IBM IT Infrastructure

Seven steps to a more secure IT infrastructure

IBM

Table of contents

Chapter 1

Recognizing that you're not alone: Security on your mind

Here's a little exercise. Walk to your whiteboard and map out your hybrid cloud architecture.

As you draw the complexity of multiple public cloud providers, private cloud and on-premises infrastructure, where are your security vulnerabilities?

Does everyone share your conviction that a secure IT infrastructure is essential for business success?

Security architecture as a key part of enterprise architecture

You may have already done this exercise on your whiteboard — or at least in your head.

Like other IT leaders, you may be considering how to elevate security in your hybrid cloud strategy. And like them, you're realizing it will take a holistic approach with your IT infrastructure serving as the foundation.

There's no doubt that hybrid cloud is here to stay. In a recent report from Forrester Consulting, approximately eight in ten IT leaders expect their companies to invest more on public cloud over the next two years.[1]

Yet the journey to cloud is at an important crossroads. Mission-critical data and workloads once contained in the data center are now spread across hybrid cloud environments. This amplifies the attack surface significantly.

More cloud providers — and more movement of high value data and workloads — put security at top of mind. In fact, 40 percent of those Forrester respondents feel that public cloud doesn't meet their security needs.[1]

40% *of IT leaders feel public cloud doesn't meet their security needs* [1]

Making the business case for IT infrastructure investment

If cloud has you reconsidering security, your solution could be in the data center. In that same Forrester study, 90 percent of IT leaders agreed that on-premises infrastructure is a critical part of their hybrid cloud strategy.[1]

But when enterprise decision-makers delay IT infrastructure investment — and plenty of them do — security becomes the top-ranked repercussion.[1]

61%

of organizations have delayed an infrastructure refresh over the last five years [1]

#1

Security is the top-ranked repercussion when infrastructure refreshes are delayed [1]

This paper is intended to help bake security into your hybrid cloud infrastructure starting in the data center, and how to build support in the business for doing so. We'll discuss:

- **Reaching across enterprise towers** to make the business case for IT infrastructure security
- **Addressing the basics first** to place on-premises security at the center of your hybrid cloud strategy — from chip to hardware to OS and beyond
- **Recognizing all threats are human**, and answering them with the right technology and processes
- **Doing more than checking the compliance box** to meet regulatory requirements at the pace the business requires
- **Tackling the influx of data** at scale headed your way from IoT, AI and blockchain, while preparing for 5G and quantum
- **Collaborating to elevate security** from proof of concept to production with insights from leaders in hybrid cloud architecture and on-premises security

Register to watch "Secrets of the C-suite: Building a Secure Hybrid Cloud" →

Chapter 2

Reaching across enterprise towers:
Helping decision-makers see the value you see

Imagine wondering aloud to your CEO, "Why do we even need business insurance?" Chances are you know the feeling. Seventy-five percent of IT leaders say they've received significant pushback on IT strategies other than cloud — including investment in data center security.[2]

Creating a business case for data center security built on the facts

The average IT buying committee now has 21 members.[3] So you're familiar with different voices weighing in around the table.

To cut costs, perhaps your C-suite has convinced themselves that cloud is the way to go. Or if the enterprise hasn't had a security issue yet, everything will continue to be fine. Or other stakeholders and their business needs should come first.

This gives you an opportunity: making a business case for IT infrastructure investment based on security. One that proves that the data center is not a cost center, but intrinsic to delivering business growth.

You can start the conversation with the realities of enterprise security.

~60%

of enterprises have had security breaches in the last three years [4]

36%

say it's likely they're being attacked now without knowing it [4]

64%

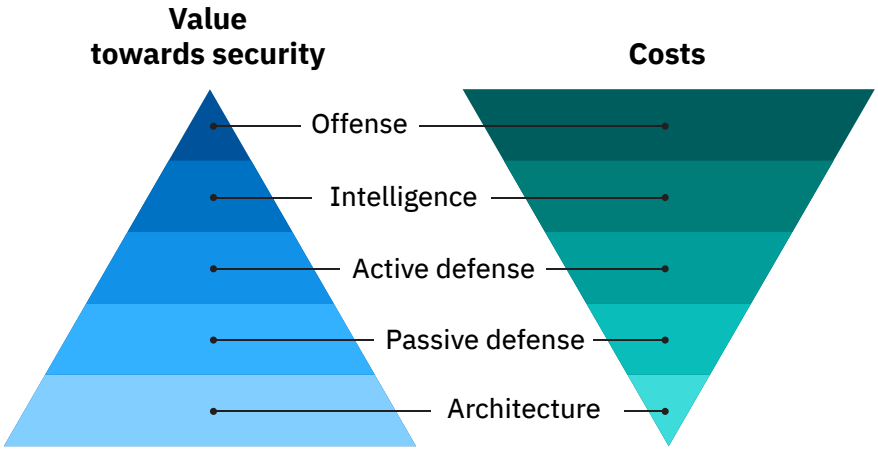
say data breaches are the leading cause of downtime [5]

$1M

is the average cost of hourly downtime for 40% of companies [5]

Even with these numbers, you may face resistance from your peers. They may say that building a secure on-premises infrastructure in a hybrid cloud world takes too much time, effort and money.

But according to a paper by the SANS Institute, investing in architecture — the planning, establishing and upkeep of systems with security in mind — **costs the least and delivers the most value towards security**.



(credit: SANS Institute)

What's more, investment in architecture makes it possible for the other four levels of cyber security — passive defense, active defense, intelligence and offense — to deliver their optimal value.[6]

"...the establishment of a proper Architecture aligned with the organization's needs causes the other (security) categories to become more effective and less costly."

Robert M. Lee
"The Sliding Scale of Cyber Security"
SANS Institute, August 2015

Bridging gaps in the management team

IT leaders can achieve success with a business case by addressing key challenges and priorities of other stakeholders — and by showing how a security-first posture beginning in the data center can benefit everyone.

- **For the C-suite,** your message is clear: without security that extends to every facet of your hybrid cloud strategy, the business is at risk. The business case should demonstrate how to take your recommendation from pilot to production, making infrastructure security the normal course of operations. You will want to address quantifiable returns for the business related to risk avoidance and an analysis of opportunity costs.
- **For Line of Business leaders** – likely to push back with arguments for their needs – the message is similar. The customer experience is everything today. Without investments to protect high value customer data and workloads in the data center and elsewhere, LOBs face losing hard-won customer trust and loyalty.
- **For Security leaders**, they may argue that your focus should be on anything but security. But an on-premises strategy encompassing everything from the latest cryptography to tried-and-true air gapping can make efforts like Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) and others more effective.
- **For Innovation leaders**, your opportunity is to convince them of the value of DevSecureOps. It's true that cloud is an appealing environment to develop and deploy in. But the ability to work inside an infrastructure hardened by design can bring new confidence to both innovation and operations.

Few would ever question the wisdom of having business insurance. With the right business case, the same can be true for a secure infrastructure.

What's Forrester's take on enterprise hybrid cloud security? Find out now →

Chapter 3

Addressing the basics first: Building a secure foundational infrastructure

Picture a two-story home. Upstairs, every window in every room is locked and secure. Downstairs, the front door is wide open.

It's like a hybrid cloud strategy that fails to account for on-premises security.

Cloud providers have proprietary security protocols to protect your data and workloads. And they offer Security Information and Event Management (SIEM) for visibility into their respective clouds.

For collective insights from these different pools of information and to respond to security events, your security teams have most likely added Security Orchestration, Automation and Response (SOAR).

It can look safe and secure — at least from the second floor.

Securing the enterprise from the ground up

Down on the first floor, there's work to be done. To keep pace with the threats you face, modern data center security needs to be built-in from chip to hardware to OS.

Today's rule of thumb in security is, "Be prepared at all times." Statistics from the Ponemon Institute's Cost of a Data Breach 2020 report back this up.

For data breaches due to malicious attacks, it takes:

230 days

to identify [7]

315 days

to contain [7]

In response, enterprises are working to "instrument everything." They're deploying multiple layers of tools to account for the what, where, when and how of threats across the digital landscape — and how to respond.

It's why the National Institute of Science and Technology (NIST), the Payment Card Industry Data Security Standard (PCI DSS) and others advocate for models that address foundational security. And why building hardened security into the data center can make other security efforts that much more effective.

Principles to guide IT infrastructure security

Let's go back to our house analogy. Modern security for the data center is more than locking the front door. It's securing every item in the house with a system that follows them in the house — and everywhere they go.

At rest or in flight, **pervasive encryption** protects data and workloads across your hybrid cloud architecture. This software-based security intelligence is built into the encryption mechanism of hardware solutions.

The result is pervasive encryption at the database, data set or disk level that doesn't require customers to change or adjust applications. Instead, each app has its own encryption-decryption mechanism, so you can apply cryptography without altering the app.

But what about the house's residents and visitors? With thousands of users interacting with on-premises data, the data center also needs a built-in foundational layer of **identity and access management**. That layer can reduce risk through security policies and best practices while providing closed loop, automated security intelligence and threat remediation.

Users, groups and resources are always in flux, making **identity and access governance** crucial as well. Automated systems can simplify provisioning, governance and authorization to protect data and workloads for more secure and seamless experiences.

Learn more about infrastructure security solutions from IBM →

Managing the human element: Accounting for innocent, intentional, internal and external threats

We've all heard that two out of three isn't bad. But in creating a secure hybrid cloud strategy, accounting for only two out of three — people, processes and technology – is a risk.

As an IT leader, you can institute processes and influence decisions on technology. It's people — well-meaning or malicious, inside the enterprise or around the digital world — that will always be the most challenging to manage.

52%

of data breaches are malicious [8]

23%

of data breaches are the result of human error [8]

According to the Cost of a Data Breach 2020 report from the Ponemon Institute, three-quarters of data breaches involve humans — either bad actors or people making mistakes.

On their own, each can be challenging. When the two combine, they can become expensive. With attackers stealing or compromising credentials from innocent people, the average cost of a data breach skyrockets by nearly USD 1 million to USD 4.77 million.[8]

Three reasons why clients are opting for hybrid cloud →

Building a culture of security starts with investment in the data center. Yet investing in managing the human element is vital as well. This is your opportunity to work with leaders across the enterprise in a collective effort to address:

- **Internal threats**. These are your colleagues, and their talents are some of your enterprise's most important assets. Yet well-meaning employees can pose significant threats through easy-to-hack passwords, unauthorized workarounds, connecting to unsecured home routers and even simple mistakes.
- **External threats**. Cyber criminals continue their efforts to profit from stolen data. From 2005 through 2019, there has been a 692% increase in the number of cyberattacks in the U.S., with a 567% increase in the number of records exposed. In Europe, authorities now receive nearly 300 breach notifications each day.[9]
- **Onboarding/offboarding threats**. Many discussions about talent onboarding and offboarding focus on HR and costs to the business. But with the annual employee turnover rate at approximately 15 percent,[10] security is a significant concern as well. As many as 87 percent of employees leave companies with data they created there, and another 28 percent take data created by someone else.[11]
- **Interconnected threats**. Your enterprise extends well beyond its four walls. Partners, vendors, customers, cloud providers — each has a series of human threats to manage as well. A secure hybrid cloud strategy that starts on-premises does more than protect your data and workloads. It promotes security across all digital interactions.

Read: Forrester's insights on hybrid cloud security for the enterprise →

Chapter 5

Doing more than checking the compliance box:
Meeting mandates while keeping pace with the business

The business wants to travel at 100 miles per hour. Compliance says the speed limit is 65. You're on the team that gets to break the news.

No one looks forward to tackling compliance. It can be costly, time-consuming and drain resources. Yet its importance can't be understated. Sixty-six percent of enterprises say that compliance mandates determine the priority of security spending.[12]

66%

of enterprises say compliance mandates are a determining factor in security spending [12]

As the attack surface grows with hybrid cloud, so does the compliance arena. Data privacy expectations of regulators continue to expand. Personal Identifiable Information (PII) has stringent data residency requirements. Mission-critical data flows into clouds of different providers and is shared among business partners.

Meanwhile, you're trying to keep up with the demands of your data privacy officers, your security colleagues, your legal team and others. It's a challenging assignment.

Amplifying security on-premises — and across your hybrid cloud

It's often suggested that "compliance isn't security." But security and compliance can go hand-in-hand with the right on-premises infrastructure — from chip to hardware to OS.

As on-premises data and workloads move into cloud environments, encryption everywhere becomes key. Encryption built-in at the chip level protects data at-rest and in-flight, even as it leaves the platform. Off-platform control access and revocation continue that protection wherever data travels.

An integrated storage strategy enhances security and compliance as well. High-performance digital encryption and traditional tape air gapping add layers of security and help meet data residency requirements.

Compliance tools built into the OS help further. You can improve audit performance and lower costs with enterprise-wide compliance visibility, enforceable standards, automated analysis and simplified administrative tools.

And on the horizon is confidential computing, a new era of security that can improve compliance. Backed by the Confidential Computing Consortium of the Linux Foundation, this new technology extends encryption to data used at the application level. Data that can remain encrypted in use could be a game-changer in helping to meet compliance requirements.

Ensuring compliance without hindering the business

Business will always want to go as fast as it can with continuous innovation and delivery. Yet success can only happen with continuous security, resilience and compliance as well. In the hybrid cloud era, fast, steady and secure is poised to win the race.

How one bank keeps up with its customers while satisfying regulators →

Chapter 6

Tackling the influx of data:
Staying secure as scale explodes

This is what the dawn of a new era feels like. The world first entered the Zettabyte Era in 2012. Today, there are an estimated 59 zettabytes around the world.[13] By 2025, that number is estimated to increase to 175 zettabytes.[14]

59

zettabytes of data, 2020 [13]

175

zettabytes of data, 2025 [14]

The Internet of Things, AI, machine learning, edge computing, blockchain – the world is producing, capturing, analyzing and sharing more data from more sources each day.

Business growth will be predicated on managing this exponential data growth. At the top of that management list is securing it all – at all times, in all places, for all uses.

Staying ahead starts in the data center

Cloud will continue to play a crucial role in helping you extract value from this explosion in data. But enterprise leaders are recognizing the necessity of data center investments to handle what's next.

IT decision-makers believe that more than half of mission-critical workloads, and 47 percent of data-intensive workloads, will run on-premises or in internal private clouds within two years.[15] So it's no surprise that more than eight out of ten organizations plan on increasing investment in IT infrastructure outside of public cloud within two years as well.[15]

Considerations for the road ahead

A data center that is secure by design allows you to project security at scale. It's the foundation for a consistent security posture that can keep pace with all data, services and applications in your hybrid cloud.

As you evaluate vendors for on-premises investment, it's not only what their machines can do today. It's how they're positioned to support security needs for tomorrow as well. Considerations for you and your purchasing committee include:

Building comprehenisve security
How can new and existing IT infrastructure work together to provide security at all layers? How does that create true end-to-end security for data at-rest or in-flight?

Evaluating built-in cryptography
Can data encryption keep up with business requirements? How fast is encryption? How does it impact performance? How does it extend from chip to hardware to OS and beyond?

Determining security portability
What centralized policies protect data and workloads – even as they leave the platform? Can everything be encrypted at once? Can you revoke access off-platform? Can encryption travel between storage solutions from different vendors?

Assessing systems integrity statements
How do vendors plan to find and fix security vulnerabilities as quickly as possible?

Developing a key management strategy
How can vendors help you create best practices to manage encryption lifecycles, replace aging algorithms and prepare for quantum?

Making room for what's coming – securely
What capacity are vendors creating for the zettabytes of today becoming the yottabytes of tomorrow?

Chapter 7

Collaborating to elevate security: Partnering with you from proof of concept to production

With security in the data center as your north star, everyone benefits. And once your decision-makers change their questioning from “Why would we do this?” to “How can we do this?” — IBM can help.

Register to watch “Secrets of the C-suite: Building a Secure Hybrid Cloud” →

Security that leads to resiliency

Security events are bound to happen. It’s how you position the enterprise to respond that matters most.

According to the Ponemon Institute’s Cost of Data Breach 2020 report, detecting and containing a data breach in less than 200 days saved enterprises an average of USD 1.12 million compared to breaches lasting more than 200 days.[16]

$1.12M

average cost savings of containing a breach in less than 200 days vs. more than 200 days[16]

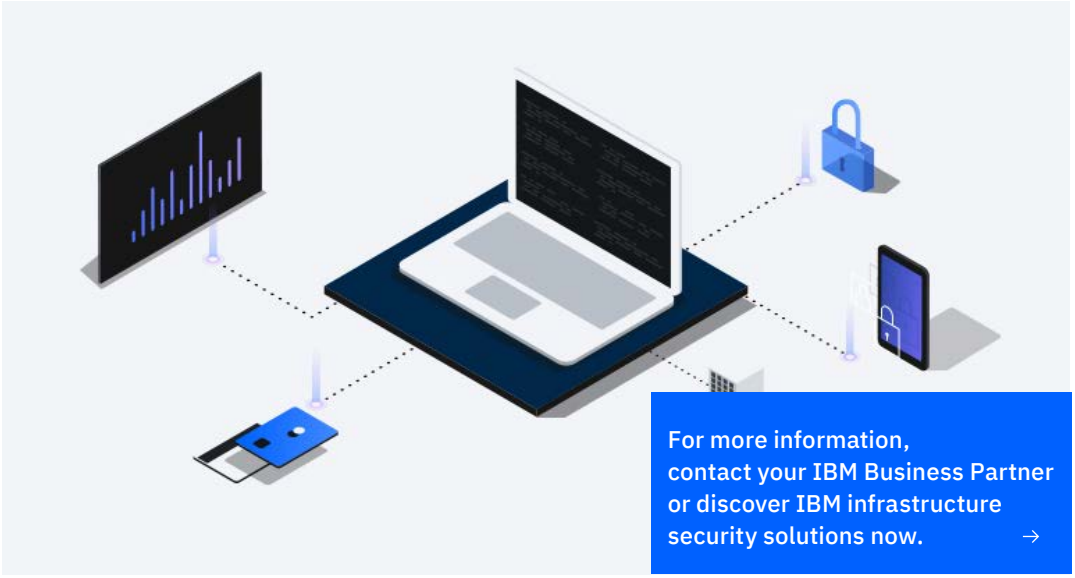
A faster response can start with a more secure on-premises infrastructure. IBM mainframes, servers and storage solutions are engineered to protect data and workloads in the data center and wherever they travel across your hybrid cloud.

But our approach to IT infrastructure security extends beyond our machines. Leveraging the discoveries of IBM Research, IBM IT infrastructure engineers create purpose-built machines with next-generation technology to run your business today. Their work is a large reason why IBM has led all U.S. companies in patents for 27 years running.[17]

The IBM IT infrastructure experience also features:

- IBM Systems Lab Services to help you through the full IT infrastructure lifecycle of strategy and planning, architecture and design, and implementation and optimization.
- IBM Client Experience Centers offering hands-on access to the latest IBM IT infrastructure technology and insights from technical experts using IBM Garage methodologies.
- A variety of technical services including Platform Test Services, Product Engineering Services, Spectrum Computing Services, and Assembly and Test Services to help you determine optimal configurations for your data center tuned to business needs.
- IT Economics Services to provide detailed insights on simplifying operations, reducing IT costs, improving ROI and meeting the demands of the business.

Read: A Spotlight on Security — The Key for Enterprise Hybrid Cloud Strategy from Forrester Consulting →



For more information, contact your IBM Business Partner or discover IBM infrastructure security solutions now. →

References

1-2 “The Key to Enterprise Hybrid Multicloud Strategy”, a commissioned study conducted by Forrester Consulting on behalf of IBM, January 2020.

3 “2019 Role & Influence of the Technology Decision-Maker Research”, IDG, 22 April 2019.

4 Macy Bayern, “Nearly 60% of businesses suffered a data breach in the past 3 years”, TechRepublic, 2 October 2019.

5 “ITIC 2020 Global Server Hardware, Server OS Reliability Report”, Information Technology Intelligence Consulting, April 2020.

6 “The Sliding Scale of Cyber Security”, SANS Institute, August 2015.

7-8 “Cost of a Data Breach 2020”, report independently conducted by the Ponemon Institute, July 2020.

9 “ITIC 2020 Global Server Hardware, Server OS Reliability Report”, Information Technology Intelligence Consulting, April 2020.

10 Anja Zojceska, “HR Metrics: How and Why to Calculate Employee Turnover Rate?”, talentlyft.com, 16 December 2018.

11 Mark Kaelin, “Employee turnover can put corporate data at serious risk”, TechRepublic, 20 February 2018.

12 “IDG Security Priorities Study — Executive Summary”, IDG, 2019.

13 “Information created globally 2010-2024”, statista.com , 7 July 2020.

14 “The Digitization of the World From Edge to Core”, IDC, November 2018.

15 “The Key to Enterprise Hybrid Multicloud Strategy”, a commissioned study conducted by Forrester Consulting on behalf of IBM, January 2020.

16 “Cost of a Data Breach 2020”, report independently conducted by the Ponemon Institute, July 2020.

17 “IBM Tops U.S. Patent List for 2019”, IBM, 14 Jan. 2020.