GLASSWALL

CDR Insight

Cybersecurity Blindspots

The Need For Proactive Protection

glasswall.com

The Problem

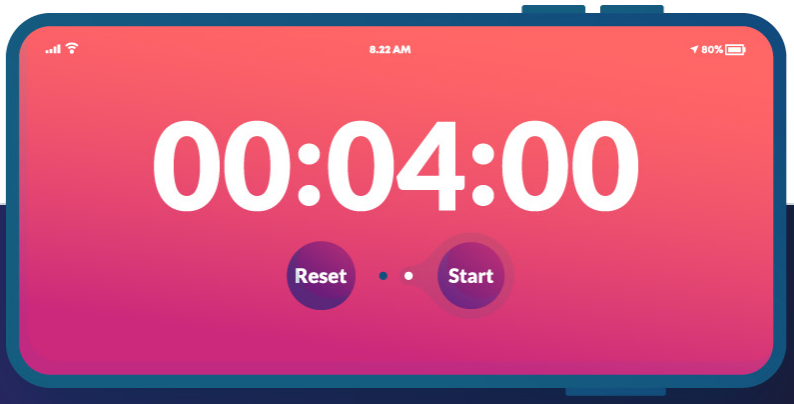
On average, cyber attacks occur every four seconds, with the impact of malware and ransomware alone now measured in trillions, estimated at $6 trillion per year, as a result of lost revenue, recovery costs and payments to cyber criminals.

From businesses of every type and size, to public sector bodies and critical infrastructure, it's now not a question of if they will be targeted, but when. As governments around the world act to improve levels of protection and legislate against cybercrime, it's more important than ever for every organization to take a proactive approach to their cybersecurity strategy.

The problem is, today's cyber criminals are confident, technical experts. Their success in identifying new vulnerabilities is only made easier by reactive security strategies and the blindspots this creates in millions of organizations.

The rise in ransomware attacks alone shows the sheer scale of the challenge:

- Ransomware attacks are soaring - up by 45% in April 2021 alone
- They now account for 69% of all malware attacks
- The average cost of a ransomware breach is over $4.5 million



Reactive Cybersecurity is failing - it's time for a better way.

Hybrid and Remote Working Bring

New Security Challenges

This is a huge problem under normal circumstances, but the last 18 months have seen a seismic shift to remote and hybrid working.

Despite the flexibility and advantages this has offered, it also broadens the level of cybersecurity risk for every organization that has digitally transformed its working practices.

As Microsoft CEO, Satya Nadella, put it back in April 2020, "We've seen two years' worth of digital transformation in two months."

As a result, cybercriminals were quick to exploit the widespread uncertainty and shift to remote working technologies. Recent research found that over half of senior IT professionals believe their employees have picked up bad cyber-security habits since working from home.

CISA CYBER+INFRASTRUCTURE

National Cyber Security Centre

> **"We've seen two years' worth of digital transformation in two months"**

Microsoft  CEO, Satya Nadella

The Rising Cost:
Ransomware Attacks in 2020

$5 million

Critical infrastructure provider, Colonial Pipeline, paid a $5 million ransom one day after the attack on its systems.

$600 million

The cost of the ransomware attack on the Irish health service is estimated at $600 million.

$75-$122 million

Hackers demanded $70 million from software firm, Kaseya, to decrypt crucial files.

Identifying Malware Blindspots:

A Reactive Response

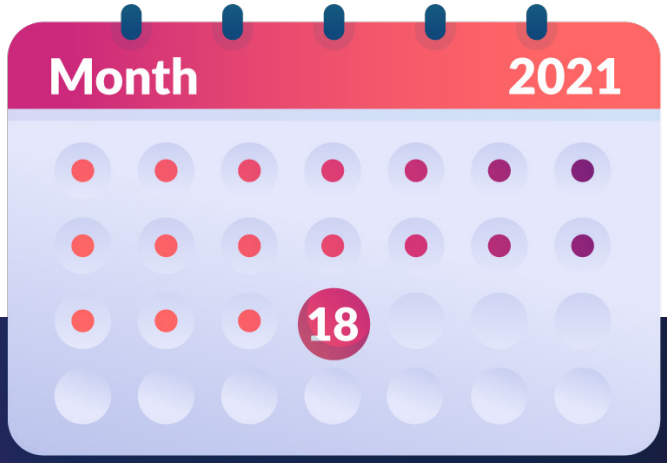
Most organizations understand the need to fend off malware and ransomware, with the vast majority relying on a reactive response based around well established antivirus and sandboxing technologies to protect their valuable files and everything they contain.

This is effective - but only up to a point. It's this emphasis on reactive technologies where conventional anti-malware and file protection strategies lead to cybersecurity blindspots.

For instance, nearly 70% of malware found embedded within files is of an unknown variant when it is received, effectively making it invisible to reactive cybersecurity technologies. That's a potentially catastrophic security blindspot, and with new malware variants appearing every few seconds and 450,000 new types of malware programmes identified daily, proactivity is now a 'must have' for any comprehensive security strategy.

The problem is, it can take days or even weeks for antivirus and sandboxing solutions to be updated so they can protect files and documents. Glasswall's own Threat Intelligence research has uncovered numerous examples of malware and ransomware sitting undetected on network infrastructure for anything up to 18 days before reactive solutions are able to respond.

For those whose antivirus and sandboxing defences are breached, the road to recovery is long and expensive. Research from IBM shows it takes an average of 280 days - that's roughly eight months to recover from a data breach.



Malware is sitting undetected on network infrastructure for up to 18 days

Proactive Protection - Closing Cybersecurity Blindspots

Glasswall takes a proactive approach to file based threats, and is a market leader in Content Disarm and Reconstruction (CDR) technology. Our dynamic approach to ransomware and malware identifies and removes risky, zero-day file-based threats from all files in moments - minimizing downtime and disruption often caused by traditional anti-virus or sandboxing solutions.

We intercept, scan and regenerate every file and document that comes in and out of your organisation to a safe standard of "known good".

Organizations that are 'Glasswalled' are always ahead of bad actors, whereas antivirus solutions are always, at best, one step behind.

The process requires no blocking, no patching, and with no false positives to hold back important business documents, meaning it delivers only safe, secure and trusted files.

The result? Every file sent or received - via email or the cloud - can be treated with confidence by organizations fully protected from zero-day malware threats.

> "...while sandboxing and almost all other techniques depend on detection of behaviors, CDR protects against exploits and weaponized content that have not been seen before."
>
> Gartner

GLASSWALL

Speak with one of our CDR experts:

UK: +44 203 814 3890
USA: +1 866823 6652

sales@glasswall.com
us.sales@glasswall.com

glasswall.com