Fred Protect

Customer FAQ 2020

What is Fred Protect?

Fred Protect is a 'real time' layered managed service designed to protect your pharmacy 24/7/365 from cyber security incidents and events, without impacting the running of your business. Tools, monitoring and guidance are provided to reduce the people, process and technology challenges faced by your pharmacy in today's digital world. It does this by;

- Real time protection, monitoring and responding to cyber threats 24/7/365,
- Helping you understand your current cyber security position,
- Upskilling you and your team through cyber security awareness training,
- Documentation in the form of incident plans and quick reference guides.

What is included in the Fred Protect plans?

- Security Assessment
  - Baseline cyber security assessment (e.g. Is anti-virus on every PC? Is Remote Desktop Protocol (RDP) turned on and using a complex password? Are you running Windows 7 on your PCs?)
  - Remediation recommendations as discovered in the assessment.
- Staff Awareness Training
  - Ongoing access to cyber security awareness training material
  - Includes understanding the threat landscape, IT best practices and regulatory compliance.
- Cyber Security Documentation
  - Cyber Incident Response QRG
  - Cyber Incident Grab and Go Guide
  - Cyber Security Jargon Buster.
- Network/IT System protection, monitoring and response
  - Hardware; intrusion protection and detection (IPS & IDS)
  - Software; network monitoring and response via a 24/7/365 Security Operations Centre (SOC).
- Monthly reports highlighting cyber security incidents and events.

Why would a hacker target my pharmacy, a small business, don't they go after larger companies?

43% of all cyber-attacks now target small businesses; and health is the number one sector for reported data breaches. Cyber criminals are targeting small businesses because they view these as the easiest targets, due to them having not invested in cyber security compared to larger companies. Further, the health sector, including pharmacies, have become a target since health data can be worth three times as much on the dark web as bank data.

Do I still need anti-virus?

Yes, anti-virus forms an important part of cyber security. Fred Anti-Virus has been specifically chosen to integrate with Fred Protect, but any anti-virus is compatible. Think of anti-virus as the locks on your door. Twenty years ago, the locks were all you needed. But if you want to strengthen your security you need to think about additional layers – the equivalent of a monitored alarm and security cameras.

Is Fred Anti-Virus included with Fred Protect?

No, Fred Anti-Virus continues to be charged separately at $5 exGST, per PC, per month.

Are Fred staying with ESET?

For Fred Anti-Virus customers buying Fred Protect we will switch the AV to Webroot. For everyone else they will stay with ESET for now. Longer term the plan is to migrate all customers to Webroot.

Why Webroot?

Webroot has a purpose-built integration with Fred Protect. Logs from Webroot are fed to Fred Protect for review and analysis.

I thought I was already protected with the Fred Server and Fred Anti-Virus? Why do I now need Fred Protect?

Fred Server and Fred Anti-Virus are important elements of your pharmacies IT systems and not only remain important, but particularly with Fred Anti-Virus, are essential elements of Fred Protect. How we must defend ourselves from cyber-crime has changed significantly in the last ten years. What was enough a few years ago, is unfortunately less sufficient today. Anti-virus on its own is just not enough. Cyber criminals are constantly looking at how to exploit vulnerabilities and Fred Protect is designed to deal with the latest threats in a cost-effective way without impacting how you run your business.

All pharmacies are now also subject to the Notifiable Data Breach Scheme (NDBS). A data breach happens when personal information is accessed or disclosed without authorisation or is lost. When this happens, you must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach involving personal information is likely to result in serious harm.

The QCPP Reform Program being delivered as Quality Care 2020 will come into effect from July 1st and will include cyber security requirements.

How does Fred Protect work?

Fred Protect aims to tackle the people, process and technology challenges, while minimising the impact to running your business. Raising awareness of what the risks are by having a baseline understanding of how your pharmacies cyber security posture is the first step. Secondly, many breaches are a result of human error or poor processes, so training staff on what to do and what not to do is essential. Having clear and concise, easy to use documentation as a constant reminder or when something does go wrong forms part of the solution. Lastly, Fred Protect does just that, the technology we put in place helps protect your IT systems and valuable data from cyber-attack.

- Detect, prevent and block active cyberattacks and intrusions
- Monitor for abnormal trends through intelligent behaviour analytics
- All in real time.

What types of threats am I protected against or what does the technology do?

- Detect, prevent and block active cyber-attacks and intrusions
- Monitor for abnormal trends through intelligent behaviour analytics
- Actively block malicious sites in real-time
- Continuously scan your pharmacy for security vulnerabilities and risks
- Immediate lateral spread detection e.g. ransomware spreading to other PCs on your network
- Immediate remote privileged activity detection
- Immediate network enumeration detection e.g. attempts to retrieve usernames and other services that can then be used to access and launch further cyber-attacks and install ransomware
- Continuous and custom monitoring of Windows process and service threat indicators
- Automated alert correlation and enrichment, including affected devices' users, VLANs, hostnames, OS versions, and more.

What impact is there on the pharmacy?

The only impact is investing some time for the training and reading the documentation. The hardware is plug and play, no configuration required. The software is installed remotely and silently. Neither the hardware or software have any impact on the performance of your PCs or speed of the internet.

What is a Security Operations Centre (SOC)?

A Security Operation Centre (SOC) is an information security team responsible for monitoring and analysing an organisation's security posture on an ongoing basis in real time. The SOC team Fred works with is internationally certified meeting the highest industry standards and compliance requirements.

What will the SOC do in the event of a cyber security event?

During our standard business hours, the SOC will notify Fred who will decide the appropriate next steps. In the event of a critical incident outside of hours the SOC will act without consulting Fred, as minutes matter. Critical incidents include when a cyber security event is taking place which is likely to result in data loss, the spread of malware (ransomware, viruses etc) across the network and/or an active hacker on the network. In such an event the best course of action is to isolate the impacted device/s as quickly as possible (seconds and minutes matter) to prevent data loss, lateral spread and access to a hacker.

Does the SOC have access to my systems or data?

No. The data shared in delivering the service is metadata only, meaning it does not contain any personally identifiable or sensitive data

Who provides the documentation and training?

Fred has designed the documentation in house to be pharmacy and small business specific. They are practical, easy to use guides and not lengthy policies that wind up as shelf ware. We will regularly review and update the documentation.

The training is via Webroot who we have also chosen as the anti-virus partner of choice. Webroot's training has been professionally produced and includes content specifically for Australia (e.g. Notifiable Data Breach Scheme)

How is the Fred Protect hardware connected?

The hardware requires both power and a network point, it does not connect to a computer. An available network port and power point is required to connect the device. Simple to follow instructions are included when the hardware arrives.

How is the hardware sent?

Fred will pre-configure and post the hardware. No configuration is required by you. It's plug and play.

What if I can't install or there are not enough network ports or power?

If you do have any issues, please call our Fred Help Team. We will first try to assist remotely and talk you through how to plug it in. In some cases, you may require a 12 or 24 ports switch, Fred can provide advice accordingly. If all else fails, we'll send someone onsite to assist.

How is Fred Protect protected, both hardware and software from unauthorised access or attack?

Being a managed service Fred will be alerted to any change in how Fred Protect is operating. The hardware and software are both near impossible to detect on the network making it very difficult for a hacker or malicious software to deactivate or circumvent. If the hardware is unplugged or no longer working or in the unlikely event the software is uninstalled, we receive an alert to investigate. There is no data stored locally in the hardware or software to compromise.

What happens if the hardware fails?

We will be alerted and provide replacement hardware at no cost. Hardware failure will not impact your store operations.

How much does Fred Protect cost?

Fred Protect has a single service plan and costs are tiered based on the number of endpoints (Windows PCs or Servers) connected to the service. Other devices on the network such as Internet of Things (IoT) devices, like smart TV's, fridge thermometers and security cameras, phones, Apple or Android devices do not count towards the cost. To view our plans visit www.fred.com.au/what-we-do/services/fred-protect/fred-protect-plans/

How can I purchase Fred Protect?

We can provide you a quote, please call us on 1800 888 828, email sales@fred.com.au or alternatively you can order directly from our website at www.fred.com.au/what-we-do/services/fred-protect/fred-protect-plans/

Do I need the software on every PC?

Yes, every Windows PC must have the software installed to ensure they are protected. Only PCs and/or servers require the software. Other endpoints, such as IoT devices like smart TV's, fridge thermometers, security cameras do not require licences. Neither do phones, Apple or Android devices. If you have a Fred 'Rental' Server, the cost of the licence is included and does not go towards your PC count.

How are these other (IoT) devices protected then?

These devices are protected by the hardware, plus whilst they don't have the software installed the SOC can still 'see' traffic flowing from them and if a device that normally doesn't have a high traffic footprint suddenly does it will trigger an alert for investigation. One of the important benefits of 24/7/365 real time monitoring by the SOC.

Does that include remedial or break fix work in the event of a cyber security event?

No. The fees include the management and provision of the security assessment, training, documentation, hardware and software. If Fred is required to send a team member onsite or spend more than 30 mins remotely standard rates apply. Fred will always seek confirmation before proceeding with chargeable work.

Will Fred Protect provide 100% protection? And what level of guarantee is provided?

No system that connects to the internet is ever 100% protected. Fred makes every effort to ensure your IT Systems and data are protected and secure via Fred Protect. There are though circumstances that may result in a cyber security event (such as, but not limited to, a systems breach, data loss, or irreparable damage) and we are unable to guarantee against this. By agreeing to use Fred Protect you, the customer, maintain the risk and liability associated with a cyber security event.

Is there a contract period?

No. The Fred Protect agreement can be stopped at any time. We will work with you to decommission software and have hardware returned to Fred upon receipt of your cancellation notification.

Can I mix and match levels of service?

No, there is only one service plan.

Can I add extra computers to Fred Protect later?

Yes, just contact Fred to have a member of the sales team discuss Fred Protect expansion requirements. Pricing may change if the total number of computers moves your service to a different tier.

Is there a Service Summary associated with Fred Protect?

Yes, the Service Summary is available from www.fred.com.au/what-we-do/services/fred-protect/fred-protect-plans/