Circle.

A Layered Approach To Security

A Layered Approach To Security

The security of your organisation is more than a firewall or password. It has many layers, with each protecting a different part of your infrastructure and services which enhance the overall strength and security posture.

Circle.

Circle.

Each of these layers must be managed effectively. With remote working now the norm and users accessing the network via mobile devices, ensuring you have a thorough security posture is vital.

User

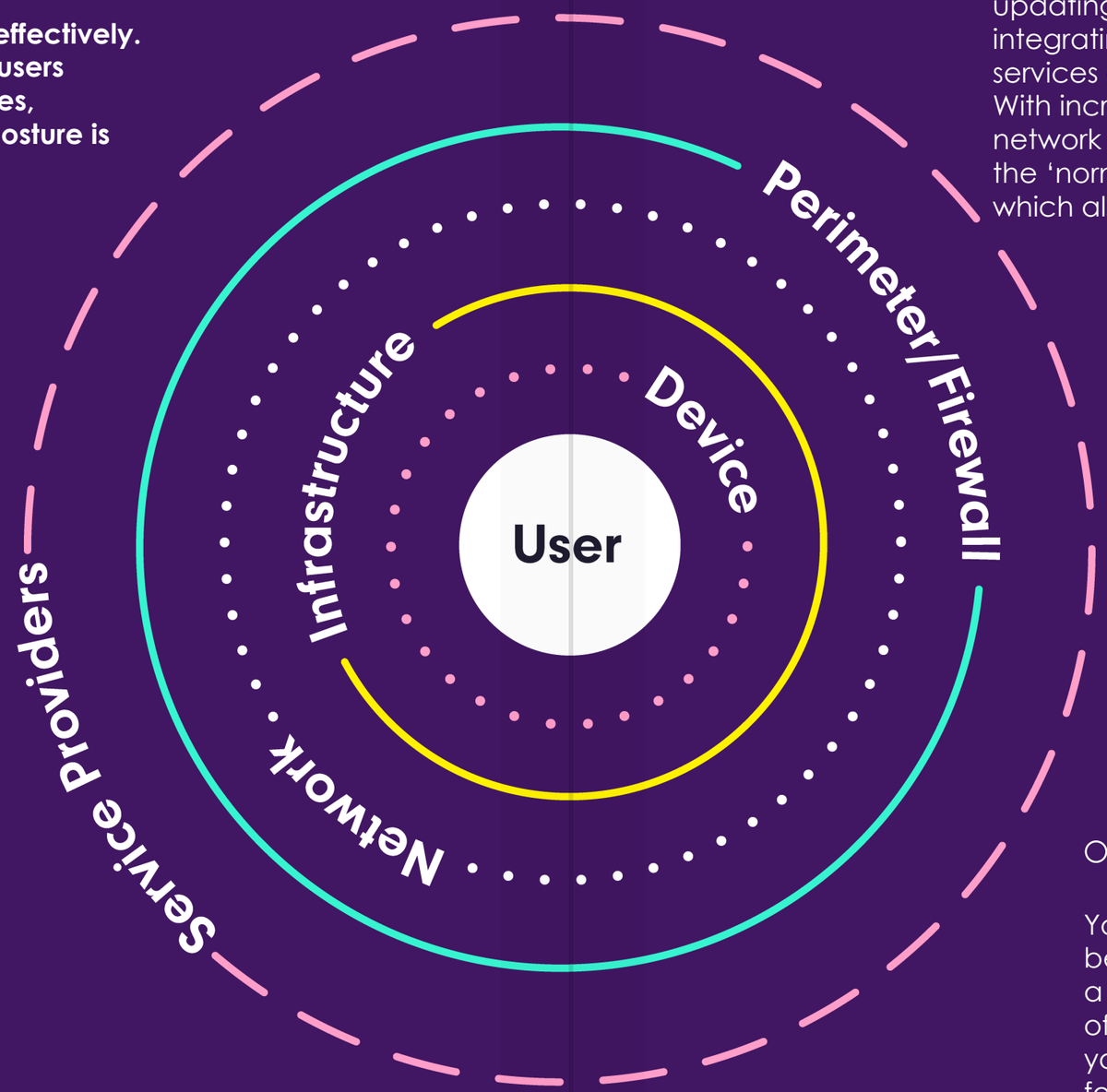
They are central to ensuring the security of your organisation and need to be protected at the ‘front door’.

Device

Having suitable security and malware protection on your device keeps cyber-threats at bay.

Infrastructure

Being able to monitor and manage your infrastructure is vital. Made more important by modern threats, being able to detect and respond is increasingly crucial.



Network

Policy based management, regularly updating, maintaining and integrating the network into the services are a necessity.
With increased remote working, the network now also extends beyond the ‘normal’ office environment, which also needs protecting.

Perimeter/Firewall

Perimeter protection (your firewall) is your first point of protection against cyber-attacks. Is yours suitable for the size and the activities of your organisation.

Service Provider

Your choice of Service Provider can be the difference between avoiding a cyber-attack or being the victim of one. Service providers ensure that you not only have the best solution for your organisation, but that it is properly maintained.

Book a meeting with our security experts today

Circle.

So, what should you ask when looking at your security strategy?

Are all these areas covered?

- ○ Are all your users protected by Multi-Factor Authentication?
- ○ Is your network security covered by policies to automatically configure network access?
- ○ Are your SaaS based applications covered with single sign on capability?
- ○ Do you know where all of your documents are stored and how they're protected?
- ○ Are your devices encrypted?
- ○ Can you access a dashboard which shows you the current compliance of all of your security policies?
- ○ Are all your documents/services backed up and tested regularly?
- ○ Are the devices protected with appropriate anti-virus/anti-malware services?
- ○ Do you provide your users with regular training to make them aware of potential threats and how to protect themselves digitally?
- ○ Can you detect and respond to a cyber-incident?
- ○ Do you have a security service in place to help respond if there was a cyber-incident?
- ○ Do you have a cyber-incident response plan?
- ○ End user devices – Are your users protected when they aren't in the office, such as working remotely?
- ○ Are you protecting users from 'known' malicious websites?
- ○ Do you provide a proactive phishing simulation to educate users?
- ○ Does your firewall inspect secure (HTTPS) content? 60-70% on the internet is HHTPS traffic so this is vital.

If you answer NO to any of the above, feel free to get in touch to see how we can be of assistance.

Book a meeting with our security experts today

Why Circle?

When you work with us, you don't get an IT supplier but partner with your best interest in mind. We look at your organisation as a whole, working with you to find the best solution to match what you need now and to support your future goals. Long and short of it - is this right for you? If not, then we will find the right solution for you.

We pride ourselves on building long-lasting partnerships with organisations.
Our Technical Architects and Account Management will form a key part of building a long-term IT strategy and roadmap for you. We ensure that you always have the right solution for your organisation, now and in the future.

Book a meeting with our security experts today