SYSTAL
TECHNOLOGY SOLUTIONS

From Complexity to Clarity: IT security in an ever-changing landscape

By John Bidgood, CTO Systal

Enterprise IT infrastructures today have been developing rapidly over recent years and becoming increasingly complex. Cloud computing, the Internet of Things (IoT), mobile internet access and more, have vastly increased the applications and endpoints run on typical organisational infrastructures – and the speed at which they can be provisioned.

It logically follows that all this dynamism and complexity engenders new challenges when it comes to protecting those infrastructures. The more complex and fast-moving your IT environment becomes, the harder it is to deliver comprehensive IT security across all corners of that environment.

Modern enterprise security, then, depends on the ability to cut through that complexity and make the network clear and easy to understand. It depends on getting to grips with the vast volume of devices, the multitude of traffic flows and the rapid pace of change experienced by enterprise networks today. In this article, we explore three of the key challenges facing IT security teams today amidst this landscape of complexity – and how they can best turn that complexity into clarity.

Challenge 1: decreased visibility

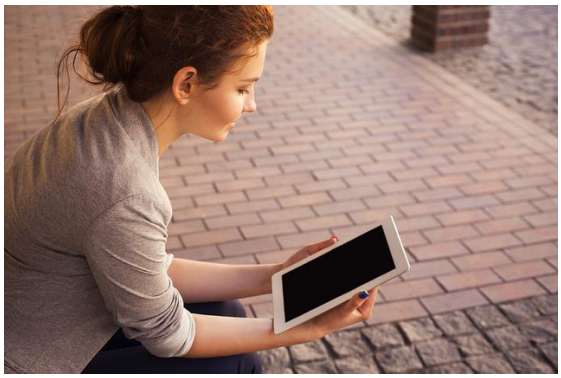
IT security begins with an understanding of what you are trying to protect. Which servers, databases, applications and devices exist within your IT infrastructure? How are they connected to each other? How is your data flowing and residing?

This is complicated enough when your entire infrastructure is hosted on-premise and managed by your internal IT team; when some of your infrastructure and applications are migrated out to the cloud it can become even more complicated.

Cloud computing brings massive business benefits in terms of agility, scalability and flexibility, and it enables small organisations to take advantage of the same sophisticated applications as larger businesses in a cost-effective way. However, it moves elements of your infrastructure off-premise, generating new security challenges in terms of visibility and control.

Challenge 2: increased endpoints

The Internet of Things (IoT) is, quite rightly, one of the hottest enterprise IT concepts of the moment. Deploy IoT devices throughout your organisation and you can gather previously untapped data, generate new business intelligence and ultimately drive powerful efficiencies and even the development of new products and services.



However, every connected device, no matter how small or simple it is on its own, is also a brand-new endpoint to be added to your infrastructure. Once, the endpoints within an organisation simply consisted of the computers and phones that staff were issued with – there might just be a few dozen in a small organisation. Now, that same small organisation can easily have a list of hundreds or even thousands of endpoints, thanks to IoT sensors, GPS trackers and so on. Every one of these has a potential to be a vulnerability with in your network for a malicious attacker to exploit– which means every one of them needs protecting and managing. This is no small task.

Challenge 3: rapidly evolving threats

Looking beyond each business's own IT infrastructure, it is important to consider the broader cyber threat landscape which organisations need to protect themselves against. Unfortunately, like enterprise IT itself, this is a world which has developed dramatically in sophistication in recent years – and it is still evolving.

Today's cyber threats are multifaceted, difficult to identify, tailored to the target organisation, and often use social engineering techniques. All it takes is for a single employee to click on a compromised link or download an infected attachment and insidious malware can get inside the organisation – often undetected. On top of this, regulations like GDPR mean that organisations across all sectors face ever stricter requirements to identify and report cyber incidents as soon as possible after they occur.

The answer: A multi-layered approach

When new IoT devices are being provisioned daily, when mobile devices are being taken off-premise and used to access the corporate system from remote locations, when public and private cloud environments are being used to deploy key business applications – the overall picture is multifaceted and multi-layered. This means, then, that a multi-layered approach to security is the only option.

What does this look like in practice? First, security needs to work at the network, the individual device and the application layer in order to provide comprehensive protection. Typically, this means deploying a range of different tools and technologies, rather than a single off-the-shelf solution.

Second, enterprise security needs to draw on intelligence from a wide range of technical sources – as well as first-hand human experience. Information on the threats faced by other organisations – as well as the threats successfully fended off by your organisation – needs to be harnessed and fed into your security systems, so that they learn from themselves and continually improve.

Third, enterprise security needs to work on both a proactive and a reactive basis.

Proactive IT security is focused on identifying and neutralising threats before they impact the business infrastructure. Threats need to be intelligently identified, filtered out and blocked. Applications, devices, and operating systems should be patched and upgraded whenever necessary to ensure they are always working at optimal levels of security. Staff training and development are also key elements in proactive IT security, ensuring that your employees are aware of the threats you face and know how to recognise the most obvious signs of social engineering.

Reactive IT security, on the other hand, focuses on rapid isolation and remediation of any threats that do make it into your network. Incident response and disaster recovery processes are key – you need to know how to report and escalate incidents, and recover key data and applications should the worst happen. Again, staff awareness and training are vital.

The role of managed services

Perhaps this sounds no less dynamic and complex than the enterprise IT landscape we laid out at the start? This is why for many organisations, a managed services approach to IT security is the ideal solution. It allows businesses to draw on a broader set of skills, experience and national or international intelligence than they might be able to achieve alone, through a combination of device management, automated security analysis and the added value of analyst-enriched insight. In other words, a layer of automated threat detection and analysis, backed by our relationships with the world's leading technology vendors, is supported by intelligent human insight, building on data gathered from years of experience in managed security. This enables you to focus on running your business, and be assured security is in safe hands.

SYSTAL_
TECHNOLOGY SOLUTIONS

About Systal Technology Solutions

Systal Technology Solutions is an IT Services Integrator. We help our customers optimise IT to maximise the value of Technology by advising on IT strategy, deploying, and integrating appropriate technologies, and managing elements of their infrastructure on their behalf.

At every stage, we help our customers minimise the cost and maximise the business value of their IT expenditure.

We have experience delivering globally across a wide range of industry sectors. Our people strive to deliver excellent customer service, to exceed expectations and consistently go that extra mile.

www.systal.co.uk
enquiries@systal.co.uk
0330 159 3800