Seven key Hybrid IT security priorities for 2022 and beyond

Start

FUJITSU

Hybrid IT:

More important than ever. More complex than ever.

Hybrid IT has long been seen as a valuable way to transform and enhance both internal operations and those that intersect with customers.

Over the past decade, it's become clear that organizations across all sectors understand that the capabilities of Hybrid IT are vital to their ability to thrive in our increasingly digital-centric age. And the pandemic accelerated that trend considerably.

A 2020 survey of C-suite executives by McKinsey, revealed that organizations were actively speeding up their existing plans by a factor of seven. They were focused on leveraging the power of a range of digital technologies with cloud migration and Hybrid IT as key priorities. It was as if they'd jumped seven years into the future.[1]

But that has introduced the spectre of complexity. Organizations are, of course, becoming more mature in terms of how they can deploy Hybrid IT and make use of the cloud, but it's clear that there is a downside.

When it comes to cybersecurity, complexity is a threat just as much as the hackers are. Simply, Hybrid IT environments not only exacerbate an organization's existing security challenges but also introduce new obstacles which can endanger it.

1. https://www.consultancy.uk/news/26372/covid-19-has-accelerated-digital-transformation-by-seven-years

So, as organizations enter a new phase of growth, IT leaders face a unique challenge: transform from an operational team that "keeps the lights on" to an engine of continuous innovation and business growth.

Yet while the accelerated digitization mandate is clear, the journey to sustainable success is complex. It's vital that they sustain operational excellence and help drive innovation while, at the same time, empowering business agility and enable future-ready projects to get to market at speed.

At the same time, CISOs are challenged by the escalating compliance demands and complex threat landscape as well as the increasing skills shortage – which makes it harder to speed up innovation and control risk management.

Contents

Priority 1: Coping with an historic increase in cybercrime

As one publication put it, "2021 has been a banner year for cybercriminals, they have taken advantage of the COVID-19 pandemic and the increase in remote work, attacking both technical and social vulnerabilities."[2] From increasingly ingenious methods of online financial fraud to rocketing rates of ransomware on to phishing attacks on every aspect of business especially supply-chains, the world is reeling from a wave of cybercrime. The rapid emergence of organized gangs with villainous names like REvil have become almost weekly occurrences. That's resulted in rising levels of corporate uncertainty and disruption. And that in turn has accelerated the need for even more digital technologies to protect people, data, and things.

The statistics are frightening. There were 93% more reported ransomware attacks, for instance, in the first half of 2021 than in the previous year.[3] Organizations didn't just suffer an interruption to their operations, but the hackers also stole data which they then threatened to make public. They also targeted the main victim's partners, vendors, and customers in a tactic called 'triple extortion.'

2. https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html
3. https://www.computerweekly.com/news/252504676/Ransomware-attacks-increase-dramatically-during-2021

Cybercrime will get worse in 2022. That's an easy prediction to make. The acceleration to the cloud and the use of Hybrid IT means that there will be many more millions of people working from home at least part of the week, more mobile devices with work-sensitive data and applications on them, and an increasing threat surface that's less of a 'surface' than a billion points of vulnerability moving from wi-fi network to wi-fi network. Hackers love moving targets![4]

So, the first priority is the biggest: cope with a tsunami of threats in a coherent, cohesive, and planned way. Accept the fact that nothing is safe, and no one can be trusted without letting fear inhibit your ambitions. Fujitsu's philosophy is simple: with the right planning and preparation coupled with the best technologies - underpinned by focused training and knowledge so that your people understand the threats that are out there - you can move forward with confidence, protect your people and data, and drive your business ambitions.

4. https://medium.com/geekculture/cybersecurity-in-2022-growing-concern-with-greater-opportunity-8a49828e00d5

Priority 2: Don't dig a moat, build a digital perimeter, and train your people

The new world of hybrid working has made the old 'castle and moat' approach to security obsolete. In truth, it's been becoming less effective for at least a decade or more. No organization can dig a moat, build an impenetrable wall, and then focus its defenses on a single gateway. There are no obvious corporate boundaries. You can't distrust everything that is outside, and trust everyone and every device that's inside.

That's why you need to move to a Zero Trust model

It sounds stark, but it's actually a remarkably simple concept. Assume that there will be a breach, and that anything can be compromised, and that no-one is really who they say there are or is acting in a responsible way.

That does not mean that you don't trust your employees, partners, suppliers, or customers – as people. It's actually about knowing who they are, what they are doing, what technology they are using, and what level of authorization they have for each thing they do, every time they do it, wherever they are doing it. The 'perimeter' surrounds their device, connection, and identity. No walls or moats needed.

The Zero Trust approach means that you must design your security from within your organization, not outside. And the technology isn't the point. It's vital, but what's more important is establishing a security mindset that extends from employees to third-parties to customers. Put your security controls close to your devices and train your people to be constantly vigilant and to do the right things every time. The simple truth is that people are the most vulnerable elements in your security. If they click on the wrong thing or are careless about which network they use, your defenses, no matter how elaborate they are, can't work.

Research study – Building a Cyber Smart Culture

Learn more

You can set up a 'cybersecurity mesh' which, by default, distrusts every device which attempts to access your broader network. This means that data, systems, and equipment are treated equally and securely. It doesn't matter where they are located, in your network or outside it. Nothing is trusted until you know it can be trusted.

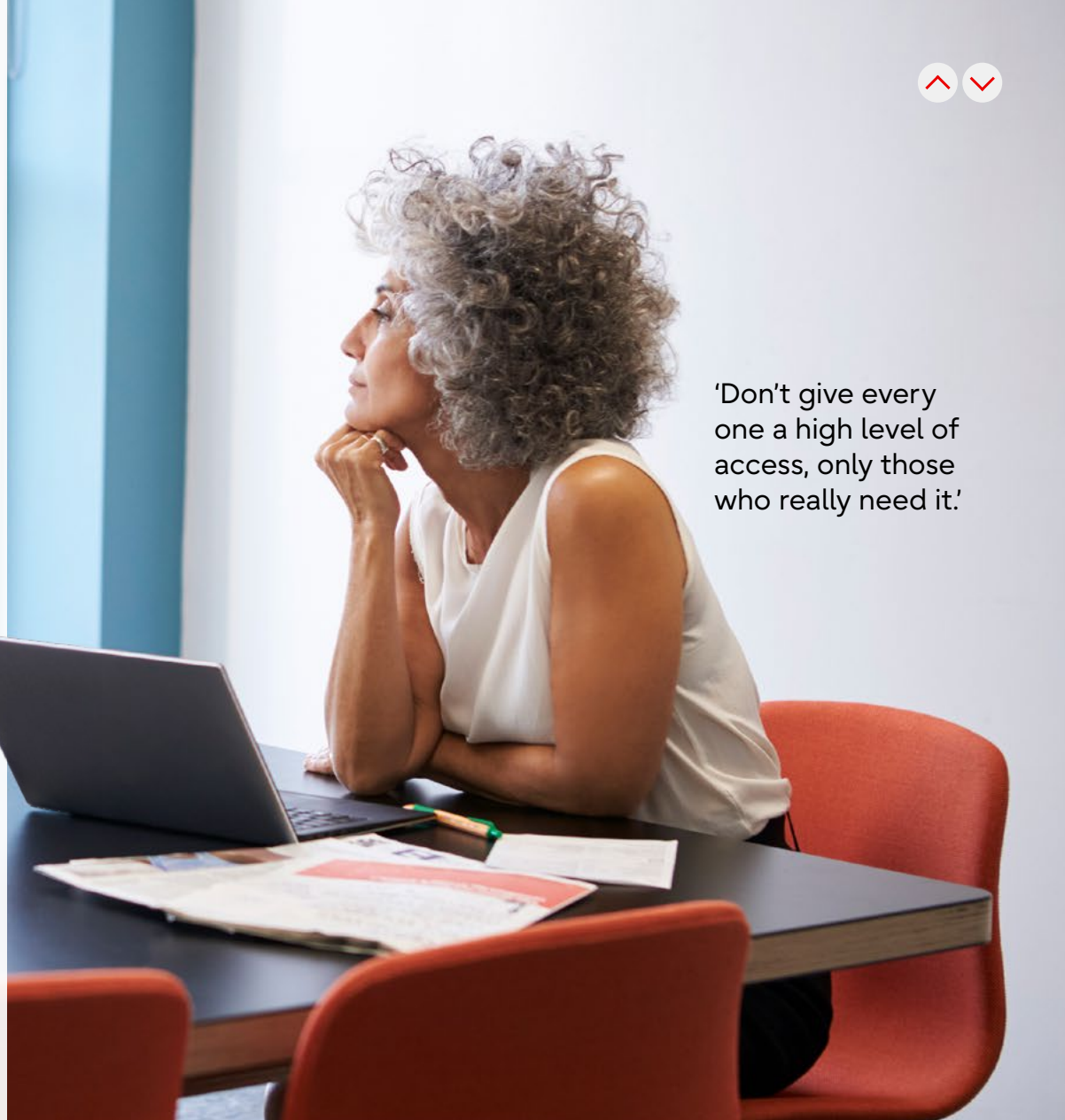
Priority 3: Identify everyone, and limit access to people who really need it

If you're working in a castle with a moat around it, then you know that everyone (and every machine) within the walls of your enclave can be trusted and so you can allow them access to the crown jewels. The new digital perimeter knows no bounds. That's great for agility, efficiency, and innovation but bad for security. One of the key vectors for cybercriminals is to trick employees into handing over the keys to vaults.

In a Zero Trust environment you assume that the person you think is trying to access data or processes is not who they say they are. Now, that sounds like you're adding barriers to seamless operations and connections; you aren't. The point is to create secure sign-on and self-service features that match the needs of each individual and their role.

You allocate access based on specific needs. Then their credentials are also kept safe. Your security policies need to be clear and targeted. Don't give everyone a high level of access, only those who really need it.

Gartner's Hype Cycle for Endpoint Security, 2021 focused on how organizations can achieve their goals while reducing costs and improving visibility and control. The emphasis has to be on 'Unified Endpoint Security' which Gartner says will be a high priority for Chief Information Security Officers (CISO's), CIOs, and cybersecurity teams as they seek to close the gaps in their endpoint infrastructure and avert potential breaches before they happen.



'Don't give every one a high level of access, only those who really need it.'

Priority 4: Govern usage for every user and cloud service

You must establish control over every aspect of your cloud environment and the usage of any cloud applications within your organization. 'Shadow IT' has always been a key threat vector for malicious attacks. A laptop that's not authorized to work on your network, a program that's not sanctioned by your IT team, anything that a user introduces into your organization which, in itself, is dangerous.

The priority for 2022 and beyond is to establish strong governance. That means defining what can and can't be used, and then enforcing your rules. There has been an exponential growth in apps which are attractive to employees because they save them time and hassle. Your security needs to define which are acceptable or, better still, provide equivalent convenience via applications you have vetted and can be sure are secure.

A Cloud Access Security Broker (CASB) service will enable you to do just that. The service can sit within your business or on cloud-based security policy enforcement points and are placed between your employees and the cloud services they use. Simply, they bring together all your rules and enforce them. People can only access what you want them to access. CASB's ensure that authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/ prevention are all carried out when and where they are needed. Fujitsu's CASB covers all of those points, and more.

Priority 5: Manage compliance across your entire cloud environment

The cloud is, by its very nature, ephemeral. That's its strength – it delivers agility, flexibility, and scalability at speed – but it's also a source of threat. The regulatory landscape around everything digital, the protection of personal data as well as intellectual property, has been tightening for the last decade, and is set to become even more stringent. That's good for all of us.

A report in 2019 showed that a massive 81% of US consumers said they needed to trust a brand before they could buy from them, with 55% citing fears for their personal data.[5] The introduction of GDPR by the European Union has concentrated minds across both business and data protection regulators. It's seen as a success by most people, and there are clear signs that regulators have become emboldened and will get tougher in 2022.[6] In 2020, the EU issued over £147 million ($193 million) in fines according to DLA Piper, a law firm.

When a regulator issues a fine, whatever its size, the specific monetary value isn't the point. What counts is trust. In sectors like healthcare or financial services, any kind of fine can undermine trust in the brand and the services provided. That can be fatal in markets which are experiencing disruption from new entrants. So, it's clear that compliance is key to getting value from the investment any organization makes in both the cloud and its security.

Cloud Security Posture Management (CSPM) is a valuable tool for any organization. It's fast becoming a much sought after feature and the size of the market is estimated to be worth $9 billion by 2026.[7] CSPM provides the solutions and services you need to protect your applications, data, networks, endpoints, and any infrastructure that's connected to the cloud. It does it by checking every configuration, policy, and standards violations based on current regulations relating to security and privacy especially of customer data. Simply, it keeps you ahead of current regulations even when they change.

So, if there are any systems which have been misconfigured, or there are weak identity checks, or there have been attempts to hack any application or database, then the CPSM will find it, help you fix it, and then protect it going forward.

5. Edelman Trust Barometer 2019
6. https://www.zdnet.com/article/gdpr-fines-increased-by-40-last-year-and-theyre-about-to-get-a-lot-bigger/
7. https://www.prnewswire.com/news-releases/cloud-security-posture-management-market-worth-9-0-billion-by-2026--exclusive-report-by-marketsandmarkets-301228180.html

Priority 6: Wargame breaches and attacks realistically

You need to go on the offensive. That's what the hackers are doing. They rely on complacency and organizations focusing on agility at the expense of security. Agility is vital, of course, but not if it leaves you vulnerable. Wargaming the future is seen by many to be the best way to understand both the positives and the downsides of cloud.

That's something that most organizations can't do properly on their own. They need a valued (and trusted) security partner to help them set up realistic scenarios, run them, and then learn from the results. A wargame is the simplest and best way to find gaps in your defenses. It's why the military run expensive war games. What you learn in action strengthens your ability to avoid needing to take serious action in the future.

Many cybercrime analysts emphasize the need to 'think like a hacker.' A hacker knows that, in many cases, seemingly stringent security policies are not followed consistently. There's always a weak point – technical or human (usually human) – so a simulated attack is a great way to find them. Working with a Consult & Professional Services provider (like Fujitsu) to deliver Breach & Attack Simulation (BAS) is the best way to test the vulnerabilities you suspect and find those you don't know about.

The attacks can be tailored to specific areas, systems, or even teams, so that you can see how effective your security posture is and where it needs to be strengthened or changed completely. It's important to work with a provider that knows what potential attackers are doing – and what they might do – so that you get as close to a real-world attack as possible.

Priority 7: Optimize and automate cloud security to cope with increasing consumption

The pace of digital transformation across all sectors is accelerating. As mentioned before, COVID has added to the urgency of many businesses' migration to the cloud and boosted consumer adoption of cloud services, but the trend pre-dated the pandemic and will continue long after it's over. One estimate predicts that spending on cloud computing will reach $1.2 trillion by 2028.[8] The full arrival of 5G will see billions of IoT devices added to networks everywhere, while AI will become standard across many applications and services.

That rapid growth in cloud consumption has been accompanied by an equally rapid increase in the number of threats and alerts. The more alerts there are, the more likely it is that they will become routine giving rise to 'alert fatigue.' IT security teams can become overwhelmed and miss the signs of a significant (and dangerous) attack. That's why it's important to use Security Information & Event Management (SIEM) and Security Orchestration, Automation and Responses Services (SOAR).

SIEM enables you to cope with the rising volumes of security alerts which come with increased usage of cloud services. It gives you the ability to see what's happening across the entire range of your IT services and provides the context you need to understand which alerts need urgent action. SIEM works by aggregating data from multiple systems and then analyses it to find anything unusual and might suggest a potential attack is taking place or has happened.

All the alerts are channelled to a central place and then the SIEM intelligently ranks them so that personnel can investigate the most urgent first. Then it's up to the team to act.

SOAR can work in tandem with SIEM, or on its own as it includes some of its features. The significant difference is that SOAR takes the analytics and creates a defined investigation path for each alert and then creates an automated investigation workflow so that by the time one of your team see it there's more information and more potential for swift action. It also means you can fully, or semi automate, responses to threats and reduce the need for manual intervention. That in turn improves Mean Time To Recovery as well as making your cybersecurity team more efficient.

8. https://www.businesswire.com/news/home/20210810005902/en/Global-Cloud-Computing-Market-2021-to-2028---Size-Share-Trends-Analysis-Report---ResearchAndMarkets.com

Fujitsu is well-placed to help you handle all your Hybrid IT security challenges

There are many cybersecurity partners you can work with as you seek to get ahead of the seven priorities I've outlined above. But Fujitsu is extremely well-placed to deliver the solutions and consultancy you need to cope with each of them without slowing down your business.

And that's the crucial point: security should not inhibit your ability to serve customers, achieve value, and drive innovation. Working with the right partners to alleviate the burden of protecting your business and people is an investment in agility, flexibility, productivity, and compliance.

Fujitsu offers you the ability to make the most of the Zero Trust model and make the most of cloud's ubiquitous advantages. We build a perimeter that is both dispersed and inherently secure at every endpoint, protecting each person while allowing them to access what they need to access and are authorized to use. Nothing more, nothing less. Our Identity Management and Access Practice provides a unified and seamless identity user experience which gives you control over passwords and ID's etc, without inhibiting users' ability to be productive.

We have extensive experience in data protection and ensuring compliance with regulations such as GDPR and PCI-DSS, and our consultants help develop effective data security policies, standards, and processes to protect reputation as well as keep you ahead of regulatory evolution.

We offer CASB, CSPM, SIEM, IDAM, BAS and SOAR to achieve all of the security benefits outlined in this Guide. When you work with Fujitsu, you will benefit from a trusted partner which has built on generations of experience to achieve the expertise and vision necessary to not only protect the future but build it too.

To find out more about all our cloud security for Hybrid IT services visit: https://www2.fujitsu.com/global/uvance/hybrid-it/

FUJITSU