Protected foundations

Enabling your adaptive future by creating a resilient, future-proof core.

FUJITSU

Protected foundations enable you to adapt with pace and precision

The organizations that succeed today are adaptive. They are highly responsive and remain relevant in the face of rapidly changing market and customer demands. They do this by optimizing cost and agility, enhancing operational effectiveness, building services faster, and driving insight and new value from data and innovation. But these adaptive characteristics and outcomes can only be achieved if the organization has a resilient core that's not only fit for today's demands, but future-proofed for tomorrow's as well.

At Fujitsu we call this protected foundations.

Collectively, they are the digital infrastructure fundamentals you must deploy and integrate to continuously evolve at pace – and to do so with precision, so that the safety of your data, digital assets, and critical services is never placed at risk as you move forward.

Read on for expert insights, advice, and guidance for creating protected foundations successfully.

Opening thoughts:

Wise organizations build their transformation on solid ground

Stuart Whatmore
Head of Portfolio for Security, Network, and Regulation at Fujitsu

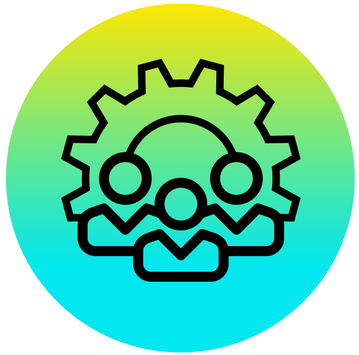
You will have probably heard the famous parable – particularly if you are from the Christian faith – of the 'wise man and the foolish man'. The former built his house on sand, and as a result it wasn't around for long when the storm came. The latter built his house on rock, and it stood firm in the same challenging circumstances.

Whilst this specific 'story' comes from a religious background, its analogy highlights the importance of making well thought through, long-term decisions – particularly those that concern the fundamentals on which you build and grow for the future, and more-so during times which demand resilience and adaptability.

The same thinking, albeit in a business or organizational context, is at the heart of protected foundations.

Often, when we have helped organizations to accelerate change and continously transform, they have been wise from the outset. With trust and reputation so crucial, the importance of their future (and current transitioning) state being built on solid ground is at the forefront of their minds – and we make it reality.

All organizations need to create foundations that address three key requirements:



1. Connect

a distributed evolving landscape of employees, customers, and systems.

2. Protect

data, digital assets, and services to maintain integrity, reputation, and trust.

3. Regulate

a growing range of IT and OT systems to the highest regulatory standards.

In this guide you can explore our expert insights, best-practices, and recommendations for each of these symbiotic areas to help you build and enhance your organization's protected foundations.

1. Connect employees, customers, and systems

We understand that, as you digitally transform, your operational landscapes will become more widely distributed. Not least because your employees need to work collaboratively across larger and more diverse ecosystems – and access IT/OT systems and information from remote locations. But employees are only one driver.

Customer needs will also cause your landscape to disperse further. Not only will they expect to be served increasingly through digital-only or omni-channel services; but Edge-based data processing will also need to proliferate in order to enhance the accessibility, responsiveness, and quality of these, so you can remain competitive and/or valuable.

Under the surface, the increased volume and sprawl of infrastructure, applications, data, and people means that connecting employees and customers to the things they need will be more difficult to master.

Read on for our advice and insights to help you tread carefully towards success.

Giving people timely, flexible, and secure access to data

In the current climate where pace and agility are key, every organization including yours is likely to recognize the benefits of a more autonomous culture – whereby in contrast to traditional models with hierarchical decision-making and bureaucratic processes slowing the organization down, employees are encouraged to be self-sufficient and make key decisions based on insight.

This more democratized approach usually demands democratization (and often decentralization) of data – available with real-time visibility and continuity anytime, anywhere, and across any set of devices. There are two pieces of fundamental best-practice we suggest for making this possible, to enable the desired levels of connectivity and secure accessibility.

The first is a shift towards an internet-first approach to connectivity, whereby relevant systems and data are cloud hosted and accessible via the internet. While this facilitates more effective user access and management, it requires a mindset shift regarding data access and network security. The key shift is moving from 'old-thinking' in terms of deploying traditional security controls such as firewalls around a traditional perimeter (i.e., the data center), towards acknowledging that the endpoint is the new perimeter and that as a result, focus needs to be directed towards enabling secure interactions between the cloud and Edge at network level.

The second is 'central' policy enforcement across your organization and its sites through the implementation of a single software-defined network (SD-WAN). This provides a standardized overlay network, rather than needing to rely on the traditional separate levels of connectivity per 'site' or component which many organizations will be used to. With this, you can control the network and everything that is deployed on top of it in a consistent and controlled manner. And crucially, you can deliver a consistent user experience wherever the user moves and whichever device they are using, to facilitate fast access to data needed for rapid, autonomous, and remote decision making. If any adaptations to the deployment are needed, for example configuration or access rights, SD-WAN enables a 'change once approach', with updates then applied consistently to the relevant users and systems.

Carefully connecting your growing and changing ecosystem

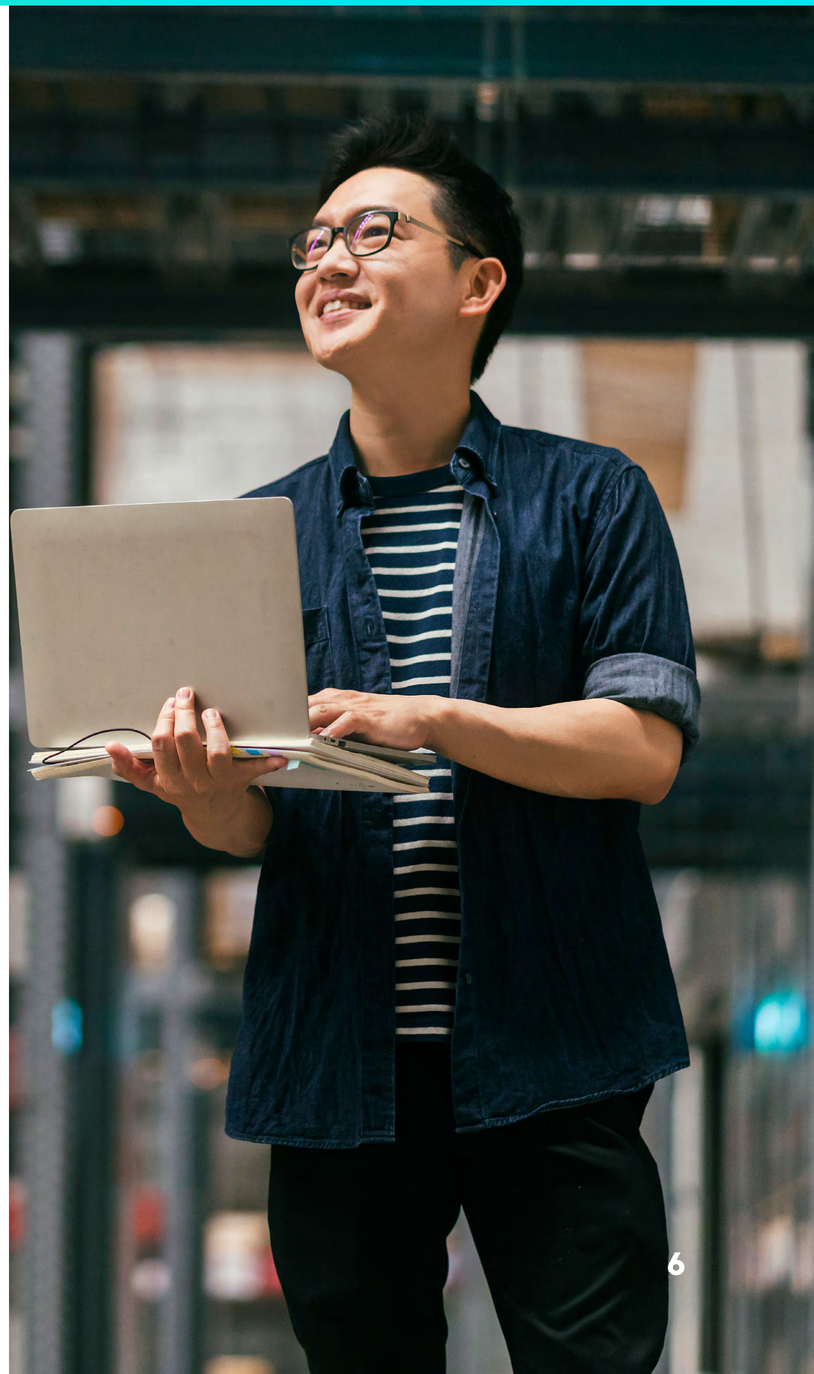
As an organization grows and changes over time, there is a constant push and pull between the flux of change and a workforce that requires access to services at all times to do their jobs well. You are probably experiencing this to some extent already.

Creating better services, products, and experiences with emerging technologies means connectivity requirements increase, and so does the attack surface (but more on that when we explore the topic of 'Protect' later in this guide). Part of the connectivity challenge today is the dizzying number of IoT devices that need to connect across an often hybrid infrastructure.

In the average office environment, previously 'offline' items are now intrinsically linked: door controls, water pumps, heating controls... the list goes on. And that's before we venture outside of the corporate HQ and look at the operational technology (OT) that underpins critical aspects of day-to-day service delivery – and we understand that this is unique to each industry and organization.

Fundamentally, supply chains and manufacturing plants have different OT requirements, constraints, and existing investments to navigate when compared with, say, bank branches, retail stores, and transport networks. Further, with the emergence of the Internet of Everything (IoE), organizations across different industries need to make their OT connect, integrate, and work together.

Keeping control of this rapidly expanding sprawl of technologies is critical to making sure they contribute towards your target outcomes whilst not putting your organization, its services, and reputation at risk. We recommend thorough, regular IT/OT combined assessments to understand and then be able manage your environment as it changes – as even a simple oversight in altering your connectivity design can have surprisingly damaging consequences.



Expert view:

The need for ‘connectivity with care’

Stuart Whatmore
Head of Portfolio for Security, Network, and Regulation at Fujitsu.

It is not uncommon for organizations to find out the hard way about the importance of having the right connectivity mechanisms in place and the right controls around them. It really should go without saying, but connectivity needs to be handled with care. This means fully understanding your organization’s connectivity relationships and the knock-on ramifications of making an adjustment before going ahead.

Of course, there have been high-profile examples of organizations not treading carefully enough. In one recent case, a prominent digital business’ servers went offline in several regions due to a DNS issue. The problem was exacerbated as engineers could not physically access the servers to fix the issue. Why? A recent update of the organization’s OT environment had unwittingly caused the doors to be locked.

If a large organization that delivers a global service and handles sensitive data can have this type of operational oversight, then it demonstrates the need to have the right procedures, measures, and controls in place.

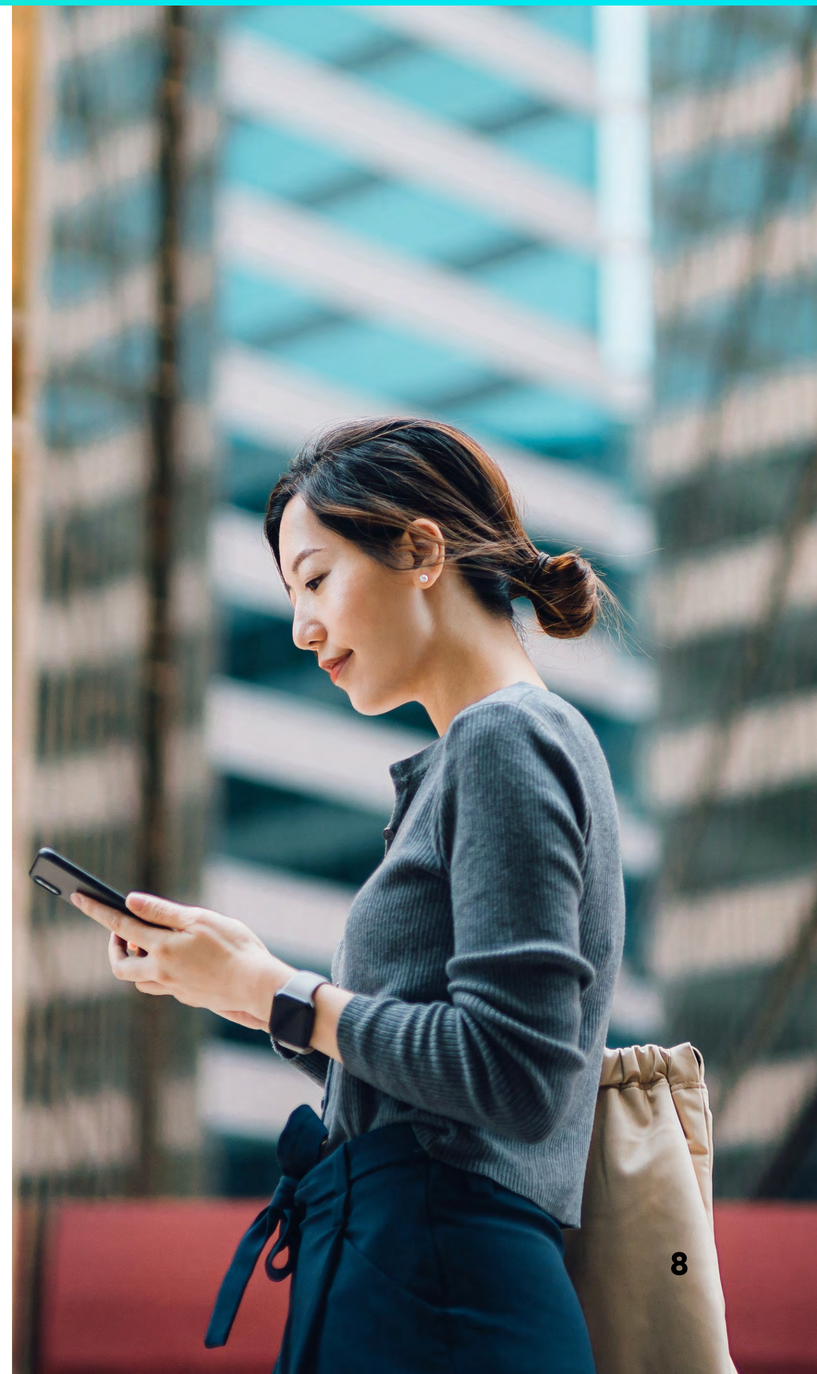
Embracing the Edge in the next era of connectivity

Gartner predicts that Edge computing will grow 75% by 2025, as even more organizations target the move away from centralized data processing to enhance operational speed and product/service value.

This will accelerate further with the maturity of hyperscale platform Edge capability and the rollout of 5G, which will bring ultra-high availability and ultra-low latency to Edge-based solutions.

To take advantage of the benefits of Edge applications and data processing, firstly you need to prioritize connectivity of your core infrastructure environment, which ideally will be cloud or hybrid IT based – with a clear view on where your data is stored and how your various applications, users, and devices need to interact with it.

The second priority is to securely control data and user access to it. Beyond the intelligent network overlay provided by SD-WAN, explored earlier, we recommend controlling network traffic through a secure cloud gateway, particularly if you are looking to move large amounts of data between your core, cloud, and Edge systems using your own private networks. Many organizations are also seeing the benefits of encrypting data at an endpoint, so that it is 'shielded' as it moves through the cloud in either direction.



Case study:

Best-practice examples: Deploying and connecting IoT and Edge platforms – safely and securely

The majority of the IoT and Edge technologies capable of driving improvements in business agility, effectiveness, speed to-market, and new value are no longer 'emerging' – they have existed for some time and are present in many organizations.

But they are now showing their potential because their adoption is moving beyond 'proofs of value' and experimentation. Organizations are getting these technologies into enterprise-grade production – and crucially they are integrating them with existing infrastructure and data environments; ensuring that they are connected, protected, and regulated as they do so.

Some of the organizations we have helped to do this include Proventia, who are using an IoT event processing platform to reduce Transport for London's carbon footprint. They also include Mitsubishi Heavy Industries, who are making the production of aircraft faster and more reliable through real time sensor data and Beam Suntori, who have transformed their stock management of over 1 million products per year.

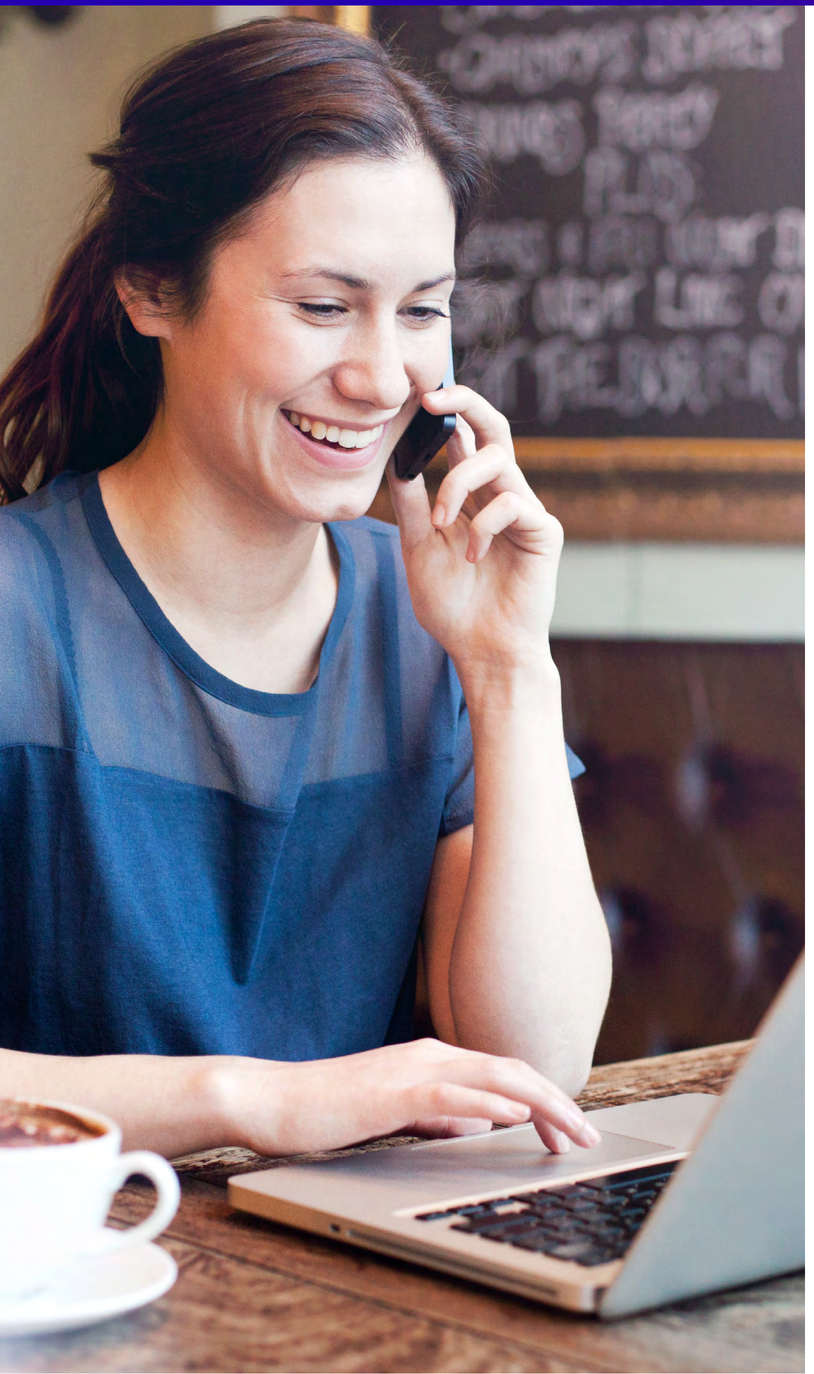
Read more about these cases, above, to see how Edge and IoT technology can be seamlessly adopted and integrated.

2. Protect your data, digital assets, and critical services

The stakes have never been higher for ensuring the security of your data, digital assets, and services. With consumer trust and brand reputation so crucial to your future, you must look beyond your current security measures being fit only for today's challenges. They must be adaptable to external change and the way your organization responds.

Working with our customers, we see two common problems to overcome:

- First, security posture challenges when dealing with an increased attack surface across people, processes, and technology.
- And second, keeping pace with the growing sophistication of cyber-criminal tactics.



Ensuring a future-fit security posture

It has always been important for security leaders to deliver value to the company's bottom line. But new demands are raising the bar much higher for CISOs – and many other key stakeholders.

With the increased velocity, complexity, and business impact of attacks (nowadays possible across a rapidly expanding attack surface thanks to the surge in distributed IT, OT, and users), you should now realize the need for a fundamental rethink of how your security strategy works so that, yes, your security posture ensures that your organization is protected at all times – but also so that your security programs have customer needs and business goals front-of-mind.

You may have initiated this change already, but in this model, security stops being viewed as a constraint of digital transformation, and instead it is allowed to become an enabler for the organization to deliver its products and services – and therefore new or continuous value – in a way that customers will always trust.

Recalibrating and fine-tuning your security thereafter, to create this level of harmony, is complex but at a basic level it can be broken down into its simplest or most abstract components: people, processes, and technology.

Explore these components on the next page

People:

creating a secure culture

Security just being a set of technologies, measures, and policies that your IT department applies to systems and users should be a thing of the past. Creating an employee culture that promotes security as “everyone’s business” is more important than ever – and there’s a key reason why.

It’s because sadly, employees are often the weakest security link – and it’s becoming increasingly evident just how easy it is for even the most savvy end-user to be tricked, persuaded, or cajoled into undermining their organization’s security. The opening of email attachments containing malicious code is, for many organizations, still the doorway for up to 90% of breaches.

Whether they are using such common methods or more sophisticated ones, cyber attackers benefit from a lack of security awareness and untrained employees in the organizations they target. Make sure to train and periodically re-train employees in cyber security and embed a sense of responsibility in every member of your staff.

Processes:

supporting productivity and UX

We touched on the idea of security and transformation needing to have a harmonious and mutually supportive relationship. This is particularly true when we consider processes – firstly because they are key to ensuring convenience and peace-of-mind as equally as important needs for customers – and secondly because security measures that are built to enable a better user experience are more likely to be accepted and adopted by internal users.

You need to target two things – building convenient processes that are secure and continuously enhancing security processes. An example of the former is embedding the secure use of online resources via Cloud Access Security Brokers (CASB) services and secure single sign-on. An example of the latter is implementing clear procedures for security teams to predict, detect, highlight, and respond to emerging threats – underpinned by modern security monitoring tools.

Technology:
the need for multi-layered security

The need to balance target outcomes (like operational agility and competitiveness) with control and regulatory compliance has resulted in many organizations adopting a hybrid infrastructure which is key to connecting a growing number of distributed applications, datasets, and devices across locations.

But this is only the start of how your technology landscape will continue to change. In particular, your future appetite to adopt or scale multi-cloud, composable applications, and emerging technologies will not only mean that the reach of your security strategy will need to be wider, due to the increased attack surface caused; your security programs within your organization will need to continuously develop at the same pace as all of the technology innovation you are implementing, so as not to hamper or undermine your transformation progress. And as you may be discovering, thanks to the advancements in these technologies, single layer and perimeter security has lost much of its power. The solution to this is to employ multi-layered security, intelligence-driven network monitoring, as well a thorough incident response and recovery strategy. While traditional methods, such as firewalls and standard intrusion and prevention systems still have a place as part of this strategy and should not be discarded, these should now be an addition rather than a focus – and those you select will need to be ultra-modern, as only (some of) these have adapted to meet the state of the current security threat landscape.

Expert view:

Security that gives customers the confidence to innovate and grow

Stuart Whatmore
Head of Portfolio for Security, Network, and Regulation at Fujitsu.

Brand reputation is critical for continued growth, and the old cliché rings true here: it takes a long time to build a reputation, but a second to destroy it. You need to keep your organization secure to keep its reputation protected; part of that is making sure you have a high level of data integrity. For this, we recommend working with consultants who can help you understand your specific challenges and threat levels, and then identify and design the right solutions.

A best-practice example of this kind of collaborative approach can be seen at VTT, Finland's largest research and technology company. They partner with Fujitsu to ensure its entire hybrid infrastructure is well managed and that business-critical applications have maximum uptime. Advanced security capabilities are consumed from our state-of-the-art Security Operations Center (SOC) in Finland, which provides VTT with identity services, data loss prevention, encryption, and malware protection. The SOC's advanced threat protection collects, sorts, and analyzes data 24/7 to identify and mitigate potential risks or threats to VTT's day-to-day business.

With confidence in its security posture and data integrity, VTT runs a future-proof collaboration platform, which enables greater employee productivity, satisfaction, and innovation

Read more here.

Staying ahead of rapidly advancing cyber-threats

You don't have to look far to find a cyber security horror story. Aside from the obviously damaging impact on reputation and trust, the financial implications alone are higher than ever. The cost of a headline security breach may reach as high as 10% of most organizations' stock value, which typically equates to millions lost per major security event.

Keeping your organization one step ahead of cybercrime is an ever-expanding task. As cyber-threats become more sophisticated, every organization faces increasing pressure to evolve their tools and techniques to deal with them.

This is exacerbated by the range of potential vulnerabilities that exist within most organizations and, in some cases, a lack of scale when it comes to in-house skills.

One of the key trends you should embrace, and look to build or source capability in, is active threat management – often now referred to as Managed Detection and Response. This is based on the premise that proactively monitoring potential threats, to nullify them before or just as they emerge, is more valuable than passive perimeter security – or at least that both of these methods should be deployed in tandem.

The first key attribute of this is the continuous 360-degree monitoring and trend analysis of the threat landscape. This generates actionable intelligence which allows you to rapidly put protective measures in place, or quickly intercept the security issue before it has had a chance to do any damage.

Another attribute is the ability to identify and prioritize the security threats with the most potential to cause serious harm.
This is important because security incidents can be caused by anything across the business, from patching upgrades and software revisions to shadow IT and end-of-life equipment. As a result, security professionals who, as mentioned, may be in short supply internally have to deal with a deluge of incident alerts.

An extension of this is a crucial third attribute; the capacity to be more automated and AI-enabled. New artificially intelligent tools are capable of spotting potential threats by looking at network activity through the eye of machine learning. As the system takes in the usual traffic flow, it learns to identify and separate routine, legitimate network activity from anything that seems out of the ordinary or like it could be an active security threat.

Of course, building a threat detection and management capability that can discover, learn, improve, and adapt for itself not only enables you to detect and remove in-flight security problems fast; it allows you to prevent their appearance – or that of any look-a-like threats – elsewhere across your organization and then create/iterate repeatable solutions to deal with them. By removing or minimizing the need for human intervention in this way, you can save crucial hours in response time, time which can be the difference between suffering a security breach or not.

Case study: Scottish Water

Proactively protecting critical infrastructure from malware threats

Your organization's ability to identify threats in real time and react to them as quickly as possible can be the difference between maintaining operations and catastrophic failure.

With automated security systems you can improve your ability to fight evolving, intelligent, and aggressive cybercrime, as well as reduce costs and the pressure on overworked security teams.

Speed was a key factor when we kept Scottish Water's operations up after a breach. As the water supplier for two and a half million people, service downtime isn't an option, but after a URL in an email from a known user was opened by an employee, a vicious new malware was released in the IT infrastructure.

Rapid response and action from the Fujitsu SOC using security analytics, enabled it to identify and block the signature of the virus and the host that deployed it, and then clean all devices.

Read more about this best-practice example **here.**

3. Regulate your IT and OT to the highest standards

As data privacy and security become increasingly important for both industry and the wider society, the regulatory landscape continues to evolve in step – often bringing more complexity with it.

Organizations with traditionally very few regulatory obligations now have a growing list of concerns to tackle. Companies are having to find ways to strike a balance between compliance and fast-paced innovation.

On the next few pages we look at the impact of regulatory requirements on data compliance strategies, and how you can be on the front foot with your approach.

Proactively meeting evolving regulatory needs

Failure to meet your regulatory requirements can obviously have severe consequences. As well as the direct financial implications, these regulations may make it mandatory for your organization to disclose information to the public on your security failings, the result of which can be lasting damage to your brand's reputation.

You will know and understand today's regulation but this will continuously change. Gartner research predicts that by 2023, 75% of the world's population will be covered by modern privacy laws, and that by 2024, 80% of global companies will face more modern data privacy and protection requirements. The two main types of regulation will surely always be affected.

Cross industry fundamentals

Monitoring and ensuring readiness of how major cross-industry regulation may evolve is key. The most recent and high-profile example of this was the introduction of GDPR in Europe, and other equivalent or similar regulation brought into effect in other regions. Seeing these shifts not as obstacles but as opportunities to strengthen your data practice and therefore customer trust is one recommendation. Acting on this by seeking to understand and prepare early is key to success.

Industry and geographic requirements

Whether it's local data sovereignty, privacy, or usage laws which are evolving on a more regular basis, ensuring you have local points of presence and data expertise to deal with these is crucial.

So too is ensuring you have a part of your data strategy that is dedicated not only to meeting the changing needs of your industry regulators, but to engage and collaborate with them on a regular basis to build a more trustworthy organization and sustainable industry. In line with this, we recommend carrying out a regular data compliance audit with external data management experts, to ensure that your regulatory strategy – and the measures and technologies you have in place for storing, processing, and sharing data, are up to date and meeting the most recent iteration of standards.

Cloud without compromise?

The case for hybrid and multi-cloud

As data grows, it provides the fuel for driving greater business insight and new value to propel your organization forwards. In our mid-2021 research, over 70% of organizations' business and IT leaders said utilizing data would be key to survival for the next year – and that cloud-hosted data would be a crucial enabler.

But with so many conflicting data requirements on organizations, can cloud alone really meet them all without compromise? Whilst it might not be a new debate, it is certainly one that continues to rage.

On top of their obvious benefits in terms of cost-commercials, agility and scalability, and rich tooling or innovation, hyperscale providers are investing heavily in platform security, governance, and management, which is building the most compelling case yet that a single cloud model can, for some organizations, be all that is needed for the future.

But not yet – particularly for very highly regulated industries or for organizations with data-sensitivity requirements. Our recommendation is still a 'right platform for right workload' approach, which usually involves a tailored hybrid or multi-cloud environment to balance all key requirements, rather than having to compromise on some.

Staying ahead through continuous optimization of regulated systems

As with most things in life, establishing protected foundations isn't simply a case of 'get it done and move on'. It's a continuous undertaking that must be reviewed, optimized, and improved to help you stay ahead of the regulation and security curve at all times, ensuring a safe transformation for your business.

There are a number of factors to consider: new technologies such as automation can make you more efficient and more effective; pressures from customers around sustainability may mean you need to prioritize net zero carbon emissions; and new regulations could be introduced to your industry that require a new solution, fast.

Look at your approach to protected foundations through the lens of continuous optimization, and you can make sure you're evolving in line with the needs of your customers, employees, and industry rather than standing still.

Closing thoughts:

risk-based decision making is crucial to adapt, evolve, and optimize

Stuart Whatmore
Head of Portfolio for Security, Network, and Regulation at Fujitsu.

Today, perhaps more than ever, your organization needs to work with risk based decision making each time it evolves or incorporates something new. That means understanding the risks that change initiatives pose and whether the business benefit outweighs the 'cost' of managing them. For example, enabling your employees to work from home or any other location – which was a huge recent shift for many – involves a greater risk that devices will be infiltrated and used to access the corporate network.

Yet with this example, it's hard to ignore the finding that the organizations which established remote working and implemented measures to manage the security risks have seen less disruption compared to those who were unable to – plus they've strengthened their business resilience.

In other words, a risk-based approach enables clear, fact-driven decision making based on the best outcome for your company. As such, decisions must take into account the technology, people, and processes involved in your organization. Now that dispersed workforces and remote customers have become central to our future, the most successful organizations will adapt to protect their revenue and reputation for the long term.

And just as importantly, they will do this while being able to create outstanding operations and digital experiences that set them apart.

Five key actions for protecting foundations now

Ensuring your business is fully protected and secure is a complex undertaking, but to start here are key actions you can take.

Fujitsu provides a fusion of technology, people, and process expertise to help you secure your organization with confidence.

1 **Take stock.** What is your level of connectivity? Where are your vulnerabilities? Do you understand your compliance obligations? To move forward you need a realistic assessment of where you are.

2 **Embrace next-generation connectivity.** Improve collaboration across your organization, and outside of it, by taking advantage of new developments like Edge, blockchain, and 5G.

3 **Educate your workforce.** People are the biggest security challenge. Teaching them what to look out for and how to raise the alarm will significantly reduce your risk profile.

4 **Don't risk compliance.** With huge potential costs of non-compliance, involve all stakeholders including legal to make sure you meet industry standards.

5 **Find an experienced, scalable partner.** Get consultative and engineering support, specialist skills on demand and at scale, and use latest technologies to keep your foundations resilient and ready for transformation.

The bigger picture:

Creating your adaptive organization

Protecting your foundations is just one crucial component of creating your adaptive organization of tomorrow. There are four other important areas for continuous transformation which allow you to build resilience, responsiveness, and relevance for the future:

Protected foundations

For a safe and secure digitally-enabled business

Optimize cost and agility

For efficiency today and flexibility for the future

Enhance effectiveness

For intelligent decisions and rapid action

Build services faster

For delighting customer experiences and disrupting competitors

Drive insight and new value

For business, consumers, and societal good

FUJITSU

Accelerate and evolve holistically with Fujitsu

Every business has the potential to become an agile, adaptable, and thriving entity. With the support, expertise, and experience of Fujitsu, you can turn that potential into reality.

Get in touch and get started at www.fujitsu.com/global/services/ao

Fujitsu

Tel: +44 (0) 123 579 771
Email: ask.fujitsu@uk.fujitsu.com
fujitsu.com/global