# RETHINKING SECURITY

CIO ADVISORY BOARD
SUMMER 2021

# INTRODUCTION

## DELIVERING SECURE BUSINESS IN A VOLATILE WORLD

THE SECURITY MARKETPLACE IS ARGUABLY THE MOST DYNAMIC AND DIVERSE OF ANY ACROSS THE IT LANDSCAPE

The profound changes in the way we live our lives and conduct our business over the last 18 months have fundamentally changed many things, but a central priority continues to be security.

Whether in the delivery of consumer services via digital channels or the facilitation of remote (and hybrid) working – security principles and architectures are being redefined as we further exploit technology to support and enable the demands of everyone.

Underpinning this is a holistic transformation, not only of technology platforms, but the way that it is deployed and operationalised to enable business outcomes. Technology enables us to connect people and to obtain real-time access to information. It has also been key to enabling businesses to rapidly redefine value streams that service dramatically different customer needs, preserving jobs and livelihoods.

This rapid period of digital enablement has impacts upon security for businesses, and for consumers. Security and risk are always core business concerns, and the environment today feels like one in which the previous delicate balance has been disrupted, and we must reconsider approaches to manage risk and ensure security and compliance.

This pandemic era will have an additional footnote in history of fuelling a rapid shift in digitisation. Whilst security has long been a business imperative, it is hard to over-emphasise the focus we must apply to it in the period ahead.

Security and risk, once the concern and responsibility of specific experts – is now everybody's concern and is part of every conversation and decision.

## THE PURSUIT OF INTRINSIC SECURITY

The security marketplace is arguably the most dynamic and diverse of any across the IT landscape. A typical enterprise organisation might have over 100 security tools and products, many being well established products and brand names that infer trust and confidence built over many years.

But the security landscape has been one in which we have seen massive innovation throughout recent years. The security ecosystem has literally thousands of technologies, with new products being launched to market at an unrivalled pace. Each new product seems to offer the solution to the challenges, perceived or real, of earlier on incumbent products and tools. The market also capitalises on the buzzwords and hype that pervades the IT market, with the promise of Artificial Intelligence, Machine Learning, and Observability embedded into next generation solutions, surely providing an enhancement on what is already deployed and the old ways of doing things.

All organisations are driven to resolve and mitigate any potential vulnerabilities and security threats that exist in their infrastructure, but this is also mapped by a period of significant technology transformation taking place, generating new challenges and considerations for security professionals.

## DRIVERS FOR SECURITY CHANGE

### HYBRID WORK

The most obvious driver today is the remote and 'hybrid working' world we find ourselves in, and that we must work through in the period ahead. In the face of urgent demand in Q1 2020, IT organisations enabled mass remote working rapidly.

However, few organisations had architected for a hybrid working use case, so security systems and controls may deliver an ineffective user experience or be operationally cumbersome to support in a highly distributed model. All notions of a security 'perimeter' have vanished – with lack of visibility and even understanding of when, where and how people are remotely connecting to corporate resources. The volume and variety of endpoints is increasing, a mix of both corporate and non-corporate devices impacting the 'front line' of security strategies in Endpoint Security. The core network is now the public internet, with access and controls required to provide flexible, user friendly access to on-premises and cloud (SaaS) resources.

### MOVE TO CLOUD

For years the move to cloud has occurred in the form of adoption of Software as a Service (SaaS) solutions such as Office 365, Salesforce and Workday to name but three. In many instances organisations understand how to deliver this, through Identity Management and Information Protection systems to protect corporate data.

The next phase of the cloud journey is mainstream adoption of cloud platforms – IaaS and PaaS services, and the delivery of next generation cloud-native solutions. This area will accelerate in 2021 and beyond as businesses look to drive operational efficiency and generate agility through IT, but creates new questions around how security should be designed and delivered and how responsibilities should be divided between the provider and the customer.

The move to cloud also keeps topical the questions of data governance and sovereignty – particularly relevant not only in the face of recent drivers like Brexit and GDPR.

## ALL NOTIONS OF A SECURITY 'PERIMETER' HAVE VANISHED

### DATA AND INFORMATION

The explosion of data growth, and its usage over past years has presented opportunities for businesses in many ways. This has also dramatically increased the importance of securing all kinds of data stored in company systems and apps, in order to protect customer information, and secure intellectual property and other corporate assets.

This data, the 'crown jewels' of an organisation, has made it a compelling reason to attack organisations to steal it, or to hold the business to ransom. Allied with the shifts in architecture being deployed, use of SaaS platforms, business partnerships and ecosystems has made the management of risk, compliance and security associated with data a primary concern.

### DIGITAL ENGAGEMENT

The digital channel is now the primary channel in many instances. From retail to hospitality to healthcare, consumer engagement via a digital app or website now provides a faster and superior experience to face-to-face contact.

Smartphones create opportunities for consumers to access services in any place, at any time – but generates an explosion at the back end for security departments to track, predict and understand user behaviour and validate the integrity of the interaction. This mass use of digital engagement opens new vectors for attacks on an unprecedented scale.

Add to this debate the human angle. We are living in a period of heightened fear, uncertainty and doubt. The ability to capitalise on the lack of digital skillsets of users or obtain success through increasingly sophisticated attacks such as spear phishing are real, current concerns.

## SECURITY NEEDS TO BE INHERENT AND INTRINSIC – RATHER THAN 'ADDED ON' AS AN AFTERTHOUGHT

## THE SECURITY RESPONSE

### ENSURE THE 'BRILLIANT BASICS'

Cyber security and the dramatic implications of cyber vulnerability was elevated to be front-page news in 2017 with the arrival of WannaCry and NotPetya. These two attacks that demonstrated how disabling a mega cyber security attack could be – particularly when a key victim of the attack was the NHS, as an example.

The back story here is simple. Software patches for vulnerable systems had been available well before the attack, but a lack of proactivity, concerns about the risk of disruption from updates as well as deficiencies in asset visibility created a time gap opportunity that these potent attacks capitalised upon.

What these events remind us of is that the basics of IT security need to be a priority. Core operational discipline could reduce the impact of different attacks. Providing continuous asset visibility, least privileges, hardened IT systems, secured DNS, and system log aggregation and correlation via Security Information and Event Management platforms (SIEM) help better prevent and detect attacks. All now core parts of the defence strategy that must be in place.

We must also change our mindset. Security needs to be inherent and intrinsic – rather than 'added on' as an afterthought. Carefully balancing the user experience against the core security controls to maximise the protection at every stage of the user journey. Security is when a system works as intended and only as intended.

Brilliant basics balance the requirements across technology architecture and operations. Effective deployment and configuration; rigorous and sustained management and operations; an outward lens on what is happening outside your immediate environment to ensure future threats are anticipated.

### THE 'NEW' WORLD OF SECURITY

Brilliant basics alone are not enough. The labour-intensive approach to the implementation and configuration of security controls is now fundamentally challenged by the dynamics of digital. Good control delivers trust in the core platforms, which itself creates opportunity to accelerate the use of new technologies in order to grow.

One of the major challenges is a critical shortage of skilled security professionals. This challenge cannot be solved quickly - everyone is fighting for the same people and skills. Human skills must be augmented with highly-effective technology to succeed. Security automation is a key example of maturing capability, as is the adoption of DevSecOps as a model to break down the siloes and challenges to delivering security effectively, whilst retaining pace with the business.

The security marketplace is buzzing with new technology that proposes to eliminate the pain and challenge of today; next generation 'data-driven AI or ML powered' tools to improve the quality and operational effectiveness of delivering security. The security market is a confusing place to operate, and the conversation nearly always focusses on the extra tool you need rather than delivering better with what you have today.

The new model of security needs to consider new technology, better operational processes, a fundamental recognition that the context for security has changed, in terms of where and how services are consumed. The limit for scaling human labour is being reached, yet businesses need to continuously grow and innovate, and security must continually be enhanced and assured.

## TECHNICAL TRENDS IN SECURITY

### SECURITY CONSOLIDATION - PLATFORMS VS BEST OF BREED?

Security consolidation is no longer desirable, it is essential. The level of complexity from platform and tool proliferation has made it almost impossible to be operationally efficient and deliver great security.

The security world was founded in a 'best of breed' mindset. This led inevitably to stranded investments, operational ineffectiveness and gaps caused by the integration cost of this approach.

More recently the 'platform play' emerged. Pick a 'swiss army knife' type product, and for minor functionality sacrifice you gain in the significantly reduced integration burden – for some maybe even providing a better outcome through simplicity in operations or UX.

Secure Access Service Edge (SASE) is currently 'in vogue'. SASE provides a new approach that delivers common networking and security functions in an integrated platform approach. SASE solutions are now commonplace across the leading security vendors and are increasingly attractive based on the potential to drive down security procurement costs, deliver combined functionality across hybrid architectures and enable flexible connectivity.

### ARE MICROSOFT A SECURITY COMPANY? YES. BUT WHY?

In recent years, the acceleration of Microsoft's position as a security vendor has been significant. Notable acquisitions and investments now see them placed firmly in the debate for modern security. And aligning with their core client and cloud offers, they offer an engaging and compelling vision.

A key catalyst was Windows 10. This was but a fundamental redefinition of user experience, and user and device management and support. The continual (Evergreen) update approach creates challenges for the third-party ecosystem to keep up, but creates an opportunity and benefit for Microsoft. And Microsoft capitalised on their consumer footprint, leveraging the 'telemetry' from globally deployed Windows 10 devices to deliver innovative security insights and services.

Microsoft are not a new security vendor. They have built security functionality in their products for many years. They have now integrated and unified investments to deliver a platform solution. Their incumbency within the customer technology environment means you cannot ignore them, and we see many instances of security product displacement in favour of Microsoft alternatives in the months and years ahead.

### ARE ZERO TRUST MODELS THE NEXT TARGET?

Zero Trust is also 'in vogue'. The industry being quick to position the importance of the Zero Trust model to deliver security in the modern world.

Zero Trust describes a set of security principles underpinned by the need to understand context. The context could be location, device, or user identity, and it is always verified before granting access to resources, and most importantly can dynamically change. As the world has adapted to remote working, it is easy to see why Zero Trust conversations are so prominent when organisations have much less visibility and control on where and how people are connecting to their systems.

Zero Trust is not a singular solution or technology. The approach relies upon many of the 'brilliant basics' such as Digital Identity and the ability to quickly provision and de-provision access using trusted automations.

### SECURITY OPERATIONS

Proactive security operations are now a key part of a closed loop approach and vital to the maintenance of security awareness and response. It is impossible now to be secure by operating in a reactive manner, and the volume of security notifications and alerts from increasingly connected users and systems need you to be able to cut through the noise to stand a chance of identifying the real threats.

A drive towards SOC and proactive cyber defence services are a key part of the strategy to protect both customer data and internal data and systems. The common challenges of poor asset visibility, proactive maintenance and support of technical assets and a 360-degree awareness of the wider environment are key to ongoing management of cyber risks.

## STRIKING THE DELICATE SECURITY BALANCE

Delivering effective information security is complex, however, a focus on good operation practices to ensure security fundamentals are maintained will deliver increased levels of cyber security confidence.

The use of cyber security compliance frameworks paired with an 'assume breach' mindset is a good place to start. The frameworks ensure that organisations benefit from the best guidance available with the potential to gain certification to validate high levels of security are in place and maintained. CIS, NIST, ISO, cyber essentials are a selection of well used cyber security frameworks and standards that deliver guidance on the most effective approach to cyber security defence, remediation and operations.

Delivering effective information security has always proved challenging for organisations but never more so than today. Defenders need to be perfect all of the time but cyber attackers only need to be successful once. This means that maintaining an up-to-date operating environment, leveraging and updating good practices, and seeking to simplify the environment is essential.

Security was once the responsibility of the technology team, implementing perimeters and controls in a world where you knew what was trusted and what wasn't, and where it was. Today's security threat is more diverse – from more users, across more locations, on more kinds of devices – and this amplifies the business risk conversation and the implication that failure or vulnerability have on organisations as well as their consumers.

## CYBER SECURITY AND SECURITY RISK MANAGEMENT IS NOW EVERYBODY'S RESPONSIBILITY AND CONCERN

## About Computacenter

Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. We help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 16,000 people worldwide.

Computacenter

**Computacenter (UK) Ltd**
Hatfield Avenue, Hatfield, Hertfordshire AL10 9TW, United Kingdom

**computacenter.com**
+44 (0)1707 631000