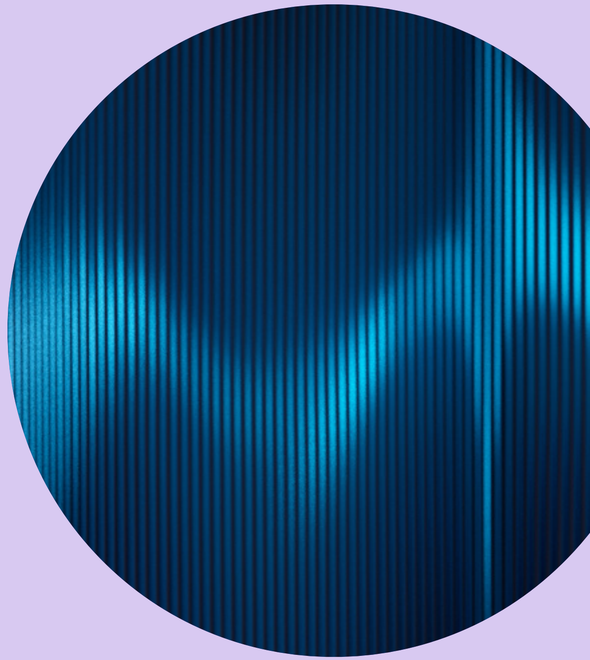
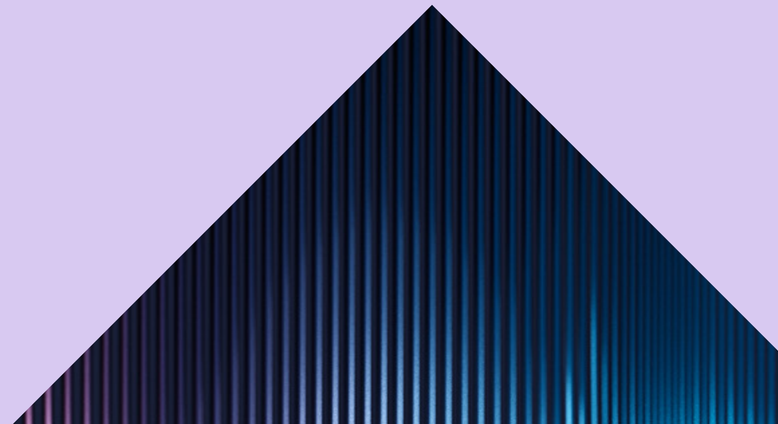
Ebook

MSP partner reflections on cloud security

Etienne Greeff, CEO of Flow,
a WithSecure™ UK Platinum Partner





Contents

Introduction 3
Weighing up the benefits and risks of cloud migration 4
Is the ‘shared responsibility’ model the answer to cloud security? 5
Why complexity is one of the biggest cloud challenges 6
What are the most common types of security threats specific to the cloud? ... 7
How can organisations build and maintain a robust cloud security posture? 8

Introduction

Cloud migration is one of the most important trends in business technology today – and also a leading cause of cyber risk. We sat down with Etienne Greeff from our partners at Flow for his thoughts on balancing risk and reward in the cloud – and how MSPs can help.

Etienne is one of the early pioneers of the internet security. Etienne first got involved in cybersecurity in 1994, after he graduated University. He really has seen the development of the industry from the very beginning.

He has spent over 20 years promoting the innovative use of technology and building services to solve complex issues. He has been involved in numerous general management roles during his career but has enjoyed staying close to the technology. He came aboard Flow as CEO in December 2020, leading the transformation of Flow becoming the smart choice for secure cloud transformation.

Weighing up the benefits and risks of cloud migration

There is always a huge amount of excitement whenever a new technology is introduced in the business world. The focus is always on the benefits and the future possibilities and the cloud is just the latest example of this trend.

So, you have a CEO reading their favourite business publication, they see a glossy headlines about the next big thing…. cloud technology and want to start claiming those benefits for their own organisation. However, there is always downsides, and these are not as enjoyable to talk about, so they tend to get overlooked in the early days – or they might not even be apparent yet.

As a result, the emphasis is very much on getting said technology online as quickly and efficiently as possible to start reaping those benefits and gain an advantage over slower-moving competitors. However, the focus on speed, can easily come at the cost of security. The hidden downsides of new technology may not be obvious until they come back to bite the organisation later on – potentially in the form of a catastrophic breach.

Introducing risk is a natural part of doing business – any decision you make will be a case of weighing up opportunities against potential risks. But when it comes to new technology, cyber risks are often entirely overlooked as part of this thought process. This is true even for larger organisations with more mature processes in place.

This isn't a new problem – it happens every time a new form of technology is introduced. Look back far enough and you can see the same thing happened with mainstays like email, and even getting online in the first place.

However, the cloud is a different proposition to some of the previous tech revolutions. One important factor is that it's such a diverse form of technology. Not only is there an absolutely gigantic market presenting a myriad of options for building a cloud environment, but it can be fundamentally very different between different organisations.

On a basic level, some firms have simply moved their workloads to the cloud. The processes and workflows are largely the same, with the essential difference being that everything is hosted elsewhere and can be accessed remotely.

On the other hand, it can be a far more complex proposition that encompasses reshaping business processes to take advantage of the cloud.

Even the more basic approach can add a great deal of complexity that the business might not understand. On the surface you can easily start adding applications to the environment, but each new element creates connections and potential vulnerabilities that can be exploited.

Is the ‘shared responsibility’ model the answer to cloud security?

> “Everyone talks about cloud security as a single homogenous thing, but there is a huge difference between security in the cloud, security of the cloud, and security with the cloud. These are fundamentally different functions that have their own priorities.”

Etienne Greeff, CEO of Flow

Tied to this is the ‘shared responsibility’ model which has been popularised by infrastructure-as-a-service (IaaS) providers like AWS. This approach holds that the cloud provider has responsibility for security of the cloud, ensuring that the hardware and software elements that comprise the cloud are not vulnerable to attack.

Users meanwhile have responsibility for security in the cloud. This accounts for key security activities such as ensuring that software is configured correctly and strong access and authentication processes are in place, as well as the regular application of patches and updates. Users are also responsible for ensuring that any content uploaded to the cloud is safe and free of malware and safeguarding against attempts to access the environment through phishing and other methods.

It's a nice idea on paper. But in reality, if you’re an organisation using the cloud, you have almost all the responsibility. It’s your data, your applications, and it’s your customers at risk! You’re the one on the hook with the compliance regulators if something goes wrong.

It’s also important to remember ‘responsibility’ is a legal term as well as a sentiment. Unless it specifically says so in contract documentation, the cloud provider may not have much of a stake in your security.

The effect is like saying BMW is responsible for the safety of your driving. Yes, they are responsible for manufacturing a safe car, but everything about how it is used is down to you as the driver.

Why complexity is one of the biggest cloud challenges

The cloud is often seen as very simple and easy. The flexibility of the cloud means firms can quickly find and implement new elements. However, this flexibility creates a great deal of complexity behind the scenes. And complexity always means insecurity.

Agility is one of the primary advantages of the cloud, but we often see organisations moving so quickly that their documentation can't keep up. This can result in a dangerous situation where they lose track of what has been integrated into their cloud and how everything connects – an ideal situation for threat actors looking for a way in.

Moving to the cloud isn't just a case of shifting things around – it's a fundamental transformation of the organisation, and security is fundamentally transformed along with it. We find many organisations are still grasping the scale of this change.

For many years, security was largely a matter of controlling the ingress and egress of network traffic. Now however, the situation is very different, and there are many different ways in and out of the network environment that don't intersect with traditional controls.

For example, platforms like Salesforce allow users to upload documents. It's a very widely used feature and is central to activity like insurance customers uploading claims and documentation. But content uploaded in this way completely bypasses network traffic processes. If malicious code is hidden in a document, it will enter the network undetected unless further controls have specifically been put in place.

So, organisations have to critically think about the implications of all those external connections and interactions that are created whenever they add a new application or plugin.

Linked to this, businesses often don't consider the shift left that comes with digitalisation. In the past, a security department would have clear control over every element of the network. But now so many people in the organisation can impact its security posture through the cloud, security responsibility has shifted left towards those additional individuals. A marketing person could for example start a campaign on Salesforce and add some new third-party plugins that provide them with additional features. If they don't understand or address the security implications, this could cause serious problems.

Even for organisations with more mature security strategies, controlling all of the interactions and connections across the entire cloud infrastructure can be extremely challenging, particularly with third party providers.

However, organisations can directly control the security of their endpoint devices. Implementing layers of security to protect endpoint devices will reduce the chances of threat actors compromising individual machines and user accounts to launch attacks on the wider network, and also mitigates the risk of malicious code being delivered through compromised cloud elements.

This is where having an experienced security partner becomes really important.

What are the most common types of security threats specific to the cloud?

The headlines are usually dominated by stories about sophisticated threat actors using innovative new attack strategies to breach their targets. But in most cases, organisations are leaving themselves wide open to being breached due to misconfiguring their cloud environments.

Cloud buckets, databases, APIs, and many other assets are frequently misconfigured, often with little to no access controls in place. This has always been an issue with IT, but wasn't such a crisis when everything existed in an on-premise environment. Up in the cloud, all these poorly secured assets can be readily discovered and exploited remotely by threat actors.

Along with this, access management is a huge security priority. Being able to access assets from any locations is one of the main advantages of the cloud, but it also makes it much easier for adversaries to infiltrate the network. Unless there are effective controls in place like multifactor authentication or Zero Trust-type risk-based authentication, a stolen set of credentials will grant immediate access to critical assets.

The interconnectivity of the cloud means that a single compromised endpoint can quickly be escalated to access almost anything, whereas in previous years threat actors had to work a lot harder to achieve lateral movement across different systems.

How can organisations build and maintain a robust cloud security posture?

Strong cloud security is all about defence in depth. The environment is so complex that no single solution can effectively deliver security – it takes a multi-layered approach with different tools and services working together.

The NIST framework is a good point of reference for covering all the bases, as it breaks down the needs into five key functions: identify, protect, detect, respond, and recover.

We often encounter organisations that have invested heavily in security, but are still falling short of a robust cloud security posture. This failing usually stems from the absence of a unified point of control – all of their expensive solutions are working separately, which makes it very hard for security teams to get a view of the big picture. It also means personnel waste a lot of time flicking between different solutions and dealing with a barrage of disconnected alerts.

Organisations should ideally be striving for a single pane of glass approach that allows them to monitor and control everything in one place. This is far more efficient and enables security teams to more easily prioritise activities, as well identifying more subtle threats a disconnected system will likely miss.

WithSecure™ provides a good answer to this problem with its Elements cyber security platform. Elements combines multiple key solutions like Endpoint Protection, Vulnerability Management, and Endpoint Detection and Response (EDR) into a single and integrated cloud-based package.

Finally, organisations also need to account for Managed Detection and Response (MDR). Even the most mature companies with the biggest budgets can't assume they'll get everything right every time as determined threat actors will eventually find a way through defences. Remember that the last two of NIST's five functions, respond and recover, apply to a breach taking place.

So, you need to have MDR in place for when things go wrong. It's crucial to be able to quickly identify a threat within your system, act to mitigate the danger, and find and close the vulnerability that caused it.

Who We Are

Flow, the smart choice for secure cloud transformation.

With over 12 years of experience at the highest level, the expert team at Flow provide secure datacentre, network and cloud native solutions as well as industry leading managed services. Focussed on providing efficient solutions to organisations enabling them to do business in confidence, with seamless transition and without fear of a cybersecurity attack.

Our number 1 goal is to enable organisations to operate securely in the digital world and keep ahead of emerging threats. We work with you to do this through our belief in a holistic security strategy, engraining security at every stage of your digital journey. Cybersecurity is built into the fabric of all our solutions, enabling secure and confident business operations.

T: 01442 927 996
E: sales@flowtransform.com
W: flowtransform.com

FLOW
the smart choice

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

W / T H®
secure