The Age of Security First

Computers have always been designed to communicate. The earliest idea for the Internet, or the so-called ‘Galactic Computer Network’ back in 1963, was formed on the foundation of a network to share information.

In those days, a hacker was more commonly known as a government spy and despite early Military application, networks were only used for non-classified communication. Security might have been more of a concern if they could have foreseen the widespread and pervasive use of computing today - in every aspect of our daily lives.

We are entering an age of Security first. A more complex, zero-trust landscape where secure access to data and networks is the primary concern. Where the value associated with our information increases as it becomes more desirable to others. Where Security Operations teams are having to work hard to prove ROI and establish board-level trust in their capability to protect the organisation from risk.
Show me it’s working!

Signs are that the market is moving away from contingency planning, in the event of an incident, towards a world where executives demand day-to-day clarity on how the business is delivering on security. If executive teams continually lose sight of the risks involved, then perhaps a lack of reporting is to blame? Ultimately, management want to see operational details about Security controls – before a breach occurs.

“A 2019 survey by the Enterprise Strategy Group* showed that 39% of executives and directors want security status reports for cyber-risk, associated with end-to-end business processes and 35% want better detail on the ROI, of their security investments and planned purchases.”

 Clearly, more could be done to bridge the gap between technical capabilities and management perception. Security first isn't about just adding a box with flashing lights into the corner of the server room; it's about addressing security requirements all the way through the technology stack. Alarmingy, research is showing that not all customers have the in-house skills and budget to prioritise Security over other business challenges.

Security-as-a-Service is here.

You can't protect what you're unable to see or afford to manage. As we engage with more customers, the Marathon team are starting to see real parallels between Security and Outsourcing, as a model. Using a third party for IT services became popular in the 1980's, as the cost of hiring and training internal staff to work on non-essential projects was recognised as a good way to save money. In later years, as the size and complexity of their networks and systems increased, customers turned again to outsourcing services as a way of also shifting risk and management overheads.

Around 34% of data breaches in 2019* involved an employee of the business. Insider threats are more common-place and companies are asking themselves if managing their own security is the safest option.

“Security-as-a-Service has now emerged as a viable option, with customers looking for a multi-layered approach to managing risk. One which is designed to protect an organisations information and data, against all types of common cyber-attacks and threats.”

Paul Hepburn Marathon Professional Services

Whilst data loss from inside a business represents a significant risk, threats now extend far beyond the network perimeter and the task of managing security can be a burden for many customers - even those with a SOC. Social engineered trojans, phishing, Denial of Service, advanced persistent threats, Ransomware, Network traveling worms, unpatched software - the list grows longer in time and attacks grow more sophisticated.


*Source: Infosecurity Magazine 2019|Blogs|Three cybersecurity essentials your board of Directors want to know

marathon-ps.com 020 8329 1000
The Future. Today.

Security first isn’t something for the future – it’s here today! As we transition to this new era, an industry-wide approach to security-by-design and services is required, to meet these technical, operational and financial challenges. Let’s take a look at what this means, in practical terms, for customers looking to transform their security and the benefits of achieving this through a services approach.
Are we ready for Security-by-design?

If we could start again, it would make sense to put Security at the heart of our design. We would have probably asked more questions about challenges faced with sharing sensitive data; or built these systems on the basis of Security First.

As much as you might want to, you don’t always have the remit to rip out a complete infrastructure and start again! Today's security solutions need to integrate and wrap around the legacy systems and applications that the business relies upon.

As security professionals navigate these issues, they've also seen the boundaries between inside and outside the network disappear, with applications and data moved across internal and external networks – and back again!

This question, of where the network ends and the internet begins provides a new opportunity for Security to bounce its way to the top of the Cloud agenda.

On-premise security solutions require customers to make purchases based on anticipated demand, whereas cloud-based security allows the business to scale services up and down based on their actual consumption.

Which option would you prefer?

Proactive – Detective – Reactive.

Multi-layered protection provides control over your defences in three core directions:

1. **Proactive**: Being able to look out for risks in advance and generate intelligence that can be used within the business, to reduce the impact of security events on operations. Often includes tools for network discovery, Security Automation and Artificial Intelligence, amongst others.

2. **Detective**: The constant monitoring of user access, threats and systems for Security management. Traditionally, delivered through single-use tools on the front-line of defences for the organisation. Usefulness sometimes constrained by its ability to identify new threats.

3. **Reactive**: What happens after a breach or data loss. Involves a combination of technology and business processes to understand and share publicly what happened, recover lost data or systems and get the business up and running again – all as quickly as possible.

Executive teams may not know what sort of management control and visibility they need over their Security. Many will be led by the legislation and industry regulations they need to comply with - in some cases at the expense of day-to-day operational risk! Executives, ultimately, need control over how their security is performing for the business. The recent situation at Norsk Hydro, where the business is having to rebuild many of its production systems following a breach, is a stark reminder that operational risk cannot be ignored.

marathon-ps.com  020 8329 1000
Are customers ready to hand over the keys?

“Why get bogged down in ownership, when you can subscribe to life!”
7 Hot XaaS Stats – Marathon Professional Services

With Everything as a Service, or XaaS, gaining so much traction, there is a definite feel in the air that security for licensed software, on-premise only hardware and localised networks will be a thing of the past.

A study from research firm Deloitte*, indicates that 43% of XaaS customers see data security and privacy as their number one concern. How do they protect valuable infrastructure and applications, whilst maintaining control and visibility...? Security must be delivered in the same way!

What triggers a move from internally managed security to Security-as-a-Service? Another study from Deloitte* has shown a distinct gap between the type of solution security professionals would prefer and the reality of what they can afford or deliver. For those that haven't suffered a major breach [yet], complexity and cost can have a massive impact on budget and management buy-in.

As we begin to build the picture of what Security First can deliver for the organisation, the thought of managing multiple tools, applications and systems will undoubtably be a cause for concern. At the same time, Professional Services suppliers have hit the ground running: with the expertise, experience and structure to provide these services at scale.

The OneSecure Service from Marathon provides clients with a single solution to address all of the business risks associated with information and data. The package enables a fully managed secure business environment, removing the need for clients to invest in multiple products and licenses across numerous security technologies.

“Marathon have built a modular service so that clients can invest in the security components that fit their business and budgets. Simply choose a monthly subscription, with no other up-front costs.”
Peter Speck – Marathon Professional Services

Marathon took their experience and knowledge of Information Security and Data Protection, to bring together best of breed security tools within a single service framework. Combining key elements of the Proactive, Detective and Reactive information security protection components, which underpin a Security First strategy.


marathon-ps.com  020 8329 1000
**What next:**

The Security market has come a long way in such a short space of time. The evidence is there to suggest a strong parallel with outsourcing and how the market for Security-as-a-Service will grow. As the value of digital information grows, the risk and complexity of protecting it will continue to be a challenge for many.

Talk to the team for more information about the range of Professional Services available from Marathon. Alternatively, check out the Marathon website and blogs, for the latest market trends and an up-to-date view of what industry analysts are saying about Security-as-a-Service.