Glasswall whitepaper

Uncovering The Real Threats

How Content Disarm and Reconstruction technology brings cyber-security to life

GLASSWALL

CONTENTS

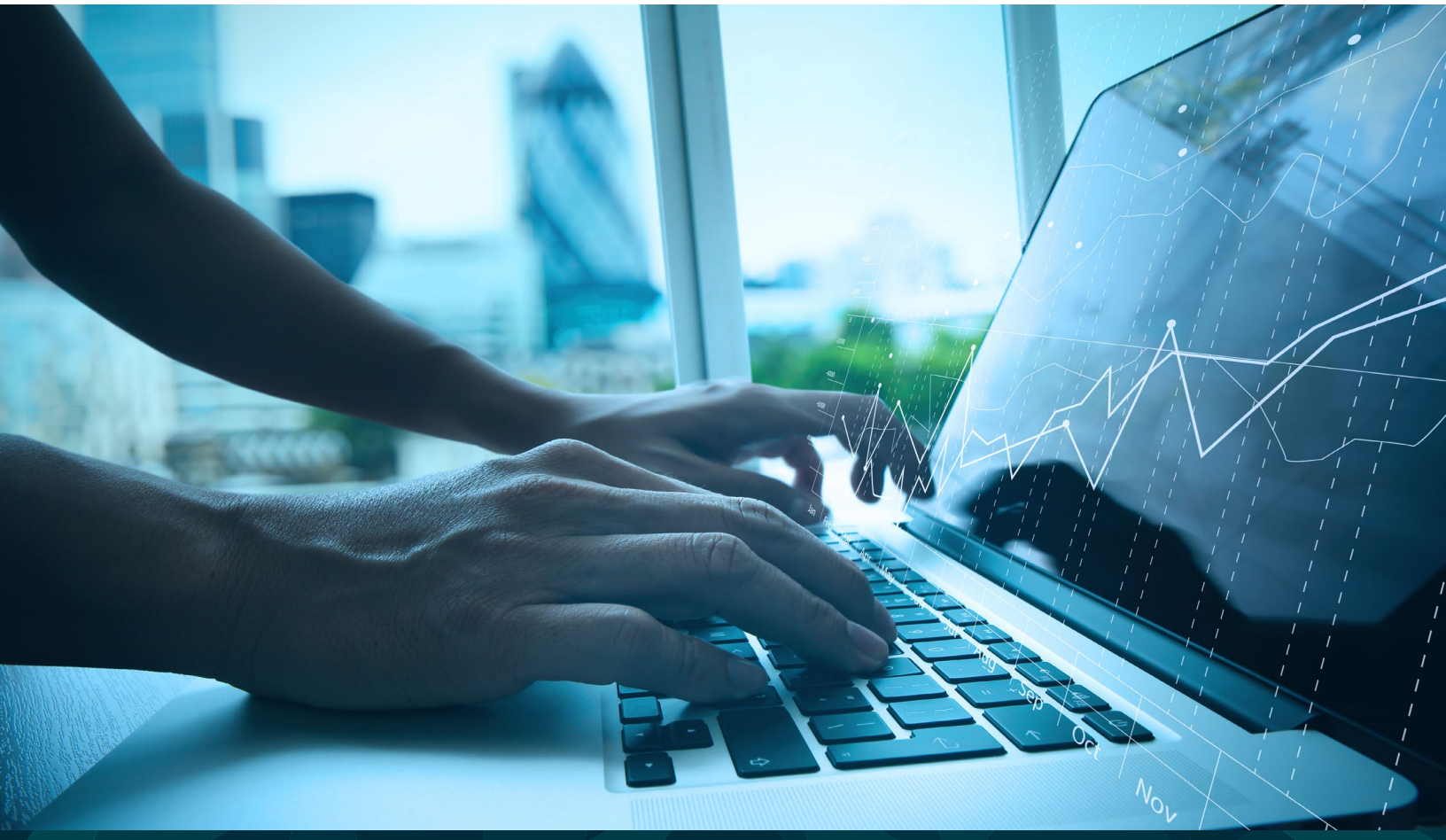
INTRODUCTION

Amid all the noise and hype generated by conventional cyber-security systems, most documents such as PDFs and Word files still remain a locked box for the majority of enterprises – hiding potentially malicious content deep inside.

These alterations to the structures of everyday files are now the biggest danger to the cyber-security of enterprises around the globe. Yet despite a better understanding of the growing scale of cyber-attacks, many enterprises remain vulnerable because the SIEM (Security Information Event and Management) systems that co-ordinate their digital security are unable to monitor or assess these fast-changing and hidden threats.

The result is that large organisations that receive thousands of email attachments every day are wide-open to attack by criminals who manipulate the structural vulnerabilities within PDFs, Word documents, Excel and PowerPoint files. A typical attack means that as soon as these attachments are opened, the malicious code in the structure will automatically contact a remote server and download malware which will either hold an organisation to ransom, siphon off highly sensitive data or empty bank accounts.

Now, however, is the time for enterprises and businesses to realise that they can protect themselves from such threats by integrating into their SIEM systems a stream of highly-detailed and unique analytics. This is achieved through adoption of file-regeneration technology, which although allied to what has become termed by Gartner as the Content Disarm and Reconstruction (CDR) approach, is more advanced, allowing an organisation to turn how it addresses security from ‘reactive looking for bad’ into ‘proactive looking for good’.



A NEW STANDARD OF PROTECTION

This proactive approach to security involves innovative technology that breaks down all files arriving as email attachments, conducts thousands of checks against the manufacturer's standard and then regenerates a clean, sanitised version in fractions of a second. A valuable stream of intelligence regarding the scale and nature of the risks to an enterprise comes from continuous analysis of document content and structure, allied to the technology's unique ability to recognise the slightest deviation from the manufacturer's standards.

These insights can be blended and correlated with all the evolving intelligence about known virus threats and for example Macros that flow from conventional AV solutions which by their nature, approach cyber-security from a different angle. By merging this information, organisations can build themselves a far more accurate and timely view of the threats they face, allowing them to take pre-emptive action to protect themselves, rather than only becoming aware of attacks when they are already underway or even worse – after data has been stolen.

1. Unknown or Malicious Documents

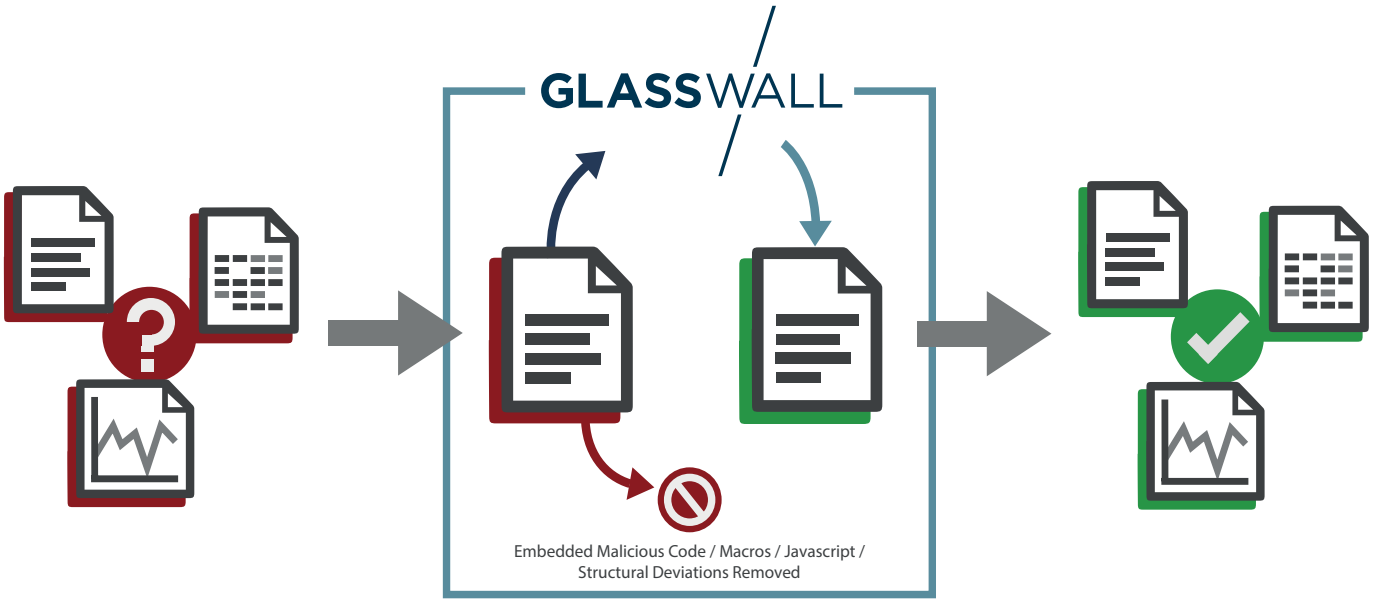
- Unknown
- Non-compliant
- Structural & functional risk
- Potentially malicious

2. Files Inspected and Regenerated

- Analyses and reports on files
- Applies policy to embedded and extensible items
- Signatureless, no updates

3. Only Clean, Usable and Benign Files Pass

- Disarmed scripts / macros / embedded threats
- Fully standardised files
- Original content untouched
- Real-time delivery



SPOTTING THE SUSPICIOUS

The first step towards achieving this new level of protection is to build a baseline from which suspicious deviations can be flagged up in alerts as part of a SIEM system. In simple terms, it may be, for example, that the baseline establishes that on an average day a business receives 100 common document-types containing Macros (code which automates a set of instructions). When the file regeneration technology's inspection analytics suddenly register that four times as many are being received in a single day – then the business is alerted to what may well be the precursor to an attack.

By the standards of today's sophisticated cyber-attacks, Macros are fairly mundane threats and their removal is relatively straightforward. Yet an increase in their occurrence may well indicate that a more serious attack is about to be mounted. Analysis by Glasswall is conclusive in establishing that alterations within the structures of files such as PDFs are now the most common vectors for attacks on businesses. Yet stopping these highly potent threats at the door demands more than conventional AV or standard CDR approaches. It requires deep file inspection technology that regenerates sanitised files that are safe to use in fractions of a second.

Nonetheless, by alerting itself to surges in suspicious activity, an organisation can step up and focus its defences on structural threats as well as Macros in a proactive manner instead of waiting for the signature of the attack to be recognised, by which time the damage may have been done.

Integrating with the Enterprise SIEM system through standard syslog protocol, analytics from CDR solutions add another dimension to conventional defences which concentrate on the detection of malicious code in JavaScript, Macros, extensible and embedded files along with monitoring unusual log-on attempts or suspicious outbound flows of emails. Once combined, this information can be used to create a far more accurate picture of what is actually happening now, as opposed to what occurred several hours ago.

Bespoke metrics can then be created using the expertise of the file-regeneration technology provider, so that the enterprise can decide what it wants to monitor and measure and how that information should be blended with existing indicators of compromise.

A NEW WINDOW ON RISK

This ability to narrow the focus of monitoring to what actively poses a threat here and now brings many gains, not least in cutting through all the noise. One of the common complaints about SIEM systems is that they generate too much information or 'noise', making it difficult for a large enterprise to see where the threats are coming from in sufficient time to prevent them doing any damage. CDR solutions and especially file-regeneration technology, however, find the needles within this vast haystack of information and provide accurate and timely alerts to the SIEM feed, making it substantially more effective.

Whereas conventional AV defences rely on picking up viruses and malware such as Dridex that have already been identified, file-regeneration technology will stop these malicious exploits at the door and provide intelligence about them. This is a technology so far ahead of traditional approaches that it is now common for it to detect and prevent exploits and threats that six or seven days later have still not been given a signature by the established virus-scanning organisations.

A key point here is to understand that this advance on CDR technology is not a brick wall that prevents an enterprise from working by stopping dead every document with a slight structural malformation or blocking all files containing Macros. Approximately 97 per cent of all PDFs do not conform to the standard set by their manufacturers, while Macros are quite legitimately used every day of the year.

It is here that the experience of file-regeneration vendors counts, since they can use their analytics to determine which are major or minor problems or potential threats. The analytics from the technology establish what is normal and also what constitutes an acceptable level of risk.

In this way, files with minor structural malformations that are not a risk can be repaired in fractions of a second and then delivered within the organisation in full confidence. The metrics governing the process can be adjusted in accordance with what is safe and what the organisation requires, giving it full control over the use of files and documents and enabling it to work to its own tolerance of risk.

The accounts department, for instance, will probably need to receive Excel files containing Macros from known sources. Yet in allowing this to happen, policy can be calibrated so that what is suspiciously anomalous will not make it through in an unsanitised, dangerous condition.

RIGHT SIZING OF RESOURCES

The integrated use of file-regeneration technology within a SIEM system also brings real benefits in resource-deployment across the whole security estate. It enables an organisation to right-size its sandboxing solutions since it is only the files that potentially pose a risk which require testing and examination. Instead of conducting tests on every email attachment, it is only necessary to examine the two or three per cent highlighted as being of high risk.

An enterprise with many supply chain partners, for example, will have many invoices and purchase orders going back and forth in emails. Yet very rarely will these documents include Macros. When Macros do start appearing, however, the enterprise can focus its resources on this area. It means the organisation is not burdened with a blanket approach that costs more money than is necessary and which slows down operations right across the enterprise. Files deemed suspicious can be stopped dead and sent for further analysis to reveal the nature and evolution of threats.

CONCLUSION

The deployment of file-sanitisation and regeneration solutions, therefore, gives enterprises far greater protection against the ever-changing nature of cyber-attacks, whether the criminals are deploying Macros or are part of the growing number using malware within the structures of documents.

The huge benefits of integrating these advances with CDR into an enterprise's defences are immediately obtainable, especially for an organisation with a large supply chain and many partners. The interplay of this technology with the indicators of compromise generated by traditional approaches allows an enterprise to view the entirety of the threats it faces before they have any effect. It can then concentrate its resources where they really count, delivering far greater security against threats identified in real time, and yielding a very substantial return-on-investment.

No document can now be considered safe without deep file-inspection full sanitisation and regeneration of only the "known good".

GLASSWALL

CONTACT US FOR A FREE TRIAL

UK: +44 (0) 203 814 3900
USA: +1 (866) 823 6652

info@glasswallsolutions.com
www.glasswallsolutions.com