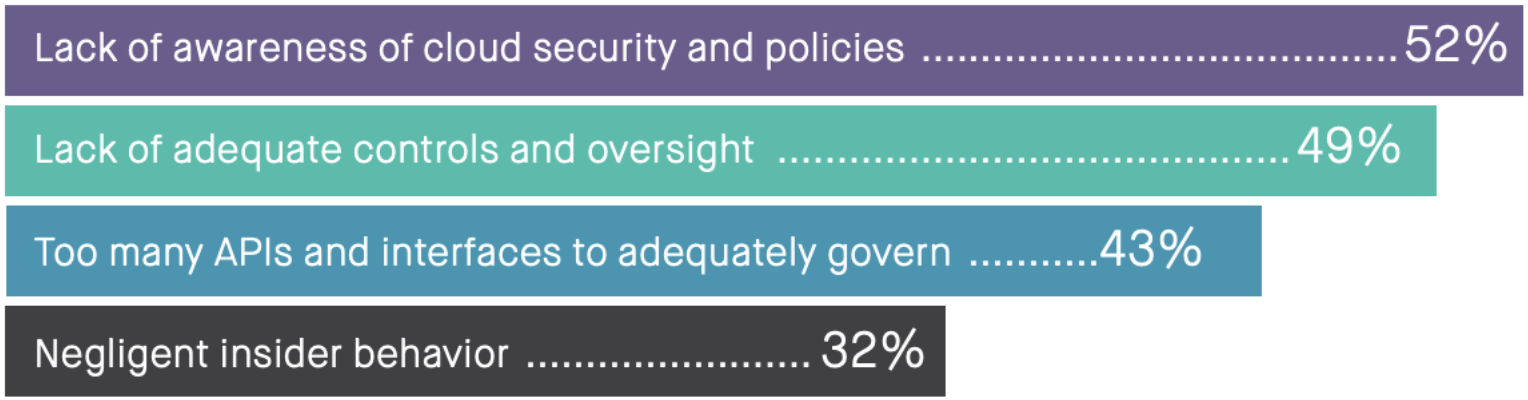
WORRIED THEY'RE VULNERABLE TO A CLOUD BREACH



MISCONFIGURATION RISK WILL STAY THE SAME OR INCREASE



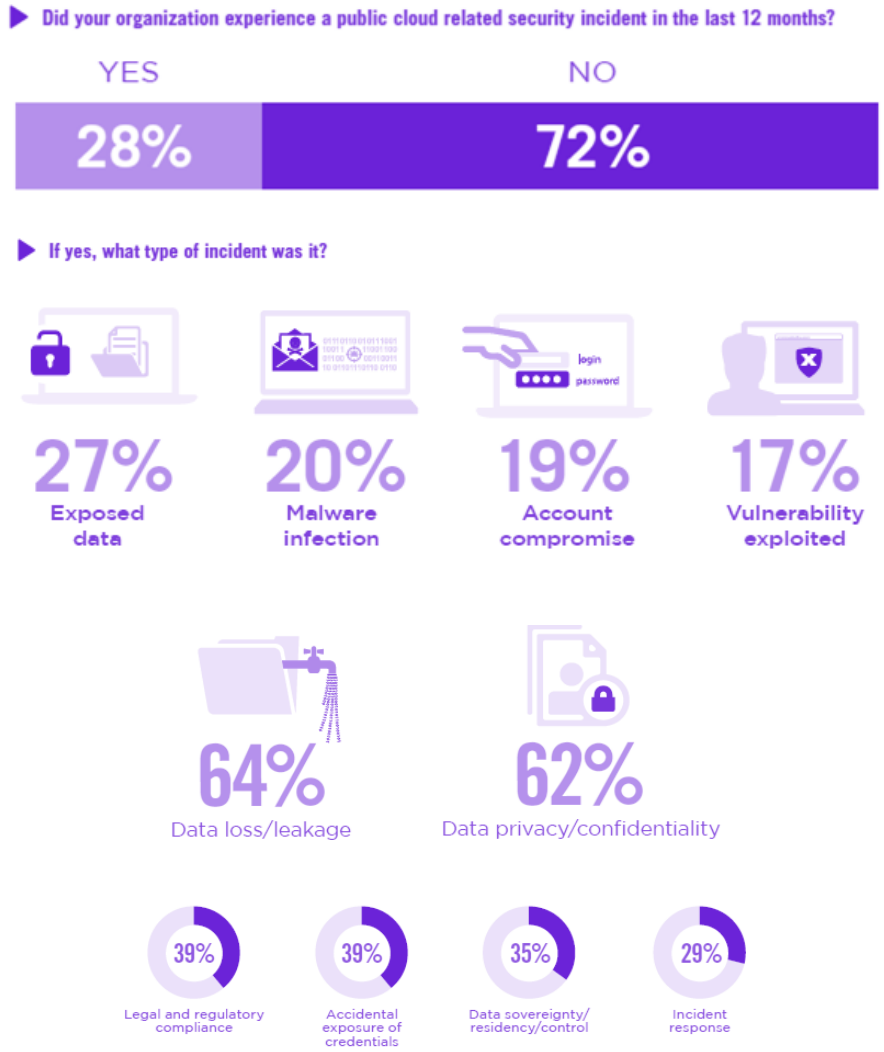
CAUSES OF CLOUD MISCONFIGURATION?



Softchoice

The Need for a Zero-Trust Solution

Consider the Facts



Consider the Solution

What is Zero Trust?

Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead **must** verify anything and everything trying to connect to its systems before granting access.

What issues are we trying to solve for our customers?

- Companies are **looking to adopt a mobile data and BYOD strategy** to ensure data is accessed through properly managed devices
- Our **customers do not have the resources to deploy the required security for data**, which can lead to catastrophic security risks within the organization
- Password changes, both manually and automatic in the event of a breach can be challenging to IT organizations

How can we utilize this strategy to help Softchoice?

- Utilizing this process ensures a standardized approach to security based on Zero-Trust concepts

Softchoice

Things to Know About Zero Trust Adoption

1. Organizations are ready to capitalize on Zero Trust strategy, accelerated by the move to a hybrid workplace and Covid-19.

2. Zero Trust strategy allows for flexibility in where organizations can begin implementing so the approach can be tailored to their needs

3. While Zero Trust strategy is widely adopted and improves organizations' ability to manage threats, there is still work to be done

4. Looking ahead, Zero Trust strategy will remain a top priority and require careful decision-making when it comes to employees and vendors

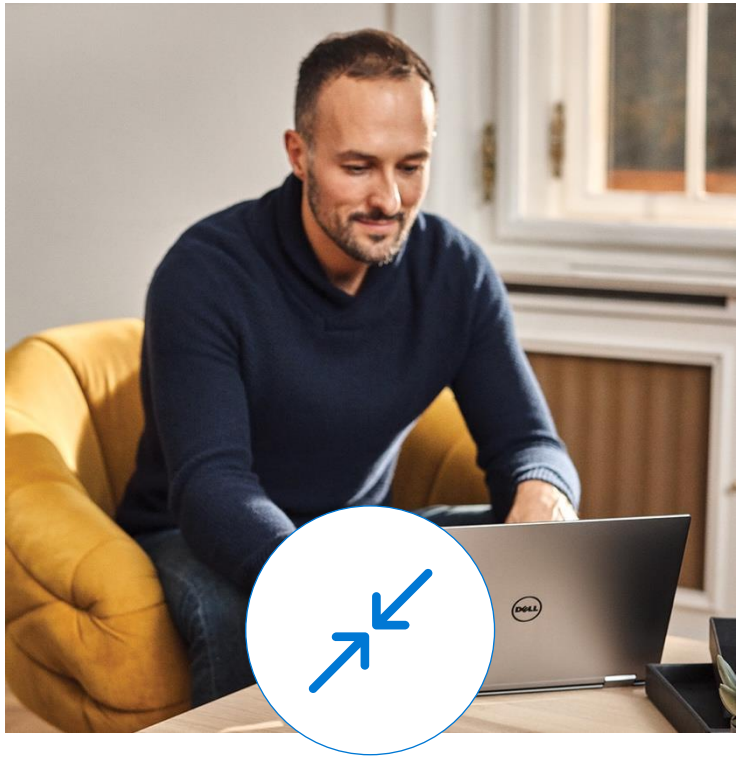
Old World vs. Current World

~~Users are employees~~		Employees, partners, customers, bots
~~Corporate managed devices~~		Bring your own devices and IoT
~~On-premises apps~~		Explosion of cloud apps
~~Monolithic apps~~		Composite apps & public restful APIs
~~Corp network and firewall~~		Expanding Perimeters
~~Local packet tracking and logs~~		Explosion of signal

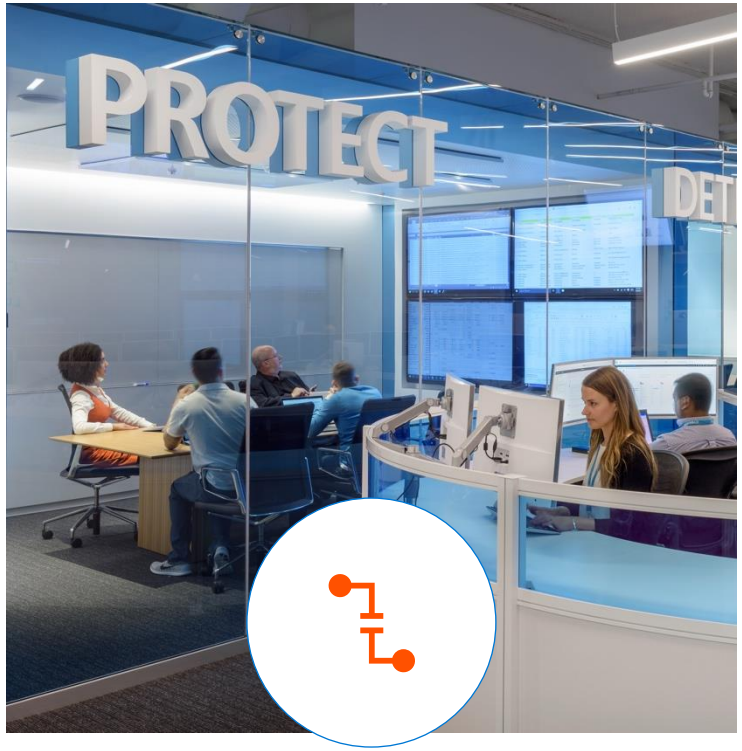
Softchoice

Zero Trust principles and holistic security strategy

Verify explicitly



Use least privilege access



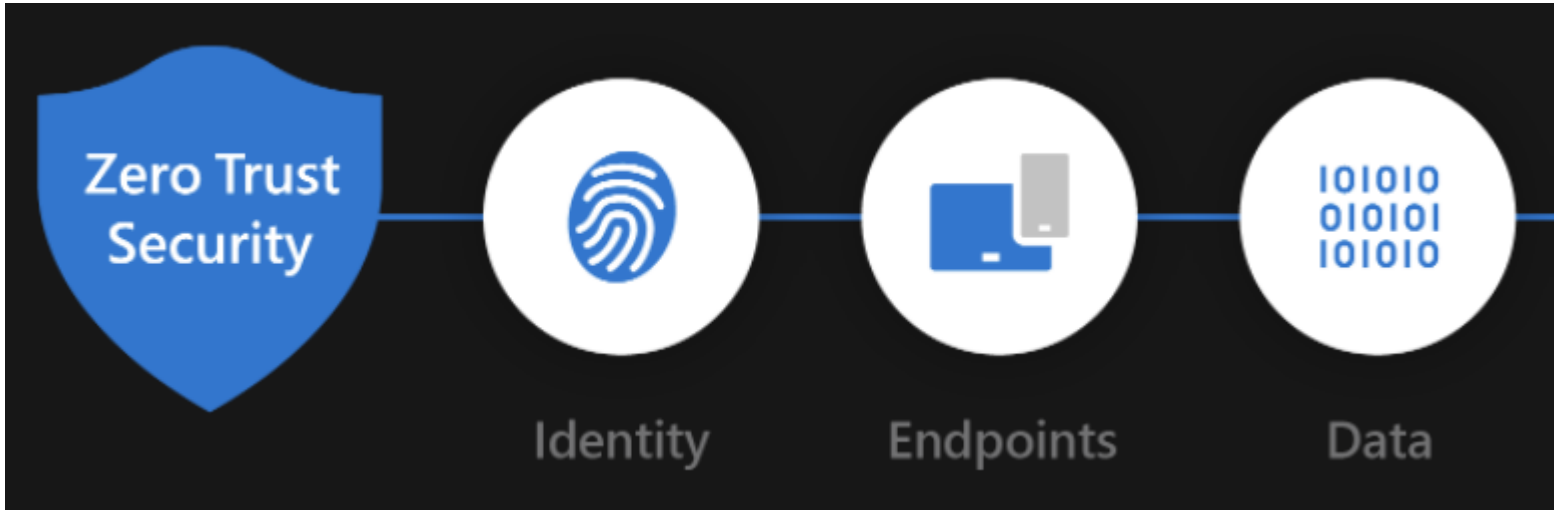
Assume breach

Softchoice

Softchoice Offerings: Overview

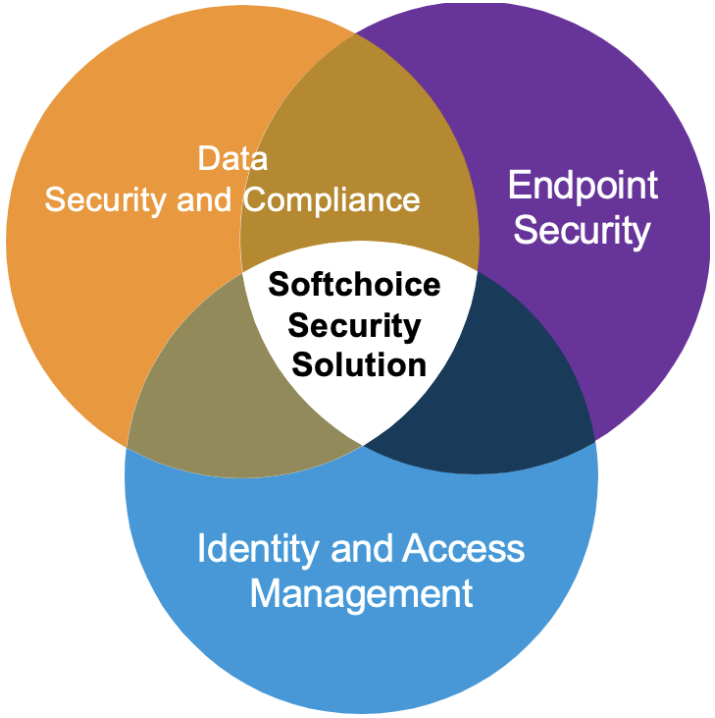
Softchoice Zero Trust Workplace Solution

The Softchoice Zero Trust Workplace Solution builds off the core concepts of Microsoft Workplace Zero Trust and provides the customer with a modular solution based on where they are on their security journey.
The key pillars for security exist with in Data and Compliance, Identity, and Device



Softchoice

Zero Trust Workplace Solution Overview & Direction



- **Zero Trust Workplace Solution** – This engagement provides security assessment workshops following the three pillars of security and access
    - **Data** – Encryption and protection of Intellectual Property and confidential documents within a customer's infrastructure
        - Azure Information Protection
        - Data Loss Prevention and Labeling
        - Microsoft Defender for Cloud Apps
    - **Endpoint** – Securing the endpoint is critical when deploying a security strategy. Deploying an enrollment mechanism ensures only approved devices access corporate data
        - Microsoft Endpoint Manager
        - Microsoft Defender for Endpoint
        - Microsoft Defender for Cloud Apps
    - **Identity** – Protection of the accounts accessing the corporate network is a key component of a customers overall security strategy
        - Azure Identity Protection
        - Microsoft Cloud App Security
        - Privileged Identity Management
        - Passwordless Identity Initiative
- **Microsoft Sentinel Advanced Configuration** – This module builds on the core functionality of Azure Sentinel demonstrated within the Advanced Security Accelerator
- **Cloud App Security Advanced Configuration** – This module integrates additional workflows to encompass network discovery and hardware monitoring to create restrictions based on customer need
- **Information Protection Advanced Configuration** – The AIP Advanced Configuration module expands the capabilities of AIP to include on premise and cloud documentation scanning. Configuration of this additional feature allows the customer to further identify and add classification to existing documentation.
- **Microsoft Defender for Cloud** – Provides additional configuration of the Defender stack to include tools from the Defender for Identity and Azure Security Center

Microsoft Defender for Endpoint

Softchoice

Zero Trust Workplace Solution – Breakdown

Microsoft Sentinel for Office 365

Data and Compliance

- **Discovery**
  - Discuss current security posture relating to data security – Secure Score Review/Discovery
- **Design**
  - Work with client to design and roadmap security capabilities for data
    - Microsoft Information Protection
      - DLP Policies
      - Sensitive Info Types
      - Retention/Labeling
      - On Premise Scanning
      - OME
- **Implementation**
  - Deployment of technologies and workflows defined in the security roadmap
- **Knowledge Transfer and Review**
  - Review with the client on the enable policies and placement in the overall data security roadmap developed in the Design section
- **Follow On**
  - ACM for Data Security
  - Softchoice Managed Office 365 offering

Endpoint Security

- **Discovery**
  - Review any MDM/MAM capabilities currently deployed within the environment and detail any advantages or restrictions – Secure Score Review/Discovery
- **Design**
  - Work with client to design and roadmap device requirements
    - Microsoft Endpoint Manager
      - Enrollment Process
      - Compliance Requirements
      - Application deployment
    - Defender for Endpoint
      - Attack Surface Reduction
      - Threat Analytics
      - Advanced Hunting
- **Implementation**
  - Deployment of technologies and workflows defined in the security roadmap
- **Knowledge Transfer and Review**
  - Review with the client the currently deployed device security infrastructure
- **Follow On**
  - Softchoice Managed Endpoint Service

Identity and Access Management

- **Discovery**
  - Discuss current identity management technologies and review the clients posture – Secure Score Review/Discovery
- **Design**
  - Work with client to design the identity security roadmap for implementation of the following workflows
    - Identity Components
      - Azure AD Connect
      - IDFix
    - Identity Restrictions
      - Conditional Access
    - Risk Based Identity
      - Login/User Risk
      - Integration of risk-based securities
- **Implementation**
  - Deployment of technologies and workflows defined in the security roadmap
- **Knowledge Transfer and Review**
  - Review with the client the current deployment of identity restrictions
- **Follow On**
  - ACM for Identity Management
  - Softchoice Managed Office 365 offering

Questions?

Softchoice

Thank you.

Comments or Suggestions

Abel E. Molina – Workplace Leader, Microsoft

Matthew Raida – Workplace Engineer, Microsoft

Softchoice