WHITEPAPER

RISING TO THE NEW SECURITY CHALLENGE

BUILDING AN OUTSIDE-IN, INSIDE-OUT SECURITY STRATEGY

Data Integration

CONTENTS

EXECUTIVE SUMMARY

OVERVIEW

Changes in working practices, the demand for ubiquitous connectivity, the proliferation of 'smart' mobile devices, bandwidth hungry applications and access to anytime, anywhere services are all having a huge and fundamental impact on the way that organisations operate and conduct business. Providing secure communication and protecting data are amongst the biggest challenges that service providers, network operators and organisations face globally on a daily basis. Cyber threats have become increasingly sophisticated and the need for preventative rather than reactive measures has never been more important, particularly in light of the attacks and security breaches in the news recently.

How are today's cyber threats any different from those of the past? Two key aspects have changed – the type and source of the threats. Modern cyber threats are more likely to be at the application rather than network layer and they sometimes originate, unknowingly or deliberately, from the inside of organisations as well from the outside. The 'new challenge' is not only to more effectively combat external attacks but also to protect against internal threats from personnel who may inadvertently be harbouring and spreading malicious code to collect and transmit sensitive information to the outside.

Organisations are, rightly, still focusing a lot of effort on preventing externally sourced attacks. External sources account for 80% of attempted security attacks whilst 20% are initiated internally using exploitation techniques such as phishing, spyware and the propagation of Trojans.

As well as this, in recent findings it revealed 32.5%[1] of the respondents stated that their boards receive no regular report on cyber security and only 35%[2] of organisations plan an increase in cyber security spending.

It is extremely difficult to strike the right balance between allowing users to take advantage of the plethora of collaborative applications and restricting access to the detriment of productivity. However, once the outer security perimeter has been breached, these internal threats are very difficult to control using only traditional, outward looking security solutions.

Modern, more advanced security solutions are able to identify and monitor individual users and application traffic streams, and to apply fine-grained policies to control content and application traffic from multiple outside as well as inside sources. In parallel, these security solutions have the capability to carry out traffic pattern analysis, to use heuristics to deconstruct, identify and delete malicious code and to dynamically learn and adjust their behaviour according to permitted, 'good' traffic characteristics.

In the increasingly complex world of security threats and solutions, security and network managers are constantly striving to keep abreast of new technology developments whilst, at the same time, trying to manage limited budgets.

This whitepaper outlines some of the key considerations for organisations to develop a rounded security strategy and the benefits of adopting an 'outside-in', 'inside-out' approach to protect their business.

" External sources account for 80% of attempted security attacks whilst 20% are initiated internally using exploitation techniques such as phishing, spy ware and the propagation of Trojans."

KEY CONSIDERATIONS

COVERING ALL ANGLES

Several factors mandate the need for organisations to change the way in which they protect their business. In this section, we take a look at these factors and subsequently outline how to build a security strategy to address them.

ADVANCED MALWARE

Usually distributed via email and almost impossible to detect with conventional security methods, advanced malware uses the Internet as the distribution channel and effectively evades signature based antivirus scanning. Once through the barriers, malware can cause immense damage by not only disrupting business activities but also appropriating and transmitting sensitive information to third parties. Malware is mostly activated by users opening email attachments or by downloading and running unauthorised applications on their machines. It can persist undetected for weeks or even months. The business ramifications can be significant and clean-up costs are rarely budgeted for in advance. Re-imaging every machine is extremely time consuming and costly.

REGULATION AND COMPLIANCE

As the list of compliance requirements gets longer and regulatory controls strengthen, most businesses, regardless of size, market sector or global location, are affected in some way – either by law or best-practice. Examples of well-known regulatory and compliance requirements include:

- PCI-DSS - Protecting consumers, banks and businesses from fraudulent card use
- FSA (Financial Services Authority) - Regulating the financial services industry in the UK
- Basel 2/3 (financial control) - Recommendations on banking laws and regulations

In addition, broader compliance around standard data protection is often overlooked. In all cases, if non-compliance is proven, businesses face not only a financial penalty but also potential damage to reputation; often irrevocable.

Every company that takes online card payments needs to be PCI DSS compliant.

SOCIAL NETWORKING

With the rising use of Facebook, Twitter, LinkedIn and other social networks, business' concern for security and privacy safeguards gains even more importance.

Organisations need clear Internet usage policies. Blocking all access to social networking sites can have a negative impact on hiring personnel, maintaining staff morale and launching important marketing initiatives. The higher education sector is a prime example. Universities often attract students by offering flexible access to social networks and subject matter sites and applications. This flexibility need not be a risk if the right user-based security solution is in place to monitor and control access.

APPLICATION CONTROL AND VISIBILITY

The monitoring and control of protocols, such as FTP and P2P file sharing (e.g Limewire, Isohunt, Megaupload and BitTorrent) is crucial. Applications such as WebEx, IM and remote diagnostic & control software, can circumvent explicit block policies by using HTTP/S over TCP ports 80 and 443 as a transport mechanism, making them look like any other permissible web traffic.

The relationship between certain protocols and their well-known TCP ports is no longer a reliable means of enforcing policy.

> " With the rise in malware and social networking capabilities, regulations and compliances, are all the more important to ensure minimal business risk."

Known as 'port hopping', there are many instances of applications using alternative ports when the well-known ports are blocked (e.g. Skype). The new security challenge entails dealing with these applications, many of which are developed by reputable companies who, nevertheless, design their applications to deliberately get through conventional security defences.

In addition to protocols, unauthorised items such as executable files, drivers, Java apps, ActiveX controls and scripts all add to the security challenge that organisations face. Many traditional firewalls allow these applications through undetected to execute on users' machines.

MOBILE DEVICES

In addition to laptops, smartphones and tablets have become everyday business tools. Many organisations rely on mobility for their remote homeworkers, travelling workforce and business partners. Bring Your Own Device (BYOD) has also gained momentum in recent years with personnel using their own devices instead of a company-issued PC. Locking-down PCs used to be the norm. It has now become almost pointless and security policies must accommodate the new challenge of permitting BYOD connections, together with whatever applications may be running on them.

Another consequent risk of BYOD is that personnel access, download and store potentially sensitive information on their devices, which they can easily take beyond the organisations' security boundary. Indeed, this is often essential for workers who are constantly on the move. There is no technology that can prevent this from happening but an enforced data encryption policy will reduce the risk of information getting into the wrong hands if BYOD devices are lost or stolen.

Centralised, cloud-based services are available to allow an organisation to monitor and control SIM-based mobile endpoints but many organisations do not use them due to their complexity and device management overheads.

DATA LOSS PREVENTION (DLP)

In addition to preventing unsolicited application data and malware from entering an organisation, it is vital to ensure that personnel do not upload or publish unauthorised information via social media, blog posts, forums or other social channels. Posting sensitive information can adversely impact not only a company but also its customers. News travels fast, bad news travels even faster. Inadvertently or deliberately leaking pre-public domain financial information can affect a company's share price and, ultimately, its value.

Another consideration for DLP is the loss, theft or improper disposal of data repositories, such as fixed and portable hard disks and memory sticks. Programmes to carry out numerous iterations of disk information scrubbing are freely available.

> " As more of everyday business relies on mobile devices, mobility is a necessity to many organisations."

MEETING THE NEW SECURITY CHALLENGE

WHAT'S EXPECTED

Data Integration takes a holistic approach to help organisations to develop and implement their security strategy and policies – combined, of course, with best-of-breed technologies and security design best practices. It is imperative to not only focus on the 'outside-in' but also the 'inside-out'. An organisation's greatest asset is its people. With the right balance of flexibility and control, Data Integration can assist you to empower your personnel to participate in, and contribute positively towards, the implementation of successful security measures.

OUTSIDE-IN

User and application policy management is essential at all levels. Stateful firewalls that rely exclusively on IP, protocol and port information are out-dated and no longer offers sufficient protection against today more sophisticated threats.

Key considerations when building an 'outside in' security strategy:

- Application visibility and control - The majority of security threats today are targeted at the application rather than network layer. The 'bad guys' use fewer brute force attacks these days relying instead on the persistent and gradual acquisition of information from unsuspecting employees. It is necessary to identify and monitor the applications being used and who is using them. Deploying technology that is able to analyse traffic behaviour, identify protocol anomalies and remove potentially harmful code is essential.
- Malware detection – Whilst signature-based scanning is still important, script and sandbox-based code analysis are important tools in the anti-threat arsenal. Integrated, real-time analysis is essential for web, email and protocol traffic - particularly suspect protocols such as IM and P2P.

INSIDE-OUT

Scalable user-ID based User / Network Access Control (UAC/NAC) enables:

- BYOD (Bring Your Own Device) and mobility security – Traditional web filtering techniques that reside on the gateway are not sufficient. Inside-out filtering and real-time visibility of personal mobility devices allows the application of custom policies to control per-device and per-user resource access and usage.
- Guest access – Guest registration allows the application of flexible guest policies to restrict or permit the appropriate level of access. Post connection monitoring is important to gauge the effectiveness of the policy and to what extent non-organisational users may be attempting to breach security.
- Endpoint compliance – An automatically loaded, automatically updated anti-virus / malware detection engine coupled with the use of a host compliance checker to ensure that the end stations meets standard requirements for connectivity. For example, that the machine belongs to the correct domain, that the anti-virus engine is loaded and running.
- Threat prevention – Real-time identification and disconnection of any rogue devices that have connected to the network thereby reducing the risk of malicious code propagation within the internal network.
- Integration with security management & reporting systems – The ability to manage the security policies centrally across a number of disparate platforms in geographically dispersed locations. The ability to collect and collate information to report on real-time and historical events for analysis.

> " With the right balance, a business can empower & control successful security measures."

OTHER CONSIDERATIONS

WHAT ELSE YOU SHOULD KNOW?

THREAT PREVENTION

Many of today's sophisticated cyber threats are embedded in common protocols and attempt to exhibit application-like behaviour in order to avoid protocol non-compliance detection. A combination of signature checks, traffic behaviour analysis and sand-box code analysis / execution (heuristics) are the main ways in which to combat these attacks.

DNS CLOUD SECURITY

DNS service attacks are extremely high-impact and are on the rise. Multiple, repeated DNS lookups from distributed locations is a form of Distributed Denial of Service (DDoS) attack that can generate large amounts of traffic to/from DNS servers eventually disabling them. Malware can also poison DNS caches causing total DNS failure or illegitimate entries to be inserted compromising the validity of legitimate domain to IP address mappings.

SECURING THE CLOUD

Cloud, Infrastructure as a Service (IaaS) and Software as a Service (SaaS) providers are especially focused on protecting the data of their clients, particularly during a time when multi-tenant data centres may contain zettabytes of data. The providers face an extremely difficult task striking the right balance between implementing tight security and providing sufficient flexibility so as not to adversely impact their customers' productivity.

Virtualisation in large data centres poses a whole new challenge. Virtual machines within the same IaaS or SaaS environment may need to be protected from each other let alone from virtual machines that belong to other environments, as well as access from the outside world. This is normally accomplished using virtual security devices, which most of today's best-in-breed security vendors provide.

> " With a host of best-in-class vendor solutions, each address and protect against some of the major IT security concerns currently existing in today's business landscape."

CONCLUSION

IN SUMMARY

Older traditional security technologies are no longer sufficient to protect organisations from the plethora of new and more sophisticated cyber threats, nor can they cater for the increased demand for applications and services or the changes in today's working behaviours.

Next generation security, UAC/NAC and management systems are being implemented today to address the main challenges posed by threats such as advanced malware, the need for regulatory compliance, improved user / application control and visibility, the increase in user mobility and data loss prevention.

Large IaaS, SaaS and hybrid data centres are commonplace around the world. Virtualisation of security systems and their integration with networking equipment and management platforms is a key component of these environments. The Network Functions Virtualisation working group (part of ETSI) is currently in the process of defining standards for virtual systems to interface to one another, and to provisioning, management and orchestration systems.

Security design best practices underpin the successful deployment of security solutions in every network. Design best practices go beyond the implementation of the right and most cost effective technology to looking at how best to integrate that technology within the entire network, including the DNS infrastructure and, if necessary, development of APIs to the OSS/BSS platforms.

Is your network ready for the new security challenge? Contact us today to discuss your IT Security.

" Successful design, deployment and best practices for IT Security in every business will not only protect against threats but also provide many cost efficiencies & technological advancements."

REFERENCES:

[1] The Boardroom Cyber Watch Survey 2014

[2] UK Cyber Security Standards Research Report 2013 by PWC and Department for Business Innovation & Skills

ABOUT DATA INTEGRATION

Data Integration specialise in managed networks, security services, mobility solutions and high performance hosting solutions, delivering scalable and optimal bandwidth applications over a secure and high performance network infrastructure.

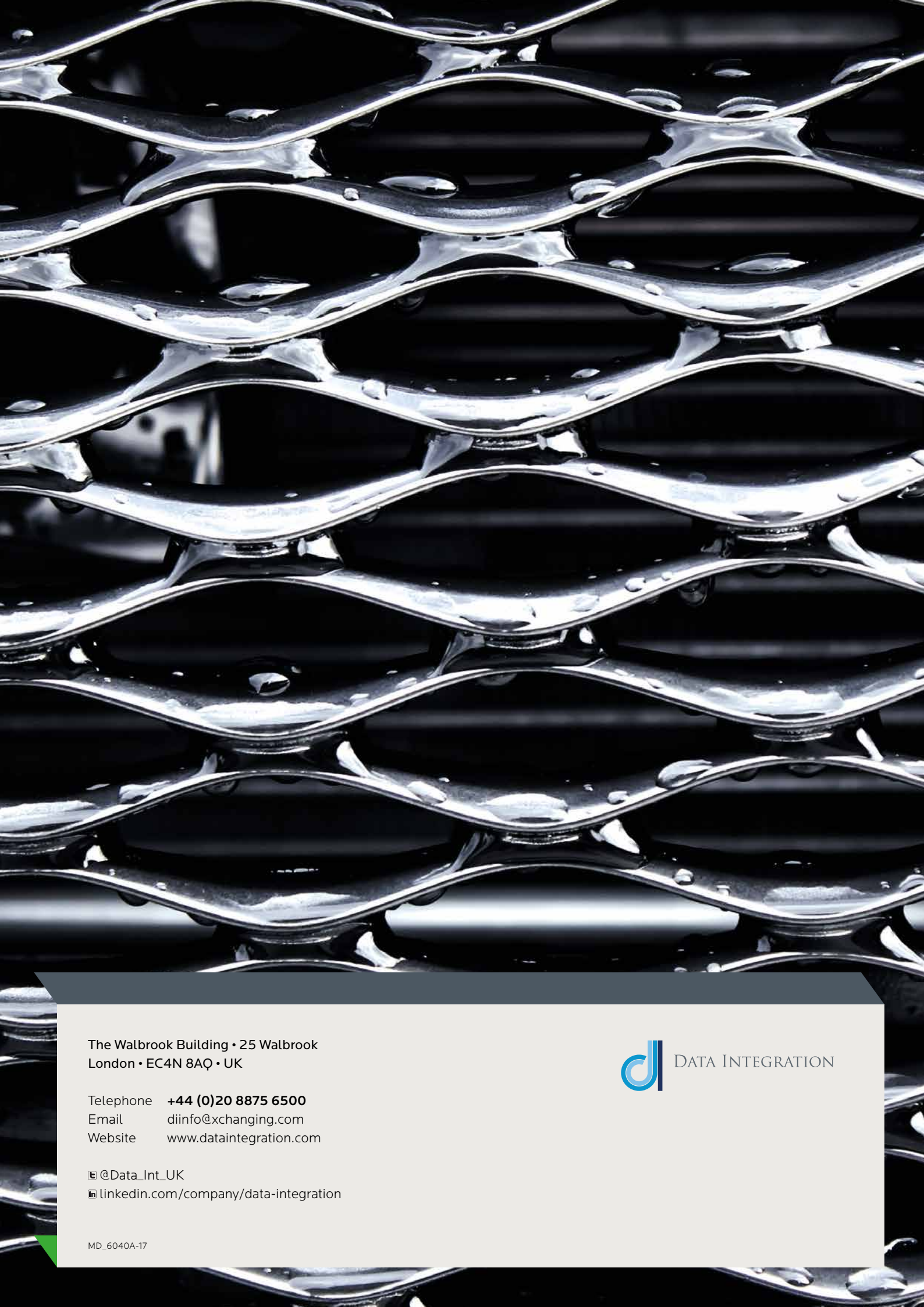
With over 15 years' experience, Data Integration work with the leading product technology vendors to design, implement and manage networks for its customers to add value to their organisation, meet business demands and protect against networking threats.

With its end-to-end intelligent solutions, Data Integration has designed and managed networks for over 300 leading organisations in a variety of sectors which also includes Education, Insurance, Finance and the Public Sector.

Data Integration plays an important role in supporting its customer through business changes and challenges by providing a fully scalable and flexible infrastructure for complete security protection, visibility and control of their network.

Data Integration was acquired by Computer Sciences Corporation (CSC) in 2016 and is now part of their Cyber Security business.

For more information on Data Integration, please visit www.dataintegration.com



The Walbrook Building • 25 Walbrook
London • EC4N 8AQ • UK

Telephone **+44 (0)20 8875 6500**
Email diinfo@xchanging.com
Website www.dataintegration.com

@Data_Int_UK
linkedin.com/company/data-integration

DATA INTEGRATION

MD_6040A-17