

Digital & Physical Security Infrastructure

THE IMPLICATIONS FOR YOUR
FLEX-SPACE PORTFOLIO



essensys
we power ambition

Executive Summary

With as-a-service models increasing across all industries, companies of all sizes have moved to cloud-based applications, making their work available from any location. When working from the office, they need safe internet connectivity to access their applications securely.

If not private and secure, sharing across the cloud makes malignant access to commercial and confidential information easy for hackers and opportunists. The odds of a brand shattering security breach are higher if the right measures aren't in place.

A gap in enterprise-grade technology – that is, no infrastructure or protocols in

place for privacy, compliance or security within the network – is a deal-breaker for today's occupiers. It's about more than attracting and retaining customers; it's about preserving brand reputation and mitigating risks.

As more companies look to flex as a long-term real estate strategy, having the right tools and partners in place can foster trust with your tenants and safeguard your proposition. Understanding and acting on the critical components of security infrastructure is vital.

In this eBook, we outline the core components for a secure tech operating model that reassures the integrity of your space, operation and infrastructure.

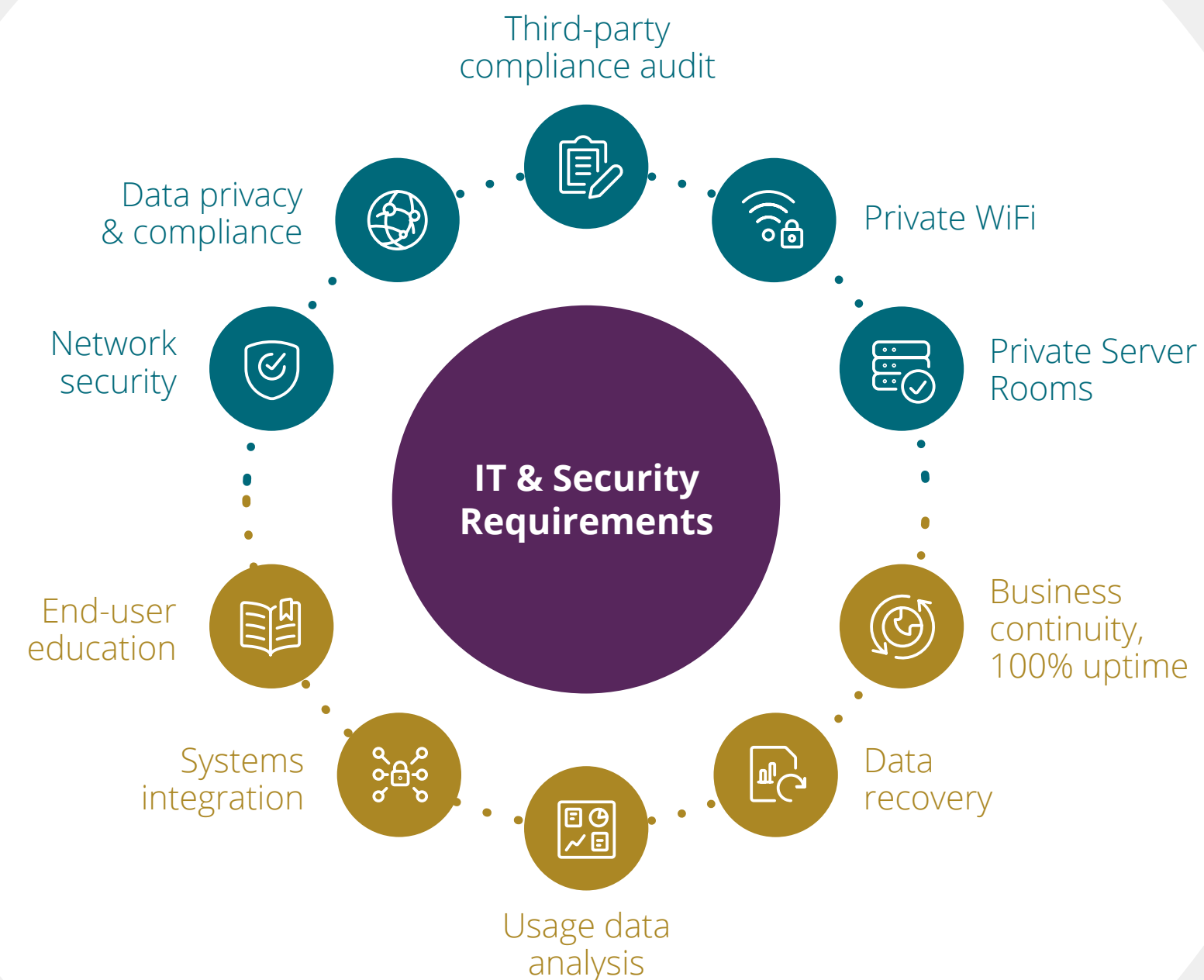


1-2	VARYING TENANT REQUIREMENTS	10-11	SOURCING CLOUD INFRASTRUCTURE • DIY • Outsource to multiple vendors • Purpose-built, enterprise-grade network solution
3	NOT ALL RISKS ARE APPARENT	12	BALANCING SECURITY & OCCUPIER EXPERIENCE
4	AVOIDING SECURITY BREACHES	13	THE EDUCATION PROCESS
5-8	HIERARCHY OF SECURITY NEEDS • Physical Security • Network Security • Cyber Security	14	WORKING WITH A PARTNER
9	TESTING	15	INVESTING IN SECURITY INFRASTRUCTURE

Varying Tenant Requirements

While enterprise tenants tend to be the most demanding, size isn't always the determining factor when it comes to strict IT and security requirements. For example, a startup may be growing quickly and need more tech as they scale. The pandemic has changed how enterprise companies think about their HQ. They may take multiple floors or smaller spaces across various locations.

Occupiers requirements have become more sophisticated when it comes to technology infrastructure & security.



Varying Tenant Requirements

Companies of all size can be subject to differing regulatory and governance requirements. For example, PCI-DSS for companies that handle payments, HIPPA for companies that handle personal medical data, or financial and fintech firms which will have stringent requirements. Many will also need to conform to generic security certifications such as **ISO27001** and **SOC2**.

When it comes to security, it isn't easy to quickly put infrastructure in place, react on the spot or retrofit tech requirements. Plan from day one for the most complex tenant. Think about security early so you have the confidence to support any customer that walks through the door with the foundation in place to meet their checklist of requirements.



SOC 2

is a compliance requirement for service providers & SaaS companies to ensure the security, confidentiality, processing integrity, availability & privacy of customer data



ISO27001

is an international standard for managing risks of information security management

Not All Risks are Apparent

Security risks are not always visible, but that doesn't mean they aren't there. Security comes in layers. Layers are beneficial because they help keep perpetrators out. As an example, if you live in a gated community, you still lock your front door.

Greater visibility into your operations, systems and data helps to identify vulnerabilities, lack of compliance and risks across your operation. If your business is strictly regulated, you could incur fees until any noncompliance is corrected.

As a space provider, you're responsible for ensuring that your space and infrastructure are safe from possible breaches and that account numbers and

other sensitive client data are safely stored. Your tenants may hold you liable for compliance, disclosures, and privacy requirements. You need to know how and where data is stored, how it's managed, who has access to it, and what protocols are in place for it - whether lock and key or firewalls and limited permissions.

Managing multiple systems and tools can be a risk. Having a single repository for data, processes and customer management minimizes the need to login to different systems to add or remove a user or restrict access or services. Consolidating data to reduce touchpoints to as few as possible makes it easier to ensure



essensys

optimum security. Administer individual logins to your network from a single platform, making it easy to enable and disable services. It restricts access to only those you grant it to and minimizes the attack surface of your operation.



LEARN MORE ABOUT **RISK PROFILES & SECURITY THREATS**



Avoiding Security Breaches

You won't know the impact of a security breach on your business until it happens, and it's better not to go down that road. According to **IBM**, the global average cost of a security breach in 2020 was \$3.8M. While the cost varies per industry, the biggest hit is to lost business and brand reputation, not to mention the time and operational resources to correct the damage.

Large-scale high-tech breaches are devastating, but low-tech breaches can also be jarring, disruptive and an operational distraction. Events as simple as human error, an intruder stealing your receptionist's laptop, or using a shared Wi-Fi network have the potential to seriously impact your operation. A security breach, large or small, can create a knock-on effect for your customers that can quickly escalate depending on the scale of your business, making it difficult to contain and recover from.

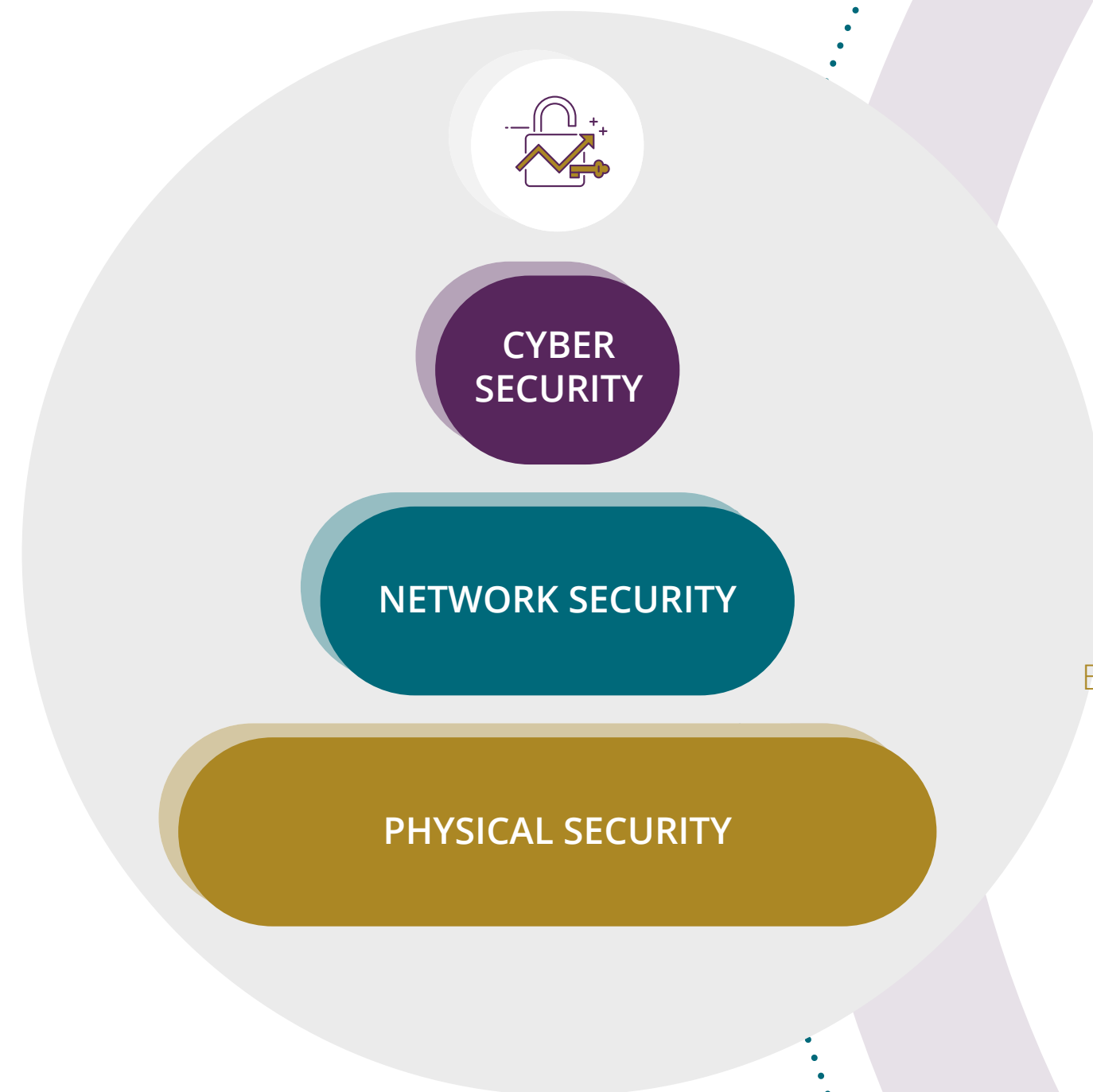
Malicious attacks are the most common and expensive type of security breach. Compromised credentials and cloud misconfigurations caused 19% of malicious breaches in 2020. After a security breach occurs, it is too late to remedy the problem. The only full-proof way to avoid them is to prevent them with proactive measures.

The global average cost of a security breach in 2020 was **\$3.8M**

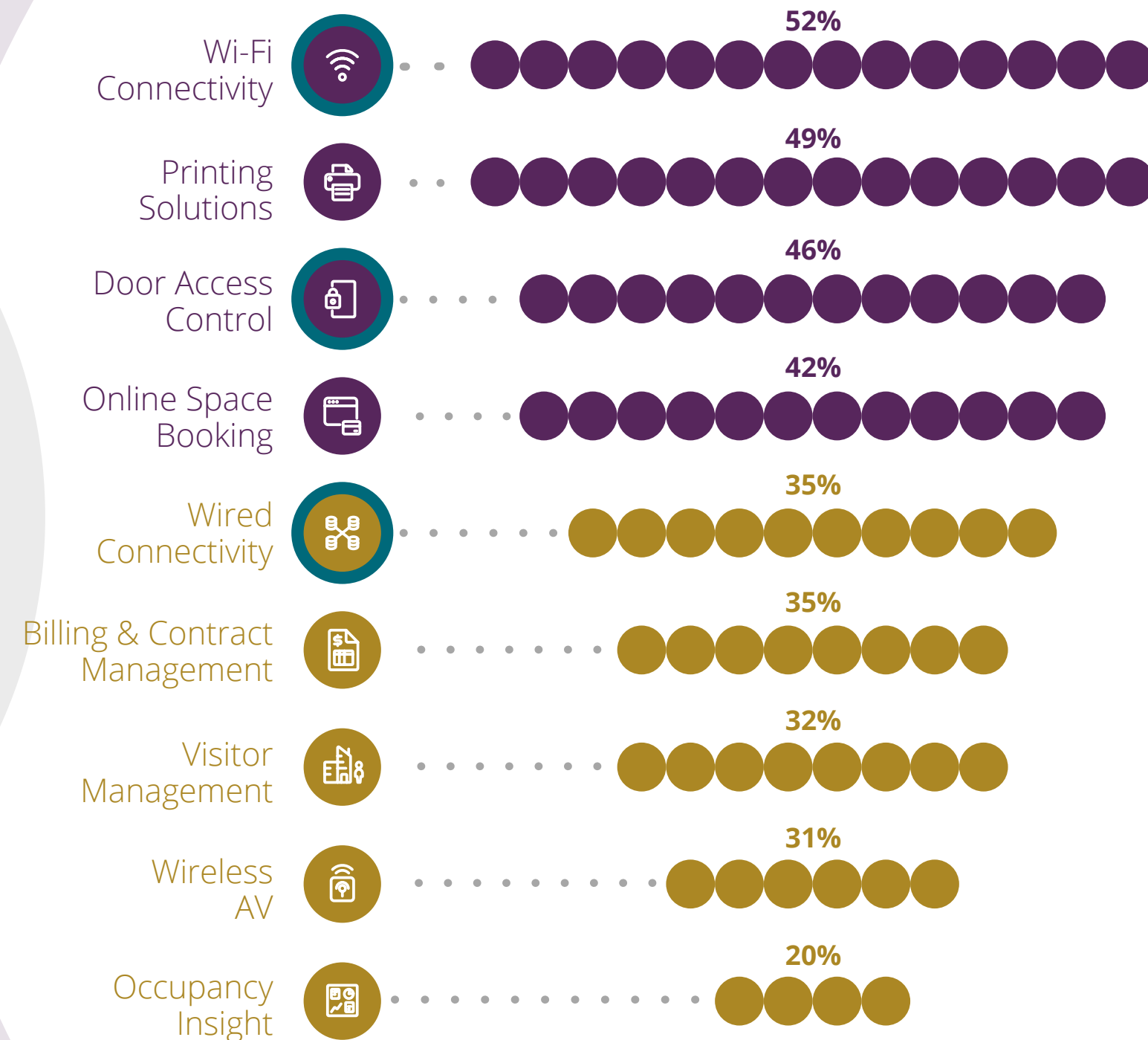
19% of malicious breaches were caused by compromised credentials & cloud misconfigurations

Hierarchy of Security Needs

Tech and security can be abstract but taking a measured and phased approach can help bring your strategy to life. In research conducted by Instant Offices and essensys, we found common pain points in a flex-space operation that overlap with security challenges. For example, how you approach security infrastructure can alleviate common challenges with Wi-Fi and wired connectivity, door access and network access.



HIERARCHY OF NEEDS



FLEX-SPACE INDUSTRY PAIN POINTS

Physical Security

Physical security is the absolute foundation for any security policy. How are you securing and managing access to the outermost perimeter of your space or building?

Door access control is more than giving occupiers a means to unlock a door or access a space. It can enable user tracking and visitor management, two increasingly important elements to your operation as re-occupancy becomes a priority focus. Smart access is also about when people are entering and using the space. Scheduling building access where appropriate offers an added layer of security.

When granting access to the building, to the workspace, and to meeting rooms, consider if the process is seamless for the customer, secure for the business, and tracked to capture revenues.

From a network perspective, it's critical to protect your infrastructure investment by making sure access to the IT or comms room is restricted from unauthorized users and that WAPs (wireless access points) are secured and physically out of reach to prevent tampering and theft.

WORKSPACE ACCESS:



Seamless for the customer



Secure for the business



Trackable for insight



LEARN MORE ABOUT SMART ACCESS CONTROL



Network Security

When it comes to network security, processes and solutions should be in place to protect the platform from any attacks. This includes having visibility and control over the range of devices connected to your network, and managing and monitoring wired, wireless and guest network logins around the clock.

Secure Wi-Fi networks encrypt and authorize access based on specific and individual usernames and passwords rather than issuing a shared password common for WPA networks. This provides insight into who is on your network and helps create a footprint of activity to prevent unwanted risks. Per-user credentials also prevents the need to change a shared password for all users when one person leaves – whether a staff member or an occupier. The alternative is to not change the password and risk that person still having access to the network and system.



essensys



Traffic must be appropriately encrypted and segregated by tenant with dedicated VLANs and blocked inter-VLAN traffic. Firewalls are essential to protect the infrastructure. Implementing VLANs and firewalls is to create virtual Trust Boundaries, a technical cloud-computing term for borders between program data or systems that indicate a change between trusted and untrusted sources.



LEARN MORE ABOUT NETWORK SECURITY

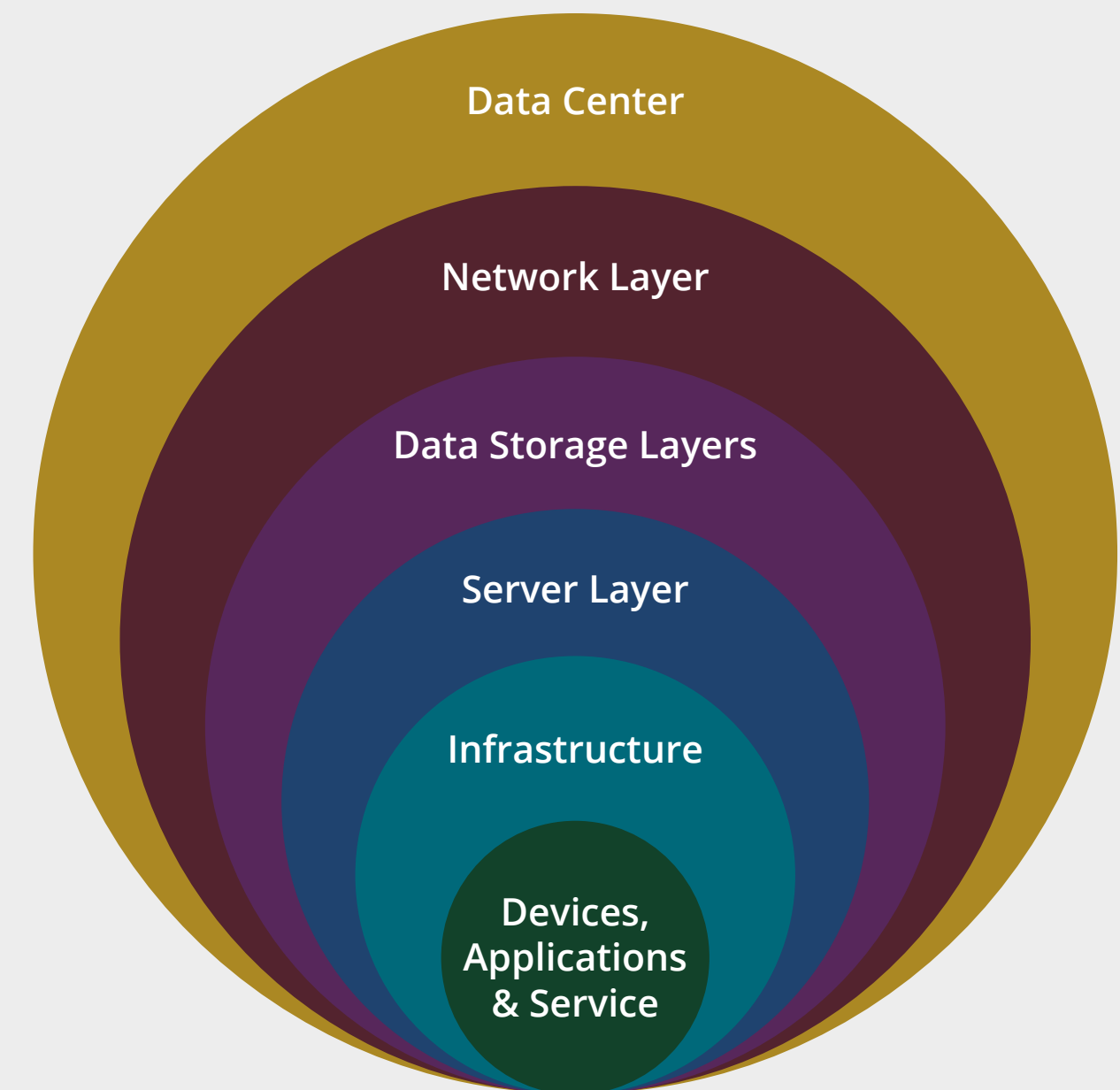


Cyber Security

Are you prioritizing this critical yet often left behind component of security infrastructure? From malware and payment processing to compliance and phishing attacks, cybersecurity is a moving target if you don't have a framework in place to manage the invisible threats in today's increasingly digital world.

Cybersecurity is about protecting data and the systems used to process & store that data. It is all-encompassing in that it comprises network, application, data, cloud, & infrastructure security in addition to disaster recovery and business continuity planning.

Start by understanding which components and systems in your operation are vulnerable to attacks. Take steps to protect and monitor any possible weaknesses. Best practices include keeping cable patching and switch port configurations up to date to prevent risks to connected devices; firewalling and VLAN segregation to prevent targeted cyber-attacks on tenants on the same infrastructure; real-time protocol monitoring to contain and identify compromised devices.



LAYERS OF NETWORK INFRASTRUCTURE

An enterprise network solution is designed with the hardware, software, configuration and management components to support speed and security requirements of tenants across your portfolio.

Testing

We've driven home just how critical it is to implement a wide range of security layers and infrastructure. It is equally important to consistently test the infrastructure and processes in place to ensure they are effective. For example, regular pen testing (short for penetration testing) is the practice of running simulated attacks against your system to check for vulnerabilities. This can be conducted within your organization, but is often more effective when performed by a third-party who specializes in this area – they will have the best skill set and will have the most up-to-date security knowledge.



Another aspect of this is auditing your controls. This could include scheduling time to regularly review user accounts for your key systems or access control permissions. As staff or users come and go, these accounts can sometimes be neglected and leave access to your systems open to people who should no longer have it.

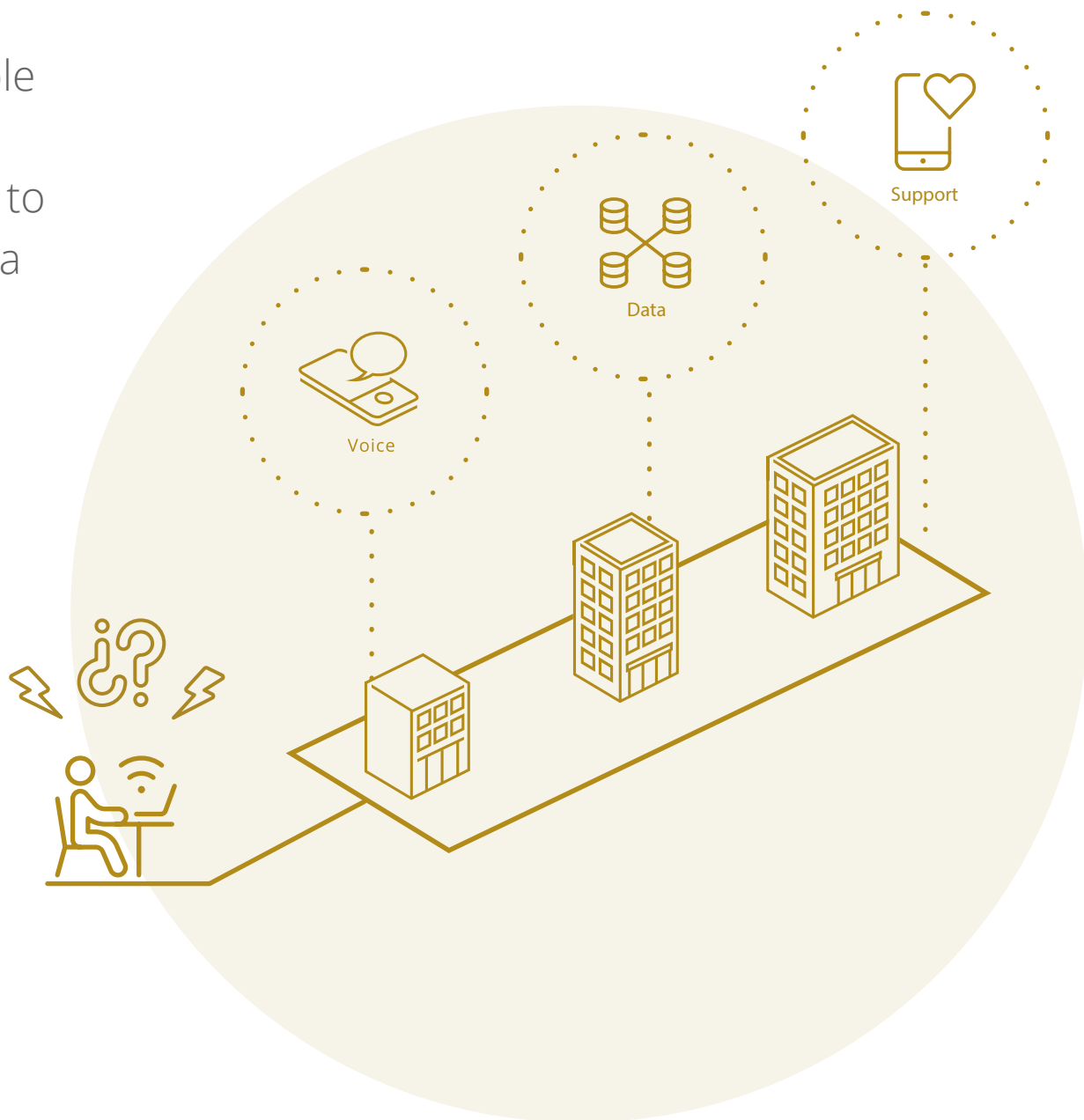
Sourcing Cloud Infrastructure

Your cloud infrastructure strategy, how you connect your business and services to the internet, will determine how safe and reliable your proposition is and it can affect your ability to attract and retain occupiers. Putting critical cloud infrastructure, private network platforms and security processes in place can be an investment but it is the ultimate insurance policy for your portfolio.

THERE ARE A FEW WAYS:

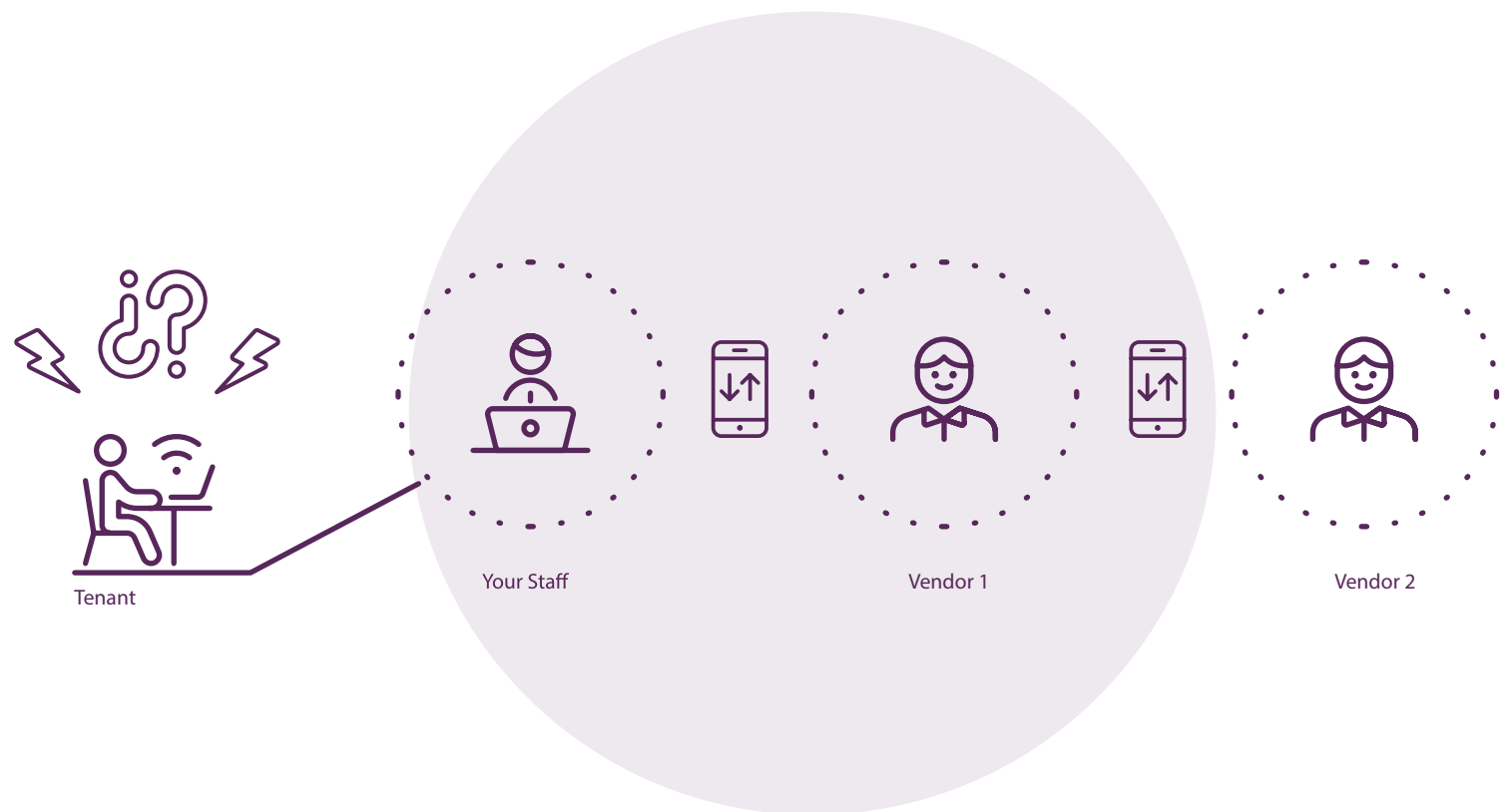
1 Do it yourself - DIY

Cobbling together multiple disparate systems limits the control and flexibility to offer tailored services to a wide range of occupiers. A DIY model is complex and doesn't scale; it can be a strain on your staff, it limits quick customer onboarding and seamless service delivery, and cannot guarantee a consistent, productive tenant experience.



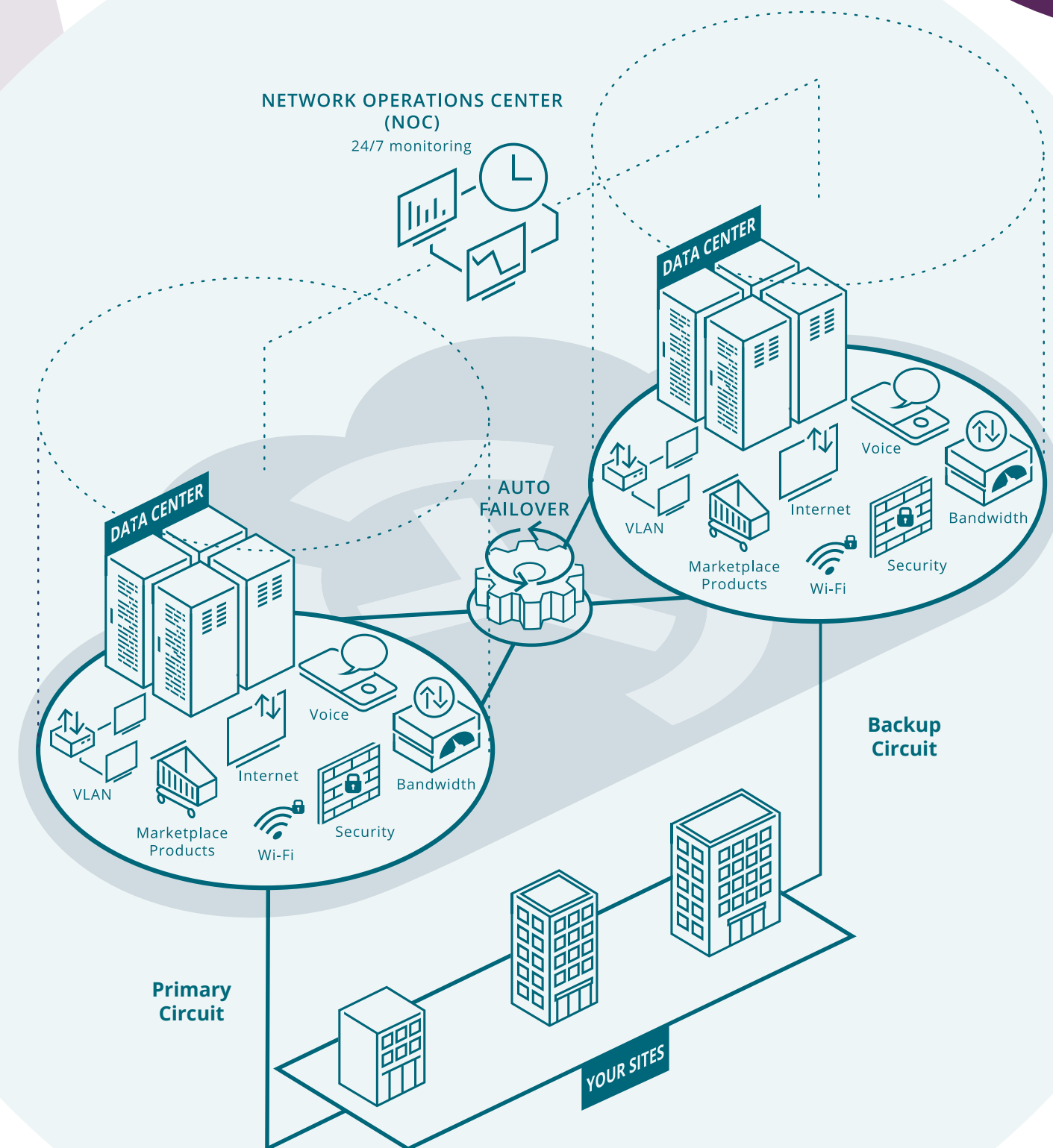
2 Outsource to Multiple Vendors

Like DIY, an outsourced approach to connectivity services means relying on multiple vendors, limiting the ability to tailor services to customers, streamline service delivery and support, and scale the operation. It puts you at the mercy of a queued ticketing system, unpredictable costs, long wait times, and limited control over services and the occupier experience.



3 Purpose-built, enterprise-grade

Software overlaid on a secure private network and resilient cloud infrastructure designed for flexible and multi-tenanted portfolios gives you control and flexibility over shared, dedicated and custom tech services. It's an enterprise-grade solution that confidently meets the security needs of all businesses while safeguarding your operation, ensuring effective service delivery, and facilitating scale.



Balancing Security & Occupier Experience

Making space and service access simple and frictionless for customers is essential. Anything from printing and adding devices to door access and logging onto Wi-Fi can make or break productivity and a seamless experience. Your tenants will have to interact with the space and at some point, touch the security boundary – think adding a device like a printer, Alexa or a Sonos speaker. The fewer systems and touchpoints in the process, the simpler it is to bring new devices onto the network with minimal friction.

In a post-pandemic office market, there's a renewed focus on making the space a safe place that supports good health and wellbeing. Technology can help to monitor re-occupancy and track user behavior throughout your portfolio. Tools such as smart access control systems and remote desk-booking minimize touchpoints throughout an office, making it a more comfortable experience for employees.



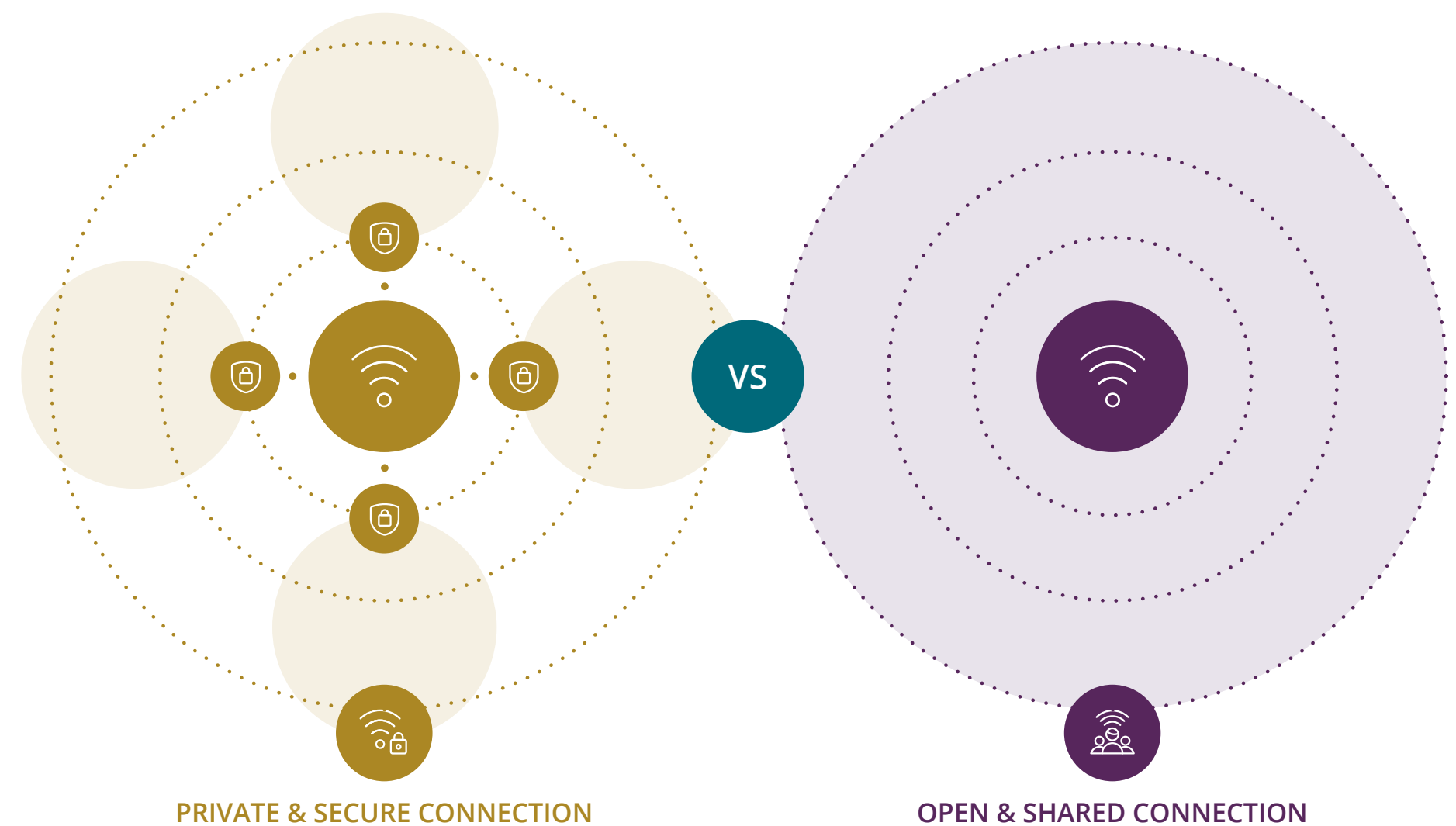
• The Education Process

Some occupiers that are new to flexible office don't realize there are significant differences and implications for security when they connect to a network. Connecting to Wi-Fi at a coffee shop is not the same as the Wi-Fi at a flexible workspace with proper infrastructure in place. Other occupiers have specific needs dictated by their HQ or compliance departments, such as bringing their own equipment or network.

Having scalable and secure network infrastructure in place better positions you to be flexible on-demand, removing the need for prospects and customers to re-invest in technology upfront, especially if they're leaving a traditional office behind. Taking prospects and customers through this educational process garners trust and adds value to your proposition.

Security infrastructure is not visibly apparent in any space and it can be quite complicated behind the scenes, and therefore difficult to explain to a customer or prospect. But it's advantageous for your brand integrity to educate them about the value of security and how you approach it. Communicating your tech infrastructure and security specifications in your marketing material and sales conversations can help broaden the appeal of your space, offer reassurance in your product and even shorten the sales cycle.

Encouraging smart behavior among staff and members is crucial. Security is a process, not a product. You could have the most comprehensive, enterprise-grade infrastructure on the market, but if you stick a post-it with your username and password to the system on your monitor, it defeats the purpose of investing in the infrastructure.



Buying Into a Proven Software & Technology Stack Partner

Working with solutions that are designed and built to compliance, security and infrastructure requirements can keep your business safe. If your business is highly regulated, your customers have strict requirements, or your ambition is to scale, a trusted, and mature solution will include critical infrastructure components like security and connectivity to safeguard your proposition. Such platforms bring sophistication and maturity to your operation and are a value-add to your customers.

Technology is a critical component to enabling productive and safe occupier

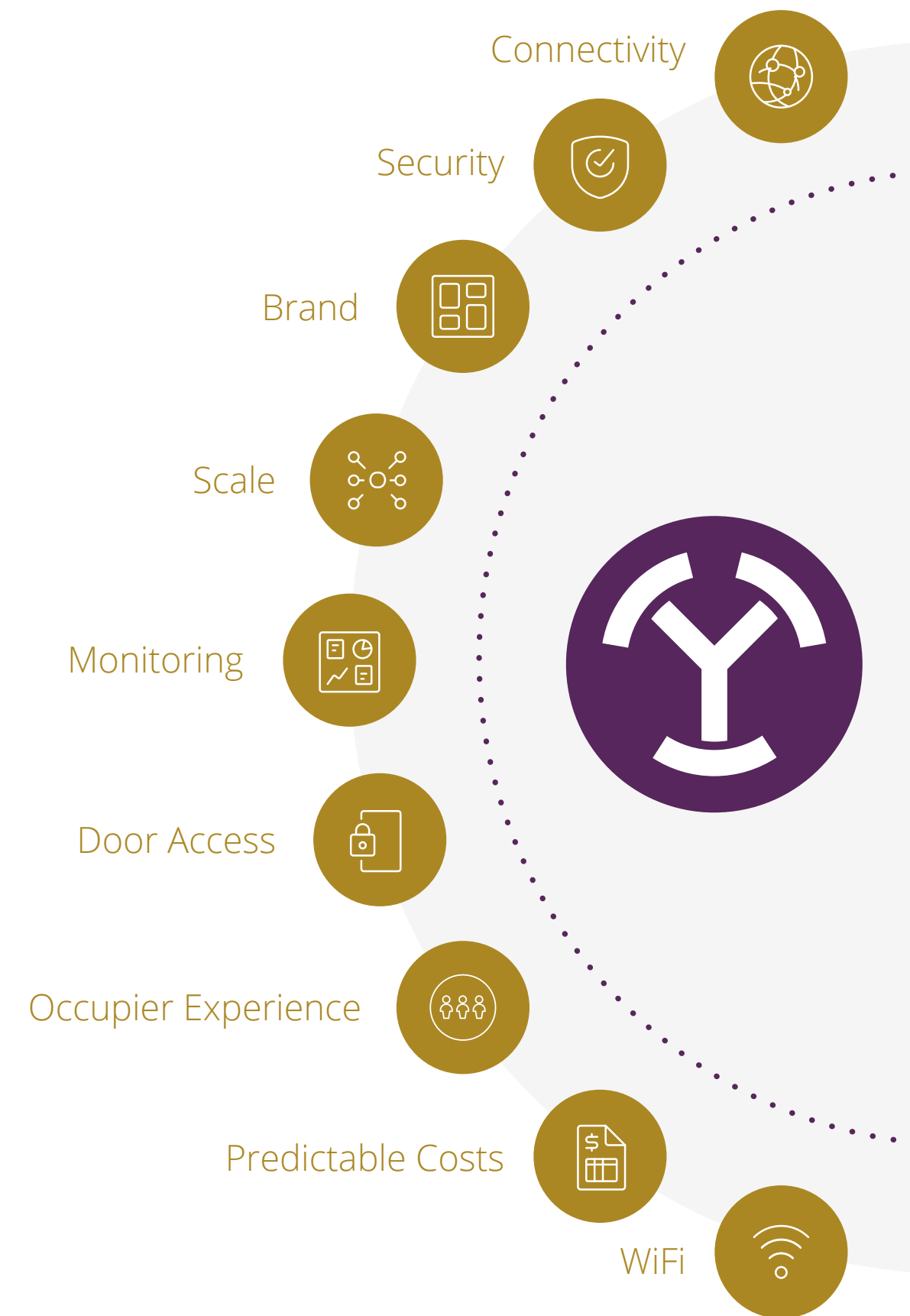
experiences in the office, but it can get complicated. Get back to basics. Your function as a space provider is to build and deliver workspace and services to occupiers, not to deal with the nitty-gritty of technology. Adopting a software and technology solution that incorporates the full tech stack,



will lift the burden of technology from your shoulders and keep you aligned with industry standards and compliance requirements.

Investing and re-investing in infrastructure platforms and updating systems is a strenuous and complex task that requires diligence, expertise and on-going costs. Offloading that burden by using a proven solution can benefit your operation. Demonstrating to customers that your technology and theirs are robust creates peace of mind that their data, payments and services are sound.

essensys



Investing in Security Infrastructure



There aren't many shortcuts you can take when it comes to reliable security technology and infrastructure. A tech operating model that can support varying IT requirements and companies of all sizes is undoubtedly an investment, one that you can't skimp on if you want to get it right from day one. But it offers beneficial results to you and your customers and can ultimately deliver on your long-term ambitions. A proper tech investment ensures secure and reliable services, efficient scalability, operational simplicity reduced risk, and long-term trust in your proposition.

MISSION-CRITICAL SOFTWARE FOR THE FLEXIBLE WORKSPACE INDUSTRY.

At essensys, we work extensively with landlords and operators globally, providing them with the technology they need to successfully enable premium occupier experiences in flexible office environments.

Born from our unique first-hand industry experience, we empower ambitious operators to accelerate their growth. Our secure platform combines technology, infrastructure and operational processes into a simple, efficient and easy to manage service experience. At the touch of a button you have complete control of your business, allowing you to deliver amazing experiences while gaining valuable and actionable insights.

Visit www.essensys.tech for your product tour.

essensys



All rights reserved. © essensys 2021
Aldgate Tower | 2 Lemn Street | London | E1 8FA
450 7th Avenue | New York | New York | 10123
2450 Colorado Ave | Santa Monica | California | 90404
marketing@essensys.tech
www.essensys.tech