A good year to harden your security : @VMblog

David Marshall, VMblog.com

3 minutes

Industry executives and experts share their predictions for 2023. Read them in this 15th annual VMblog.com series exclusive.

By Richard Suls, Security & Risk Management Consultant, *WithSecure*

The coming year will see several distinct changes, both necessary and difficult. Organizations will need to continue to scramble to understand and remediate security gaps.

The Whitehouse has issued an order, requiring agencies and those doing business with the Fed to adopt a Zero Trust architecture by the end of 2024. We will see a greater understanding of Zero Trust and adoption of it across the country.

Multi-Factor Authentication will be under continued attack. It is my hope that text-message based MFA sees a drop in use, in favor of MFA with one-time numerical passcodes which requiring matching between MFA device and point-of-login. That is how to immediately stop MFA fatigue attack.

Nation-state actors will continue to dominate much of the offensive field in terms of major discoveries by researchers.

The percentage of ransomware will start to lose ground to exfiltration-based attacks. As criminal enterprises discover that they have even more leverage by stealing data, we can expect to see further spikes in this form of attack.

We will continue to see the larger tech companies absorb smaller security groups and, more importantly, their in-house tools.

Some technology that will be big this coming year include:

- Frameworks for security response within the cloud
- Forensic investigation software

Legal requirements will continue to be placed upon organizations that handle personally identifiable data.

This year herald's great opportunities for security improvements. Information security awareness and public support is at an all-time high. To truly succeed, a cyclical methodology of assessment and understanding, followed by remediation, and testing, should be adopted.

##

ABOUT THE AUTHOR

Richard Suls is a security researcher with over thirty years of experience. He is a qualified expert witness and prolific public speaker. As lead of WithSecure's Security and Risk Management group in the US, Richard delivers tabletops, design reviews, risk assessments and assists clients in charting courses to strengthen their security' posture.