Why are organisations looking to adopt a zero trust security model?

White Paper
June 2022

Author:
Richard Hogan,
IBM Consulting

Contributors:
John Sheaf, IBM Consulting and
Stefaan Van daele,
IBM Security

Adapting security to new cloud environments

"IBM research indicates that in 2020, upwards of 90% of cyber-related incidents studied originated in cloud environments."

Source: IBM IBV Study 2021

As more and more organisations adopt a hybrid and/or multicloud environment, the ability to protect against threats becomes increasingly difficult, especially when organisations attempt to apply legacy-based security models to the new cloud paradigm.

These models may well be sufficient when an organisation's assets are in one central location like a data centre, and all users are based in physical office locations which are controlled by central IT departments, but probably won't offer enough protection for new, hybrid environments. To add to the complexity introduced by the new cloud services, the COVID-19 pandemic has complicated matters even further, as many organisations adopted a remote work policy so they could effectively continue working during the pandemic.

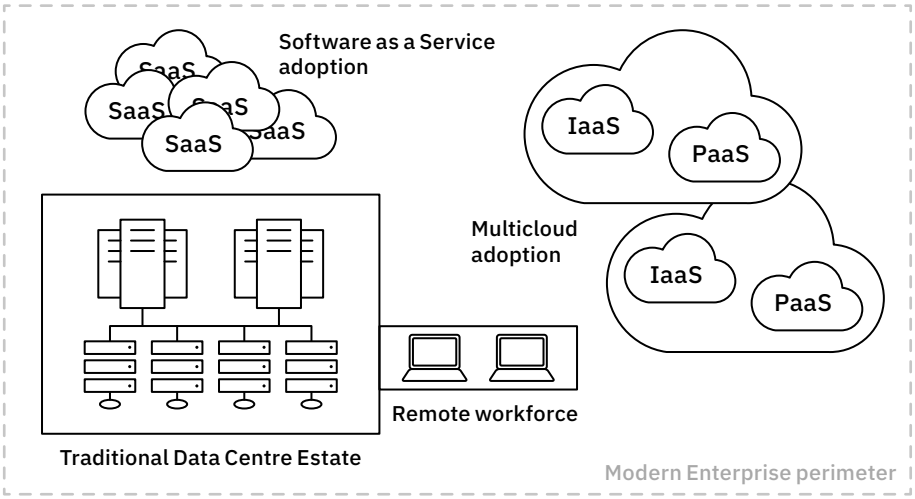

Figure 1: Modern Enterprise security perimeter

Source: IBM

This has the effect of moving the defence perimeter of the organisation away from the central data centre or company premises to a perimeter that encompasses the various cloud services (including a combination of SaaS, PaaS and IaaS services) as well as the remote workforce who can access the corporate estate via a number of means including desktops, laptops and mobile devices. This does not even consider IoT or edge devices, which further extend the perimeter.

A zero trust model can help to reduce the attack vectors and mitigate the blast zone of any impacted systems.

What is a zero trust strategy?

One of the primary differences between traditional security models and zero trust strategy is that the default posture is to assume breach – this posture effectively implies that attackers are already present in your organisation's network and appropriate controls need to be defined and applied to counter this assertion. To counter the assumed presence of threat actors within your estate, a zero trust approach provides a series of principles that should be implemented to restrict/control access to resources, regardless of their physical location. The other key principles include:

- Assess trust dynamically and consistently
- Constantly monitor and optimise
- Define the protect surface, not the perimeter
- Leverage network segmentation to implement micro-perimeters

"92% of organisations surveyed lack the ability to securely enable cloud-native capabilities to their internal and external partners."

Source: IBM IBV Study 2021

The upshot of these principles is that identity (person, device and/or application) is constantly being authenticated and authorised. Constant verification helps organisations stay on top of resources, so that any changes in the estate are monitored, identified and audited, and the appropriate teams are notified.

Benefits of a zero trust model

In a recent study the IBM Institute for Business Value (IBV)[1] found that the surveyed organisations who had implemented a zero trust model reported experiencing the following benefits:

- 54% reported experiencing an improvement in detection and response capabilities and vulnerability management.
- 61% of the zero trust adopters reported an improved ability to limit malware propagation, and a reduction in the impact of breaches.
- The ability to establish and maintain secure connections between ecosystem partners allowed 54% of the adopters to report capitalising on cloud investments.
- More of cybersecurity budget invested in upskilling resources has led to 60% zero trust pacesetters, reporting cyber resource retention rates 10% higher than their peers.

In the same study, IBM found that only 23%[1] of participating organisations are currently pursuing a zero trust policy. This figure is not surprising as implementing such a shift in both processes and technology can be daunting and potentially complicated.

[1]Source: Lisa Fisher, McCurdy, Chris, Parham, Gerald and Thomson, Shue-Jane. "Getting started with zero trust security", IBM Institute for Business Value, August 5th 2021, https://ibm.co/zero-trust-security.

What's the cost of not doing it?

In today's current landscape, organisations cannot afford to neglect the risk and security factors involved in their journey to the cloud. Even a minor breach could have disastrous consequences with long-term damage.

According to the same IBM IBV study, the average total cost of a data breach to an organisation in 2020 was $3 million, alongside 'unrecoverable impacts on reputation and brand'[2]. The most immediate and difficult challenge that organisations face is putting a zero trust policy into action, protecting sensitive information at scale across the enterprise and embedding a culture and mindset of zero trust.

The average total cost of a data breach to an organisation in 2020 was $3 million.

Source: IBM IBV Study 2021

[2]Source: Lisa Fisher, McCurdy, Chris, Parham, Gerald and Thomson, Shue-Jane. "Getting started with zero trust security", IBM Institute for Business Value, August 5th 2021, https://ibm.co/zero-trust-security.

Implementing a zero trust model with IBM and your Microsoft product set

If your organisation is already utilising Microsoft technologies, either on-premises or via a combination of Microsoft 365 and Microsoft Azure, then it is likely that you already have the tools that you need to provide a foundational zero trust model.

IBM has produced a zero trust framework that provides a well-defined and structured approach, which is designed to leverage your existing Microsoft technology investment and integrate IBM technologies, such as Cloud Pak Security (CP4S), X-Force Threat Management and our industry leading consultancy services, to provide an end-to-end, zero trust security approach.

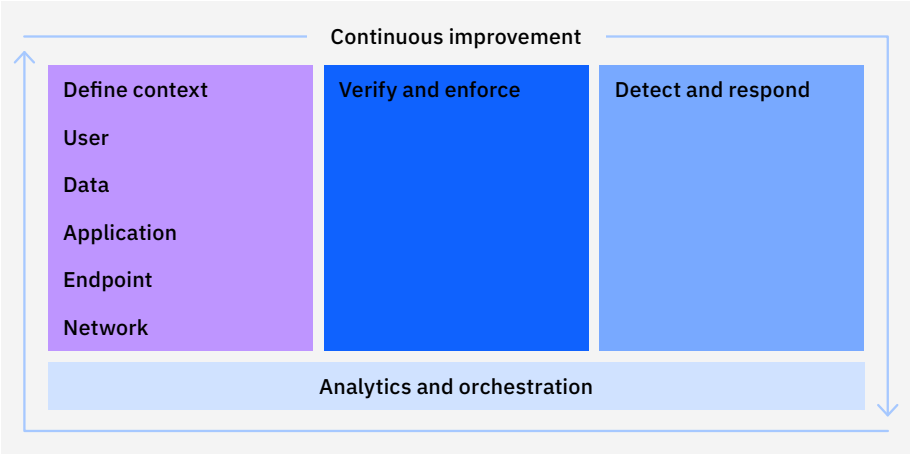

Figure 2: IBM zero trust governance model

Source: IBM

The goals of the different elements of IBM zero trust framework, include:

- **Define the context:** Understand users, data and resources to create coordinated, security policies aligned with the business.
- **Verify and enforce:** Protect the organisation by quickly and consistently validating context and enforcing policies.
- **Detect and respond:** Resolve security violations while trying to minimise the impact to business by taking targeted actions.
- **Analytics and orchestration:** Continually improve security posture by adjusting policies and practices to help make faster, more informed decisions.

Why IBM?

IBM and Microsoft have been strategic partners for over 30 years, at a product/technical level, but just as importantly at a client level.

This relationship allows IBM to leverage a variety of Microsoft technical resources, either from the product group and/or from the customer success teams. This provides IBM and your organisation with the ability to:

- Hold IBM business security framing workshops to develop solutions and architectures with IBM that can compare against Microsoft Best Practices and Guidance, including the Cloud Adoption and Well-Architected Frameworks.
- Leverage Microsoft and IBM incentives, such as AMMP to support workload migration/transformation as well as Proof of Concept, Proof of Value and/or Minimal Viable Product (MVP) activities.
- Leverage IBM's alliance with Microsoft to benefit from insights from Microsoft Technical Specialists and Architects as well as the Product Group.
- Gain understanding of Microsoft's published product roadmap and gain insights into services and features which can assist with strategic decision making around the Microsoft and IBM stack.

IBM continues to invest in the Microsoft relationship, and is committed to providing industry-leading solutions for our clients by combining IBM technology and industry and domain experience with the cloud services provided by Microsoft.

This commitment is evidenced by the recent acquisition of a leading Microsoft partner in Neudesic, adding to IBM's recent list of acquisitions in this space, including Nordcloud, Taos and BoxBoat.

Strategic partners for over 30 years

Azure Red Hat® OpenShift®

Fully managed Red Hat OpenShift service on Microsoft Azure to run containers in the cloud. Jointly engineered, managed and supported by Microsoft and Red Hat.

Joint Engineering

IBM and Microsoft regularly combine knowledge and experience to collaborate on cutting edge technologies, such as Digital Twins, Security and IoT.

Marketplace Solutions

Several IBM solutions have been published directly to the Azure Marketplace and AppSource for easy consumption and integration with client solutions.

Advanced Specialisations

IBM currently holds several advanced specialisations, including:

- SAP on Azure
- Kubernetes on Azure
- Modernisation of Web Apps on Azure
- Azure Virtual Desktop
- Analytics on Azure

Gold Microsoft Partner

Microsoft

Azure Expert MSP

So what can you do next?

Try a no cost, virtual business security framing session with IBM so you can experience first-hand how the people and practices of IBM can help accelerate your security transformation. Here's how it works:

1

Tell us about your security challenge

Maybe you've got a specific business or technology problem in mind. Or perhaps you want help building an innovative, agile culture. Share a few thoughts and we'll get in touch to schedule your session. You decide who you want to bring along from your company (up to five people).

2

We'll get to work with you

With your session in the calendar, we'll pull together a team from IBM to create a set of thoughtful activities designed to give you a new insight.

There's a variety of areas that we can cover such as: Identity and Access Management, Threat Protection, Cloud Security, Information Protection, Risk Management – but let's get the foundation first and we'll take it from there.

3

Attend your framing session

Join your interactive virtual session guided by IBM. In our two-hour meetup, we'll explore your challenges and drivers and you'll benefit from experienced perspectives. We'll jump into collaborative activities that ignite communication and fresh thinking, expose new options to achieve your business goals and build consensus within your team. Your team can gain clarity and alignment on your critical needs and a custom statement.

4

Take the next step

A no cost framing session is a great place to start, but it's only the first step. You can choose to continue a consulting partnership with IBM, with options like an Enterprise Design Thinking workshops to define how we'll get to work building on your security foundations and enable your IT team and other users to leverage the security features available to you.

For more information or to arrange a framing workshop, please contact richard.i.hogan@ibm.com.