INQUEST

DARKReading

How to Secure Your Weakest Link: Your Email

Hint: Your email provider can't do enough to protect you

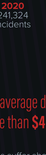
Most of us know that business email compromise (BEC) is a common vector for network attacks – but few realize just how vulnerable they are to threats.

The rapid transition to remote work during the pandemic has created massive new opportunities for security breaches. Employers often place their faith in their email provider to protect their scattered workforce.

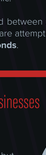
But InQuest's comprehensive experiment measuring email security efficacy demonstrates a significant gap in available protection. Neither Microsoft nor Google can do enough to stem the tide of threats.

Here's the bottom line: to protect the enterprise, you must augment your email security to close the gap.

1 94% of threats breach your environment via email



And these breaches aren't restricted to big players – 43% of breaches target small businesses.



24% of attacks result in ransomware.

But BEC covers many classes of threats: phishing, VIP impersonation, invoice fraud, crypto scams, account takeover attacks (ATO), and more.

2 Attacks have soared during the pandemic

According to the FBI, phishing rose by 110% from 2019 to 2020 – from 114,702 incidents to 241,324.

And most IT professionals have noticed – 54% of security leaders reported an increase in phishing attacks on their enterprise during the pandemic.

Ransomware attacks doubled between 2020 and 2021. It's estimated that a ransomware attempt is now made on a U.S. business **every 11 seconds**.

3 The average data breach now costs businesses more than $4 million

All enterprises suffer shockwaves from a major attack, but some never recover. An estimated 60% of small businesses are forced to shut down within six months of a breach.

$1.07 million in remote work breach costs

Remote work adds $1.07 million in breach costs on average -- compared to attacks where remote work was not involved.

$1.8 billion in compromise attack costs

Business email compromise attacks had a $1.8 billion cost to businesses in 2020.

$18 billion in ransomware & lost productivity costs

Globally, it's estimated that ransomware costs $18 billion - factoring in lost productivity.

4 How well does your email provider protect you from real-world emerging malware threats?

We set up an experiment to compare the biggest players: Google and Microsoft[1].

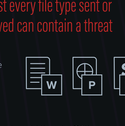
Step 1:

In 2021[2], we collected 221,160 real-world malicious attachments from the wild and sent them by email. Our findings:

- Google Suite missed 19% of incoming threats (42,590)

- Microsoft Office 365 missed 11% of incoming threats (24,300)

Google Suite Threats Missed by Month



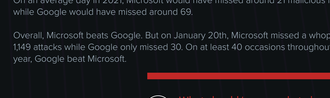
Microsoft Office 365 Threats Missed by Month

Step 2:

Further inspecting INCOMING malware that evaded at least one of the providers, we found a substantial number of UNIQUE threats:

- Google missed 21,771 unique threats
- Microsoft missed 6,702 unique threats

InQuest Email Security only missed 816 unique threats (an 8X-27X improvement)



[1] Data collected by InQuest's Trystero Project – an experiment designed to measure the security efficacy of the two largest mail providers, Google and Microsoft, as well as InQuest, against real-world emerging malware.
[2] Number of malware artifacts bypassed detection efforts for each provider between January and October 2021.

5 Almost every file type sent or received can contain a threat

Nearly half (48%) of malware used in phishing attacks comes through Office files.

In March 2022, InQuest harvested **585 evasive** real-world threats. Of these, **Microsoft missed 46%** and **Google missed 83%**. The most frequently abused file formats for embedding malware are Microsoft Word and Microsoft Excel.

6 No single provider is foolproof

So, who's the winner (blocked threats in an average week)? Neither. Results vary over time, but neither email provider provides sufficient protection.

Google VS Microsoft

GSuite Sent	GSuite Blocked	O365 Sent	O365 Blocked
27,839	27,318 (2)	27,839	17,012

O365+ Sent	O365+ Blocked	O365++ Sent	O365++ Blocked
27,839	27,304 (3)	27,839	27,338 (1)

On an average day in 2021, Microsoft would have missed around 21 malicious files, while Google would have missed around 69.

Overall, Microsoft beats Google. But on January 20th, Microsoft missed a whopping 1,149 attacks while Google only missed 30. On at least 40 occasions throughout the year, Google beat Microsoft.

7 What should/can you do to improve your email security?

Request an Email Attack Simulation

Get a fast and **free** Email Attack Simulation. Setup only takes minutes and is totally transparent (create one user with one forwarding rule).

Schedule a Briefing

Demo InQuest's Integrated Cloud Email Security (ICES) service to see how you can close critical security gaps.

References

- https://www.verizon.com/business/resources/executivebriefs/2019-dbir-executive-brief.pdf
- https://www.verizon.com/business/resources/executivebriefs/2019-dbir-executive-brief.pdf
- https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-a ccelerating-transformation-cyber-security/
- https://www.cisa.gov/
- https://www.ibm.com/security/data-breach
- https://www.verizon.com/business/resources/executivebriefs/2019-dbir-executive-brief.pdf
- https://www.ibm.com/security/data-breach
- https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/