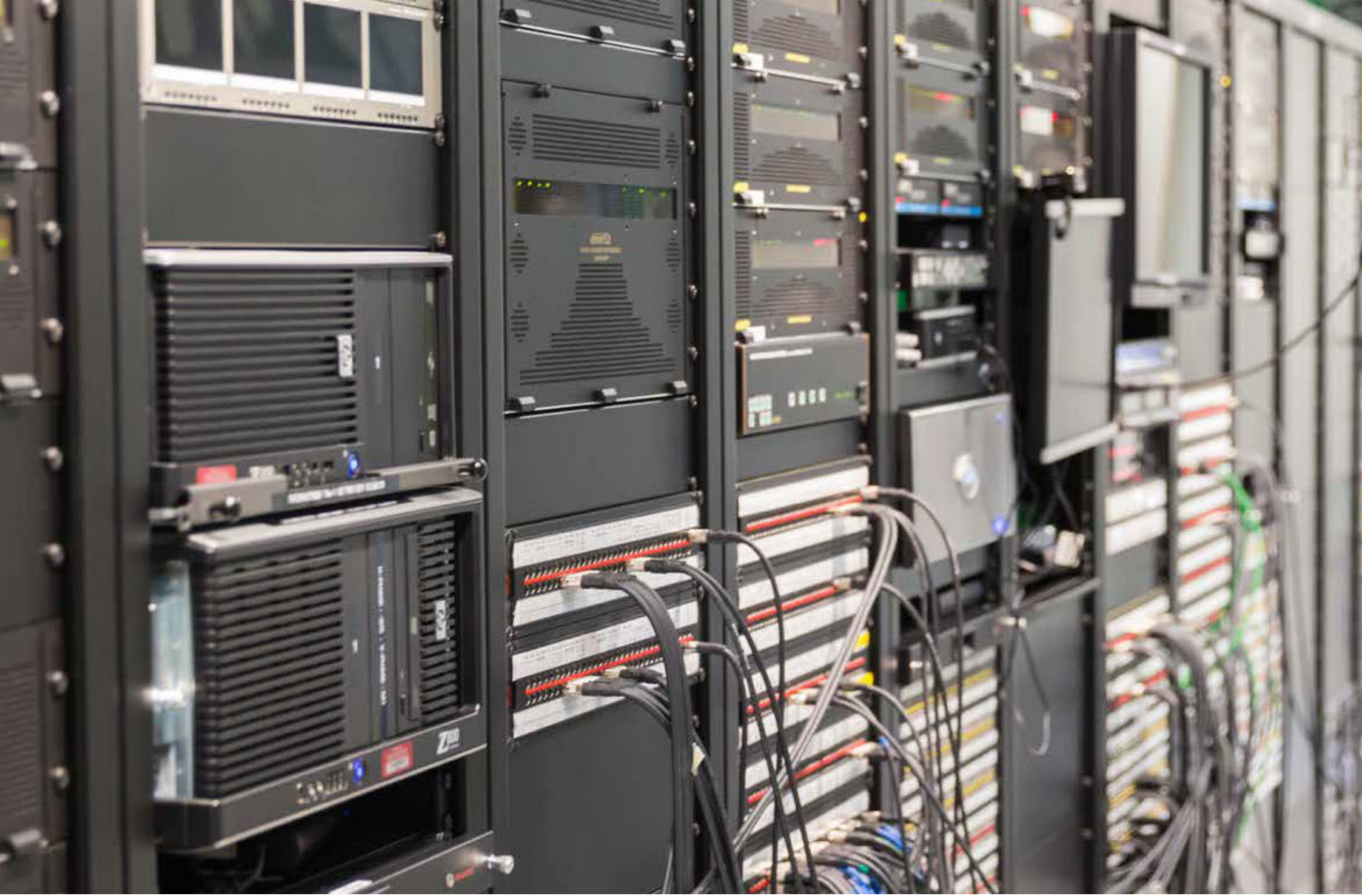
Symantec

Describing a blueprint for a bundled set of security capabilities / January 2018

Security in a box
A blueprint for cloud security architecture

pwc

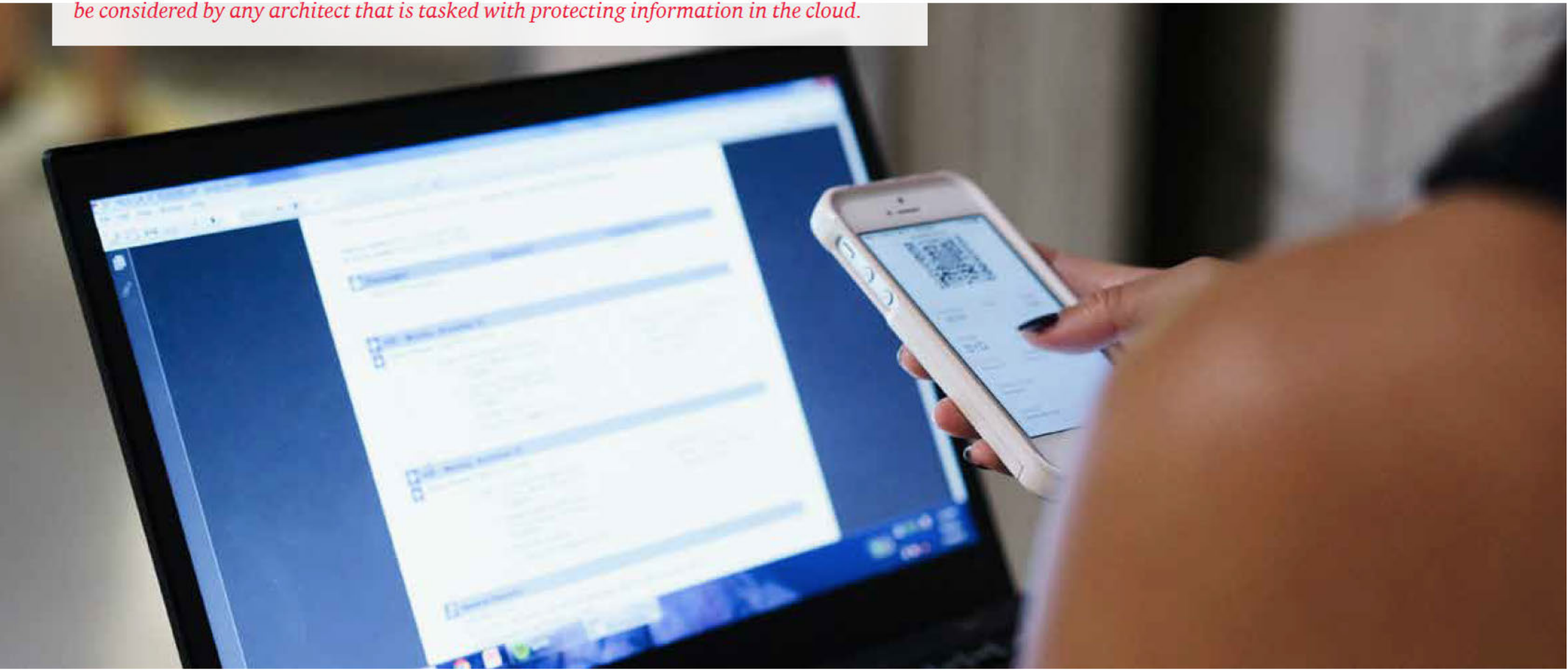
www.pwc.co.uk



Contents

Abstract

Imagine what security could be if not constrained by a large technology debt accumulated over the years of running legacy systems and applications. What if security capabilities can be procured as a black box service when you need it, as soon as you need it? This paper talks about how common security challenges can be solved in new ways. The services described are based on solutions and propositions that are available right now and should be considered by any architect that is tasked with protecting information in the cloud.

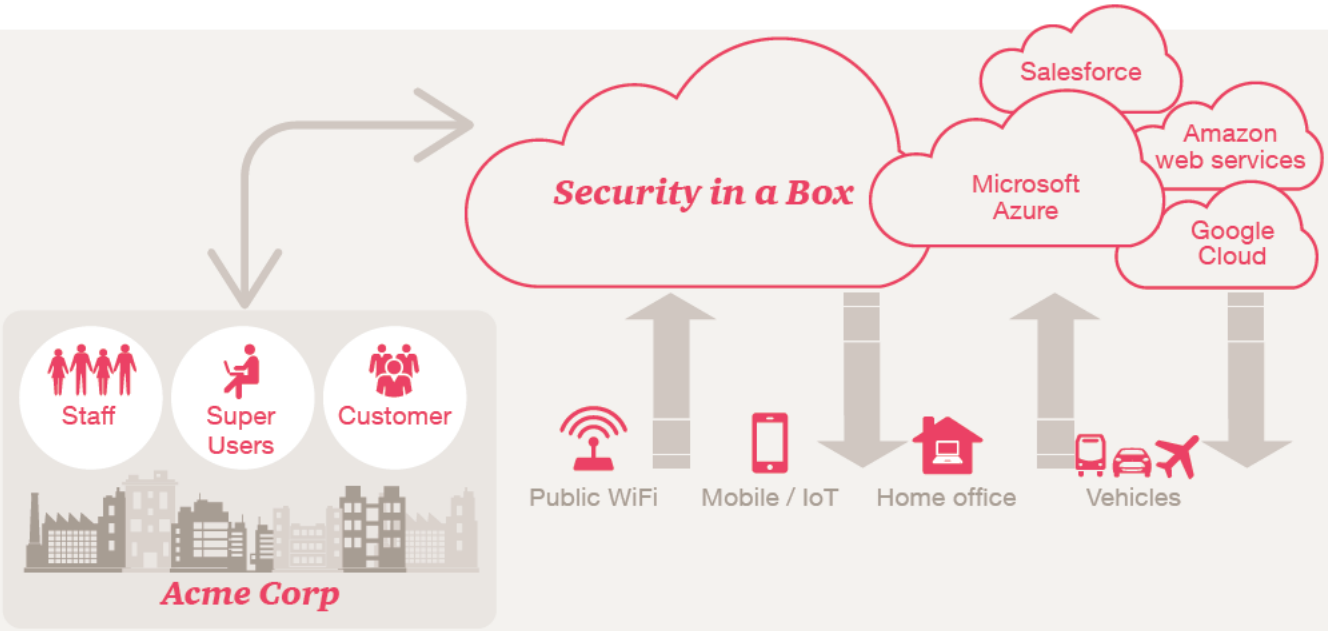


Introduction

Intended Audience: This paper is intended for all those responsible for securing cloud environments, be it a technology-centric company such as Netflix or Uber with "Cloud Native" environments or "Cloud Evolved" organisations that are extending their legacy environments to the cloud.

In today's technology-driven world, there are a number of emerging macro trends that are re-defining the way organisations consume technology. These macro trends include

- **The adoption of digital services** to improve customer engagement and service.
- **The execution of "cloud first"** strategies to improve the total cost of ownership of Information Technology.
- **The promotion of a "sharing economy"**, through principles such as PSD2 and Open Banking regulations.



These trends are also shifting the technology architecture thinking from an arms-length, closed off position to an open and collaborative one and driving:

- the use of APIs to facilitate sharing of information or various other digital transactions between organisations
- the migration of business critical systems into third party managed cloud environments
- the adoption of agile development methodologies (i.e. DevOps) to improve the speed of innovation and time to market.

To adapt to these changes, Security leaders need to re-evaluate the way they design and build their cyber security capabilities. Reliance on traditional waterfall-based delivery of data-centre focused controls won't be sufficient to secure the fast-paced collaborative business.

The new way of thinking about Security Services

This article seeks to advise how security professionals may adapt security delivery models to support these trends and ensure businesses can maintain trust in a digital society, through deploying 'a box' of security capabilities.

The solution is a set of scalable, flexible, automated, cloud based security utility services using security APIs, which can easily be commissioned and decommissioned based on the specific needs of an organisation, creating a "box of security capabilities" that can be customised at will. In order words, **"security in a box"**.

Common security challenges

We have met with many clients to discuss the problems they face as an organisation. Whilst the challenges they list include things like zero-day vulnerabilities, organisation culture and protection of distributed and mobile workforces, many historical challenges remain. Below we have listed the most prevalent ones:

1. Patch Management
2. Poor standardisation of security services
3. Overlapping compliance efforts
4. Measuring the wrong things
5. False sense of third/fourth party security
6. Retaining control over data
7. Optimal Logging
8. Access recertification
9. Tooling-based security strategies

1. Patch management

Patch management is a critical process in minimising the exposure of an enterprise to vulnerabilities in their information technology systems.

However, due to the volume of patches, multiple technologies, manual effort required to deploy certain patches, and rigorous operational testing requirements, it is easy for an organisation to become overwhelmed by the volume of patches to be applied.

Combined with the need for service downtime at a time convenient for the business, it is possible for organisations to quickly fall behind the curve. The net result being organisation's systems becoming dangerously out of date with the latest security updates and thus exposed to vulnerabilities.

2. Poor standardisation of security services

The cyber security market, populated by a range of big name brands, is constantly evolving with the latest technologies and is in a perpetual state of change.

As organisations begin to adopt various solutions, and have bespoke applications and tools developed independently by different vendors, security architects are quickly getting overloaded by the sheer number of products that don't integrate with each other and hence require armies of analysts to digest, mine and correlate the information from various sources.

Safeguarding organisational data in a fragmented environment can be a further challenge when the disparate systems do not integrate with security tooling, and multiple products are supported by an array of vendors, each interacting with differing levels of organisational data and with differing levels of system access.

If organisations are unable to obtain meaningful data from the disparate systems, it stands to reason they are likely making decisions that do not derive optimal value for the business.

3. Overlapping compliance efforts

A typical mid-size organisation has to go through 3-5 security audits a year. These could be part of financial integrity compliance, regulatory attestation or client's assurance request. Each audit requires the production of a set of evidence that must then be review with an auditor to put into context. Whilst heavily regulated industries like Financial Services suffer the most, a retail organisation could spend millions on PCI DSS and ISO27001 audits.

The problem lies in the fact that most of the questions in any security audit are the same. What might change slightly is the scope and the depth of the question. Due to different internal stakeholders that don't communicate between themselves, 1st line control operations people are asked to provide the same materials and describe the same documents over and over again which burns a lot of time and places a strain on people who are already busy with their day-jobs.

4. Misinterpretation of metrics

With the multiple reports of corporate breaches in the media that were initiated with a phishing mail, and the constant phishing campaigns launched by a variety of threat actors; the threat of an employee being phished is at the top of nearly every CISO's mind.

A result of this is the execution of continuous phishing tests that try to trick the user into clicking on a link. The results of these tests (e.g. last month 88% of users were tricked, this month we are down to 79%) are often misinterpreted.

Is a 9% drop in one month a good result? Some say yes and forget that the "human firewall" is just a preventive control and to effectively mitigate the risks of malware infection, the organisation need to ensure adequate detective controls and a rapid response capability in Security Operations Centre.

5. False sense of third/fourth party security

Whilst the agreement on maintaining a minimum security baseline may exists between a service consumer (e.g. Bank) and a provider (e.g. Application Outsourcing organisation), the consumer may still be exposed to risks through vulnerabilities in provider's supply chain.

With the advance of FinTech, InsureTech and similar compartmentalisation trends outside of Financial Services, supply chains are getting more and more complicated. It is no longer enough to solely manage the risk of third party suppliers, rather security architects have to look beyond and think about fourth and fifth parties.

Due to a lack of resource to perform the necessary regular due diligence, organisations have to rely on vaguely defined ISO27001 compliance certificates or worse – self assessment questionnaires. As everyone who has ever been on the receiving end of those questionnaires can testify, a self-assessment approach leaves too much room for interpretation which in turn means one thing for the requesting organisation – a false sense of security.

For example, a common practice could be the outsourcing of certain IT elements to a third party whose sole business model is delivering reduced cost IT services to its clients. In order to further achieve this and provide a competitive rate, it too outsources certain elements to dedicated providers, who further may do the same.

6. Retaining control over data

The need to exchange information with other parties is a central requirement for every organisation's technology estate. Furthermore, information sharing is being encouraged under the latest regulations with examples of Open Banking and PSD2 being introduced within the UK. Organisations, however, must be confident that information disclosed has reached its intended destination, containing the same message originally constructed, and only in the hands of those the information was destined for.

Whenever any information is disclosed there always exists a degree of risk as the information leaves the organisational boundaries and the controls put in place by the organisation to protect that information are lessened. For example, information may be sent in an encrypted manner, but it must be feasible to decrypt the information when it reaches the destination, so confidence must be in place that only those entitled have the means with which to decrypt and view the message contents.

There are further complexities around the time of access. I might share the information now, but would like to revoke the access if the business environment/relationship changes. It's very difficult thing to do as soon as one has pressed that 'send' button.

7. Optimal logging

The traditional approach to security monitoring has been to consume all available logs across the organisation to provide the best possible 'visibility' of the network to the security teams. Whilst this approach can be largely successful, there exist both constraints and challenges.

As the number of interconnected devices continue to increase across the organisation, and the tools and techniques of malicious attackers become more sophisticated, the logging required to detect and record all the events risk the creation of a 'data swamp' which can overwhelm even the most staffed security operations centre (SOC).

The management of a 'data swamp' also requires multiple subtasks, from investigating the action, checking logs, referencing threat intelligence, to administrative tasks such as sending emails and constructing reports, and corrective action must be implemented which may also include developing IDPS signatures, updating proxy blacklists, or disabling an account.

The balance of optimal logging is a difficult one. Either organisations attempt to consume every available log and risk overwhelming their SOC team, potentially missing malicious traffic amongst the noise of event data, or purposefully constraining their visibility of the network due to artificially imposed financial pressures of MSSPs.

8. Access recertification

An integral process in ensuring the security of an organisation, identity and access management (IDAM), remains a constant challenge with organisations struggling to regularly keep access permissions in check.

Corporate user directories are often awash with issues including unlabelled accounts without clear owners, 'copy-ids' being provided to new employees without a privilege revalidation exercise taking place, toxic access combinations where users can both initiate and authorise certain workflows, and an inability to effectively audit the process.

Revalidation of accounts is a complex exercise that requires business stakeholders to not only to understand the concept of least privilege, but also to be very well aware of various interconnected systems they own and an aggregated risk profile of a role that results from the amalgamation of entitlements. In reality the role owners just click 'accept' because the amount and complexity of recertification exercises is unsurmountable.

For example, a global universal bank who recently undertook an annual recertification exercises incurred a total of 14 million recertification clicks from system owners and line managers in a year. Such a large scale mundane activity is likely to create a 'tick box culture' where the cost vs value of risk reduction is highly debatable.

9. Tooling-based security strategies

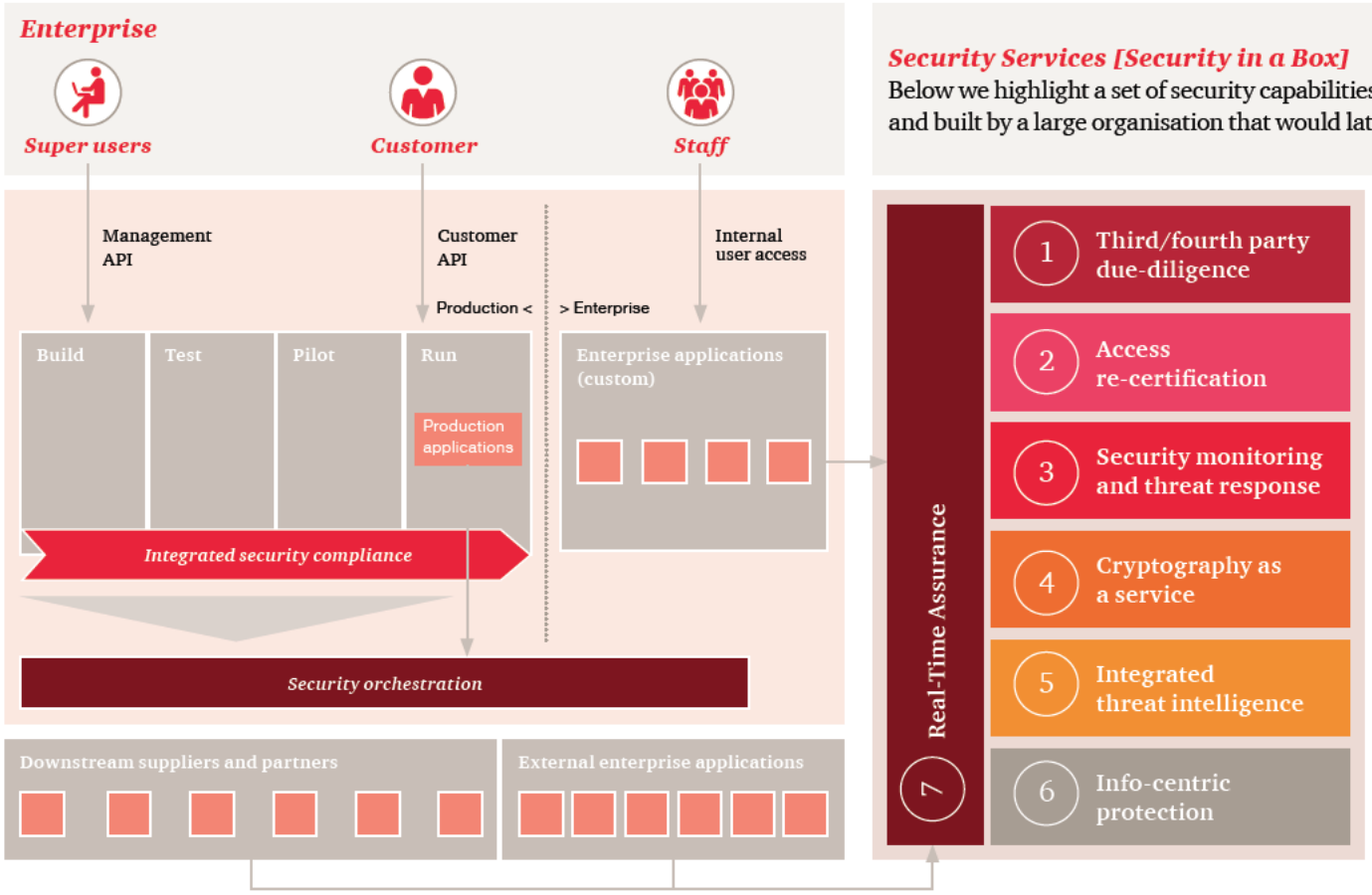
As email attachments continue to dominate top positions in the list of methods to breach an organisation, there is a continued focus on securing the endpoints. The market is booming and architects are finding themselves drowning in a variety of signature, heuristic, white/black list based, cloud threat analysis enhanced end-point protection tools. When recently performing a tooling portfolio review for a large organisation, we have found 25+ end-point security solutions with overlapping capabilities. Some of them were rolled out globally, some purchased by regions, some piloted to prove that others don't work and some are just there but no one has yet got around to configuring them. This challenge is caused by an oversaturated market of tools, lack of standardisation amongst security solution protocols and subsequent inability to properly integrate tools. This challenge is further compounded in that, in comparison to other IT and non IT industries, the IT security industry is relatively immature. Security professionals often obsess over the purchase of the latest best-in-breed solutions, with little consideration for the cost of maintaining an additional tool, which if not done effectively undermines any marginal benefit in terms of threat mitigation. As a result, many security strategies are based on the most popular tooling and not a sound architecture approach.

Redefining security architecture

Security in a box

Thinking about the Open Banking initiative established by UK's Competition and Markets Authority, a number of non-financial services organisations have already started to build their own banking products to better service their customers. While Open Banking is a huge step forward, it is just the beginning. As the technology world inevitably continues to move towards de-coupled, business-oriented web service architectures, enterprise architects will soon be able to go through catalogues of third party services and easily create ecosystems that transcend the industry boundaries and are uniquely tailored to deliver specific business propositions.

In response to the technology capability requirements of the business, enterprise and technology architects will be creating a 'box' of technology services like a product portfolio shop front, payment acceptance, loan management etc., and giving it to the business. We think that security can be a part of this 'box' of services. Security architects can use this service approach and advancement in technology to create a template for a security organisation or 'security-in-a-box'. This will allow one to address the legacy challenges and deploy security mechanisms at a pace with better agility.



Security Services [Security in a Box]

Below we highlight a set of security capabilities that can either be provided by someone or taken as a concept and built by a large organisation that would later provide those 'boxed' services to a group.

1. Third / Fourth Party Due Diligence – A prioritised list of suppliers and partners based on real-time indicators of their security posture, that focus organisational effort such as on-site audits and war-gaming exercises only on the ones that truly represent the biggest risk.

2. Access Re-certification – Radical reduction of effort required to review staff access permissions, achieved through anomaly detection and data mining.

3. Security Monitoring and Response – Radical reduction of effort required to monitor and analyse security alerts, achieved through data mining and anomaly detection.

4. Cryptography as a Service – Standardised way of executing crypto operations that helps to avoid implementation of vulnerable cryptographic protocols and methods.

5. Integrated Threat Intelligence – Rapid detection of new threats with no or minimal human intervention.

6. Information-Centric Protection – Centralised security policy that protects sensitive data even after it has left the organisation.

7. Real-Time Assurance – A dynamic, real-time overview of an organisation's security posture that is based on security risk and performance indicators.

Security-in-a-box vs Managed Security Service Provider [MSSP]

Some may question how the Security-in-a-box approach differs from that of a MSSP? A traditional MSSP typically focuses on placing security incident and event management software at the core of customer operations, collecting a pre-define set of logs, monitoring use cases and enabling integration at a process level. As previously discussed the approaches encourages ineffective logging behaviour, a false sense of security, and enables the outsourcing organisation to assume they no longer own the risk having outsourced 'security' to a third party.

This promotes a status quo, where both the organisations neither adapts to change in the threat landscape, or change in their own organisation. Further to this, there exists little incentive to challenge the status quo due to the repercussions of the MSSP bill. MSSP programme typically stop maturing at a point where key infrastructure monitoring use cases are in place and never evolve to a proactive, threat-led security operation, operating in a reactive manner to meeting security requirements. The tried and tested, not necessarily innovative, 'cookie cutter' approach is applied to all organisations, regardless of industry or operating environment.

A proactive approach is required to move organisations beyond the 'cookie cutter' methodology, where applications are analysed, rules designed, budgets secured, changes made prior to the application deployment, rather than post deployment, and the application running at risk deemed both acceptable and just part of doing business.

In comparison, the security-in-a-box approach, introduces much deeper integration at a technology layer and puts security coordination at the core, with deep integration with the software delivery function.

The prior approach to security is no longer fit for modern software delivery methods, security is often seen as a blocker rather than an enabler, and deemed the enemy that causes delayed product releases and open risks. Security-in-a-box proposes that through deep integration with the software delivery function, security requirements can be 'codified' and included as part of the development cycle and testing cycles ensuring that when the product is deployed, the requirements are already met.

Prerequisites

In order to arrive at the point where deploying a 'security in a box' model is feasible, some initial prerequisites must first be met. The list is not a definitive one as different types of organisations require different security capabilities, but if asked for a template set of patterns, an architect should evaluate the following:

a. Security automation

To effectively utilise the 'security in a box' model, an organisation must adopt an approach that will strive for automation of security controls. Simply put – A security architect must set an objective of automating himself/herself out of the job. While this will never be achievable, the mind-set will allow them to break security capabilities into a set of reusable services that can be integrated into the organisation's IT architecture and reported on in real time.

For the last 5-7 years, a number of security vendors have been producing security middleware to aid in the automation of basic use cases for security.

Such as automating the Intrusion Detection/Prevention System switching from monitoring to blocking mode in the event of receiving high confidence signal from an internal deception device. The products were largely not successful due to a lack of flexibility caused by the reliance on proprietary protocols and architectural complexity. With the advancement of DevOps and microservice architecture, security engineers can adopt/develop their own security integration platforms and continuously tailor those to organisational needs through collaboration with agile software delivery teams.

A security automation/orchestration platform will enable the tailoring of externally provided security services to organisational needs and develop necessary reporting functionality to put security signalling into the context of risks faced by an organisation.

b. Proving platform as a service

To reduce the complexity of any challenge, people must focus on what they do best. Leading cloud service providers are employing dozens of people to search for relevant compliance requirements and addressing the ones in their control so client organisations don't have to.

A security architect must work with developers to understand if the organisation can move towards a platform as a service model. If the risk appetite permits, this approach can save thousands of man hours and help to patch against security vulnerabilities faster. Large infrastructure service providers spend millions on rigorous patching schedules.

Security services

Below we describe a set of security capabilities that can either be provided by someone or taken as a concept and built by a large organisation that would later provide those 'boxed' services to a group. The list of security services is not a finite one and with time, as the market matures and the IT industry moves further into 'API world', it can be updated, expanded and enhanced. The services below are based on solutions and propositions that are available right now and should be considered by any architect that is tasked with protecting information in the cloud.

1. Third/Fourth party due diligence

An architect should look into utilising the telemetry and intelligence provided by specialist third parties to classify and prioritise suppliers. Today's technologies provide historical insights in third/forth party supplier postures using information such as association with known bad domains, outgoing malware communications to command and control domains, improperly configured perimeter controls and other indicators of bad security hygiene or weak security posture.

This will provide the much needed context to hundreds of supplier assessment requirements raised by security governance and business continuity teams.

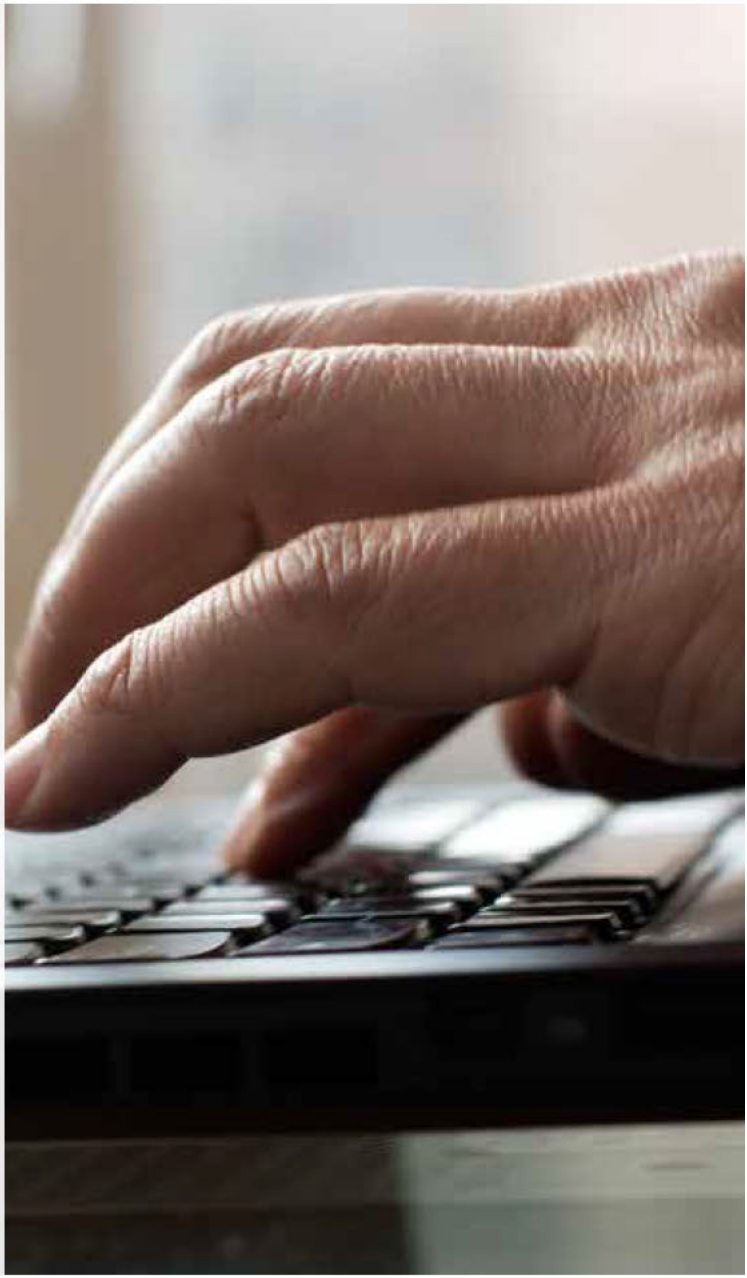
Business outcome: A prioritised list of suppliers and partners based on real-time indicators of their security posture, which allows to focus organisational effort such as on-site audits and war-gaming exercises only on the ones that truly brings the biggest risk.

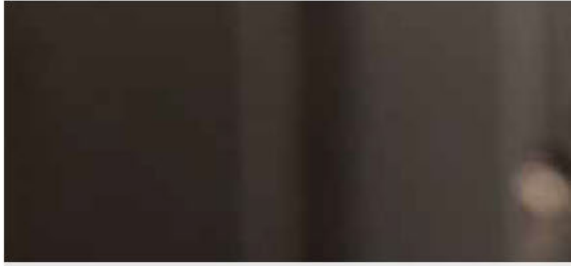
2. Access re-certification

Big data mining capabilities and anomaly detection algorithms could assist the business in making decisions in the area of access recertification. Instead of relying on human to understand 10-30 IT access policies, software can review access profiles across ground of similar employees, identify patterns and flag only the ones that look irregular. This way, the role of an application owner is reduced to just looking at the anomalies.

Further to that, if a security service can be built to produce outputs in human readable format e.g. 'access to business application A, menu B, Commands C and D' instead of 'Access to server X, entitlements group Y, Controls Z', the application owner can be much more effective in making the right security decisions.

Business outcome: Radical reduction of effort required to perform access, achieved through anomaly detection and data mining.





3. Security monitoring and response

To solve the problem of counter-productive logging practices described in the previous section of this document, security architect should again turn to computer aided analysis methods such as anomaly detection algorithms.

If a security service API accepts logs and reviews the data automatically, without human intervention, the cost of the service should not place restrictions on the amount of data that can be received. As with many analytical tasks, the more data provided, the better the quality of the output.

If 3 common cloud challenges of latency, sovereignty and security are addressed, then a security monitoring and response API can turn the current MSSP approach and business model on its head, and ultimately provide customers with much better value.

Business outcome: Radical reduction of effort required to monitor and analyse security alerts, achieved through data mining and anomaly detection.

4. Cryptography

Applications developed by software engineers must rely on a standardised method of performing crypto operations as nothing worries a security architect more than in-house developed, non- validated crypto functionality.

Cryptography API could also help dealing with a problem that prevents many Chief Risk Officers from becoming cloud adoption advocates – The risk experts feel unease when thinking about storing master keys in the same cloud infrastructure that runs your operations. Security architect must evaluate CaaS/KMSaaS solutions to ensure that keys are split into components and stored between various vendors and not one of those can construct the master key by itself.

If implemented correctly cryptography API can accelerate the adoption of the public cloud.

Business outcome: Standardised way of executing crypto operations that helps to avoid implementation of vulnerable cryptographic protocols and methods.

5. Integrated threat intelligence

The days of focusing on perimeter protection are long gone and any security architect knows that an effective security strategy must incorporate proactive threat management capabilities. Having said that, subscribing to a threat intelligence platform is not enough. Technical indicators must be extracted and operationalised, through the security orchestration layer, deep into end-point detection technologies to enable the ability to proactively scan the environment for new threats, as close to real-time as possible.

Integrated Threat Intelligence API can be used exactly for this – Upon request, technical indicators can be used to swipe the estate and search for a confirmed compromise.

Business outcome: Rapid detection of new threats with no or minimal human intervention.

6. Information – Centric protection

Cloud computing allows developers to focus on what they do best – development of applications, instead of management of the infrastructure. The same principle should be applied to security – Instead of focusing on infrastructure, security architects must focus on the data, and utilise data-centric security solutions that protect the data end-to-end. The net result ensuring only those authorised have access to the data, regardless of the infrastructure that data resides on.

Standardised, Data or Information – Centric protection service allow for further integration into organisational security capability portfolio. Using this API, security architects will be able to drive information protection decision using previously defined data loss prevention and access control policies.

Business outcome: Centralised security policy that protects sensitive data even after it has left the organisation.

7. Real-time assurance (GRC)

The days of monthly security report slides and weekly security dashboards are coming to an end. One of the central benefits of security automation is ability to mine security APIs to extract a real time view of security posture. Data provided by continuous vulnerability scans, configuration compliance monitoring, antivirus products and other controls, can be correlated to known threats and SOC processes to provide executives with a real-time view of Cyber risk.

Business outcome: A dynamic, real-time overview of organisation's security posture that is based on security risk and performance indicators.

Next steps

This article describes a set of common challenges we see while working with our clients and proposes a blueprint for a solution.

This is not an exhaustive list of the building blocks but the approaches mentioned in this paper are the ones that, in our view, differentiate the next generation security architectures from the legacy ones.

If you have thought of another security challenge or would like to suggest an approach to solving any of those, please get involved in the conversation here –

http://pwc.blogs.com/cyber_security_updates/


02D 025
02D 026
02D 027
02D 028
02D 029
02D 030
02D 031
02D 032
02D 033
02D 034
02D 035
02D 036
02D 040
ENHANCEDCAT6

Contributing authors

Anton Tkachov

Editor

Anton is a Chief Security Architect in PwC's Financial Services Cyber Security team. He is leading teams that help Banking, Insurance and Capital Markets clients to solve the most complex security challenges.

He has over 14 years of experience in the field of information and cyber security. Prior to joining PwC, Anton has worked for a Large Multinational Technology and Consulting organisation and various leading financial services organisations.

Anton believes that by adopting the principles of Cloud computing, security organisations can provide better, faster and much more agile service that will match the expectations of modern businesses.

George Florentine

Author

George is a Security Consultant within the PwC Financial Services Cyber Security team. He works with a range of clients across Banking, Insurance and Capital Market organisations.

He has a diverse range of information security expertise. Prior to joining PwC, he worked for one of the largest system integrators delivering security services to financial services clients.

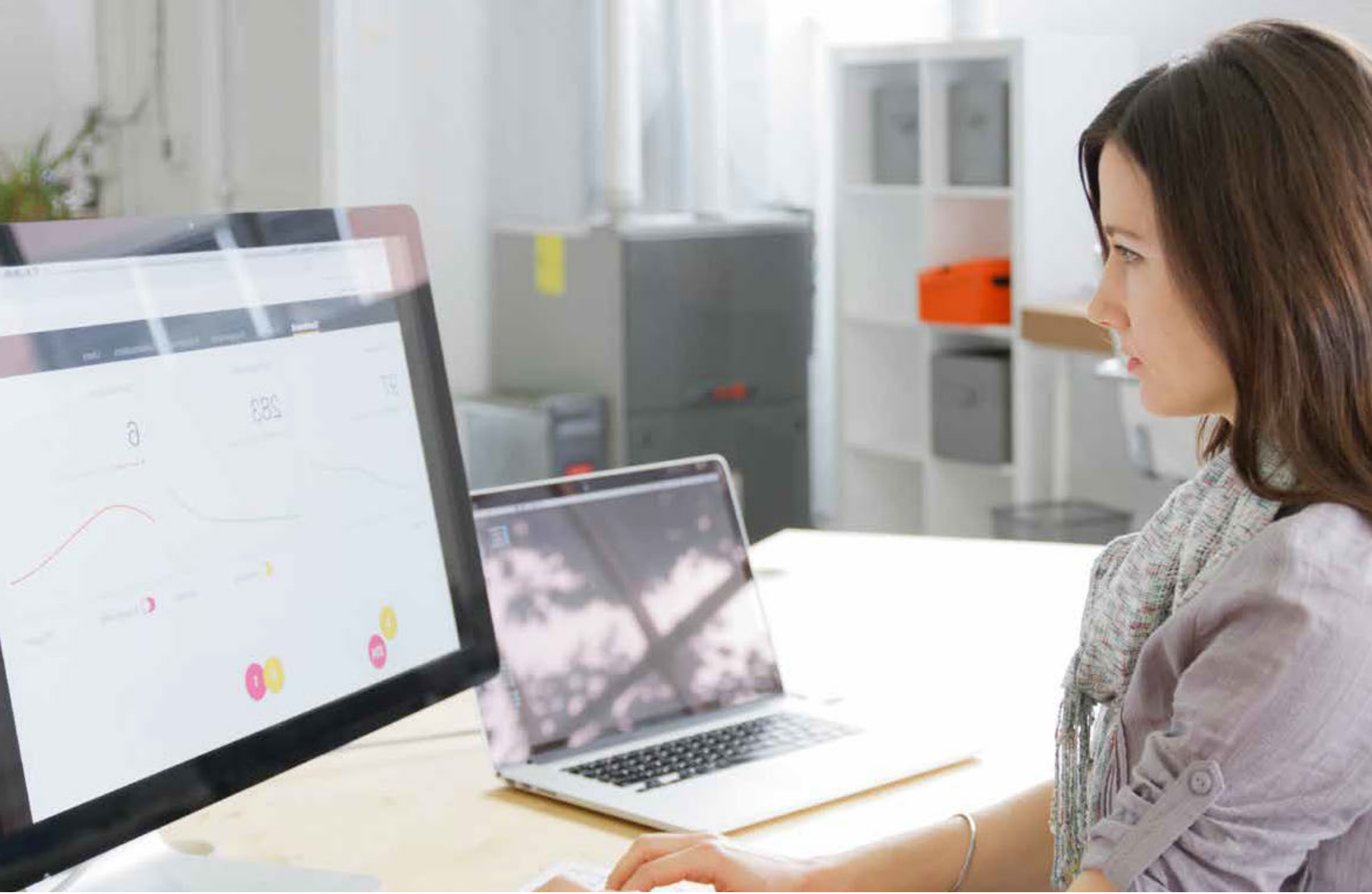
George thinks that large-scale Cloud adoption is inevitable and while some are still catching up, the security industry overall has made a great progress in enabling businesses to embrace the technology and associated methods.

Paul Gamble

Editor

Paul serves as CTO for the UK and Ireland alliances business, leading articulation of Symantec's overall technology strategy with our advisory and technology alliances as well as their clients.

He has worked in the IT business for over 25 years in areas of security architecture, information management and service management. In the last 18 years, Paul has engaged extensively across the telecommunications, finance, retail, energy and public (UK) sectors. Over much of the last 4 years, Paul's focus has been the development of joint Cyber Intelligence services with Symantec's leading advisory partners.



www.pwc.co.uk

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Design Services 31090 (01/18).