WHY ZERO TRUST SECURITY MATTERS FOR SMBs

According to NIST, "Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources. Zero Trust assumes there is no implicit trust granted." In simple terms, treat all networks as malicious and grant access only to verified users and devices.

Implementing Zero Trust Security within your business can help guard against data breaches, downtime, productivity loss, customer churn and reputational damage.

Over 70% of businesses planned deployment of Zero Trust in 2020 and it is even more important for SMBs in an era where workforces and networks are becoming increasingly distributed. [1]

COMMON MISCONCEPTIONS & TRUTHS

MISCONCEPTION #1:
Zero Trust Security is only for enterprises

TRUTH: The Zero Trust cybersecurity framework is a proven counter-threat strategy, and SMBs need to protect sensitive data and networks by taking measures to minimize internal and external vulnerabilities.

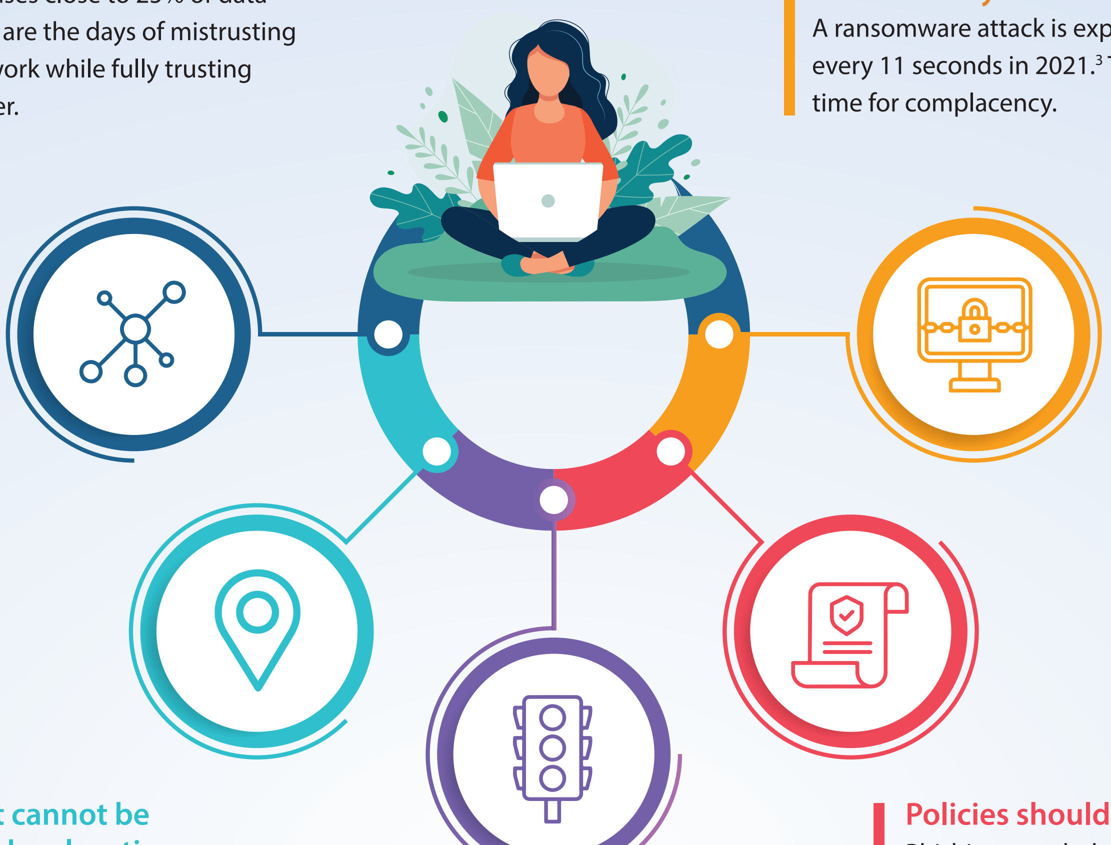
MISCONCEPTION #2:
It's too complex

TRUTH: By applying Zero Trust concepts at a scale that makes sense for your business, you'll realize it isn't as complex as you thought.

MISCONCEPTION #3:
The cost of implementing Zero Trust is too high

TRUTH: Focusing on your most critical applications and data sets first makes Zero Trust adoption operationally and economically feasible.

FIVE ZERO TRUST CYBERSECURITY ARCHITECTURE ASSUMPTIONS



The network is hostile.
Human error causes close to 25% of data breaches.[2] Gone are the days of mistrusting an external network while fully trusting even a single user.

External and internal network threats always exist.
A ransomware attack is expected to occur every 11 seconds in 2021.[3] This leaves no time for complacency.

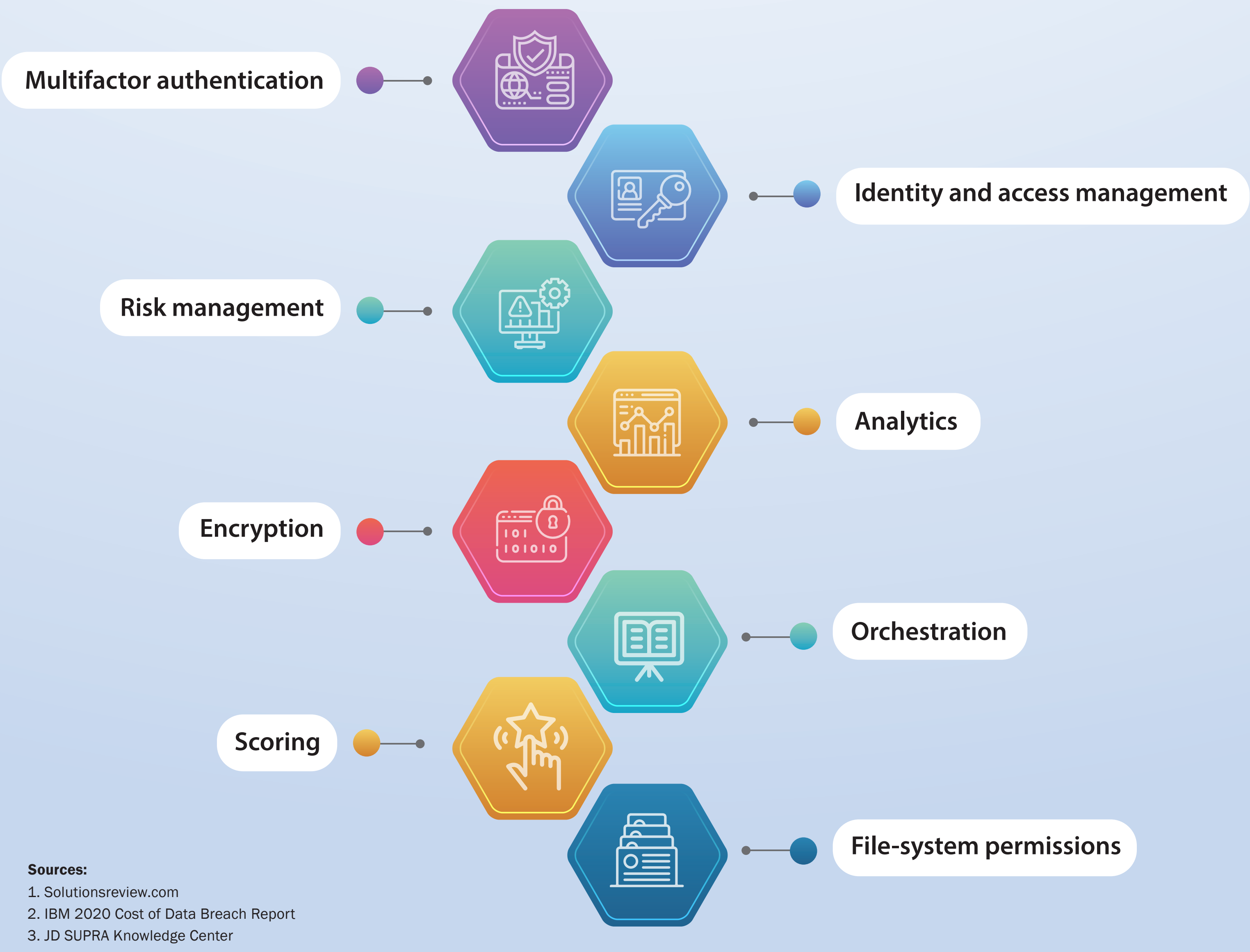
Network trust cannot be decided based on location.
With over 40% of employees expected to work-from-home post pandemic, a lot of devices, users and resources will interact entirely outside the corporate perimeter. [4] This significantly increases the probability of an incident.

All network traffic, users, and devices must be authenticated.
The Defense Information Systems Agency (DISA) recently decided to follow the "Never trust; always verify" approach to minimize opportunities for data exposure. [5]

Policies should be dynamic.
Phishing attacks have increased by over 60% since the pandemic started and to counter such an ever-evolving threat landscape, cybersecurity policies must be dynamic and adapt to address new concerns. [6]

THE TECHNOLOGIES BEHIND ZERO TRUST SECURITY

Zero Trust is built through governance policies—like giving users limited access sufficient to complete their tasks—and technologies such as:



- Multifactor authentication
- Identity and access management
- Risk management
- Analytics
- Encryption
- Orchestration
- Scoring
- File-system permissions

Sources:
1. Solutionsreview.com
2. IBM 2020 Cost of Data Breach Report
3. JD SUPRA Knowledge Center
4. Gartner Report
5. AFCEA
6. Security Magazine Verizon Data Breach Digest

TO LEARN MORE ABOUT HOW TO APPLY ZERO TRUST PRINCIPLES TO IMPROVE YOUR COMPANY'S CYBERSECURITY POSTURE,
CONTACT US NOW

RESTECH SOLUTIONS

Contact Us:
713-936-6855
info@restech.solutions
https://restech.solutions/contact