PREMIER
Technology Solutions

TREND MICRO | partners

Cyber Security Upgrade Initiative

Prepared By:

Jeremy Herbert
CIO - Premier Technology Solutions

Date: 11/04/2022

Contents

Cybercrime in 2022 And Beyond

With the world settling into the new post-COVID normal, staff are returning to work and we're coming to accept COVID as a regular part of our lives. Another issue that has become a part of daily life is cybercrime.

Data breaches are rife and ransomware attacks are soaring in number and severity across the world. While we may not hear about these incidents as much as we do COVID, cybercrime is now so pervasive that we are being called on like never before to safeguard against this equally insidious and invisible threat.

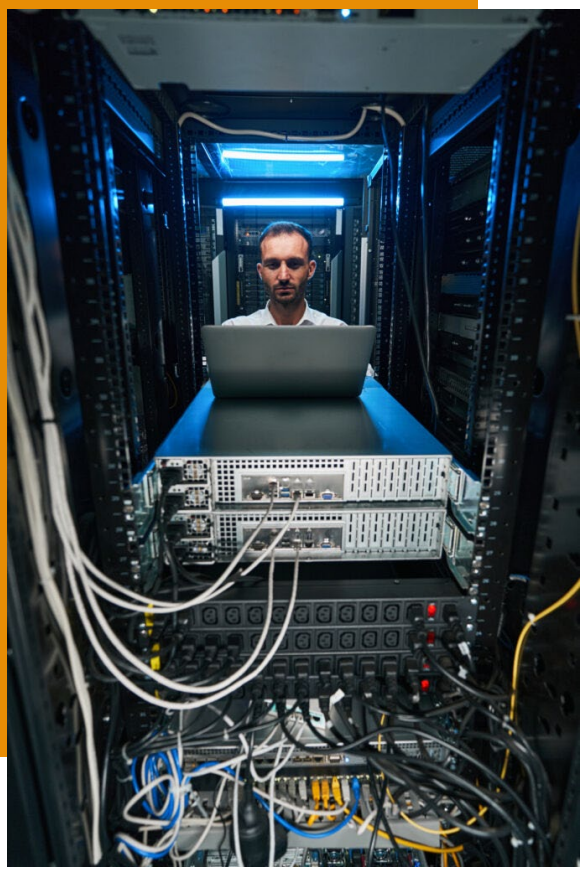
1.1 | Risks to Data Management

You've likely read the headlines about the 'Great Resignation', with workers quitting their jobs in droves to look for better pay or conditions in the wake of the pandemic. Just over 20% of Australians have changed jobs within the last year and almost 25% are considering leaving their current place of employment, with over 30% of Australians considering changing jobs, saying COVID has had a big impact on their decision.

For our customers, this has created two scenarios: firstly, a greater pool of potential recruits, and on the flip side, a heightened risk of employee-driven data breaches.

There is no doubt the cybersecurity industry requires more people. Cyberattacks have risen more than 1100% in the past 12 months alone. Seventy-three percent of organisations had at least one data breach in the past year directly or partially attributed to a gap in cybersecurity capabilities.

As such, risk mitigation planning is essential. In cases of both departing employees and remote workforces, organisations must implement security controls, including data loss prevention and security monitoring, as well as limiting access to critical information by implementing controls as simple as 'need-to-know' access policies. This style of zero-trust architecture governs what an employee can and cannot see.



1.2 | Regulation and Enforcement

The increased cyberthreats to organisations have not gone unnoticed by the federal government, with a sharp increase in regulations and enforcement meaning any business serious about their reputation and profitability should take notice.

If you're in doubt, ASIC's first Federal Court action over allegations of deficiencies in cybersecurity is underway. The test case against RI Advice alleges the financial services company failed to take reasonable steps to manage a string of cybersecurity breaches and contravened s912A of the Corporations Act 2001 (Cth). The case, which goes to trial in April 2022, provides some insight into what could become the regulator's minimum benchmarks for cybersecurity, at least within the financial services sector.

Already, there are compulsory reporting and breach notifications for private companies with a turnover of more than $3 million; the amendment to the Privacy Act 1988 (Cth) requires any malicious or accidental data breach of personal information or credit information to be reported to the OAIC. In addition, companies that fall under the scope of the Act are required to notify any customers whose data was leaked, resulting in reputational harm and potential litigation.

The actions of board members are coming under further scrutiny by the government. The Australian Prudential Regulation Authority (APRA) is turning its attention to corporate administrators and their responsibility to implement cyberattack resilience.

APRA has made it known it is taking a "much more targeted approach to ensuring CPS 234 [APRA's Information Security Prudential Standard] is being fully complied with and holding boards and management accountable where it is not". This will result in board members being held more accountable for all things cybersecurity-related, and deferring to an explanation of "we spoke to our IT" will no longer be accepted.

1.3 | The Rise of AI in Cybercrime

Cyber and ransomware attacks have never grown faster than at the rates we are seeing today – and worse is yet to come. Driven by the lucrative nature of the trade, hackers are starting to use artificial intelligence (AI) to create viruses faster than detection methods can keep up, using it to devise even more deceptive phishing emails and texts and to scan corporate networks for weaknesses.

Over the next 10 years, it is predicted that AI will disrupt the cybercrime industry, with AI tools making the capability of carrying out attacks accessible on a whole new scale to individuals with little or no technical skill.

While AI will be used to make the lives of cybercriminals easier, security vendors are investing in their own AI technology to counter the threat. In a survey of 500 IT leaders,

91% expected that some or all of cybersecurity will be automated by AI in part or in full by 2030.

We will continue to see AI driving an increase in sophisticated cyberattacks over the next year. However, AI's use for prevention, at its current rate, looks set to win the battle.

Trend Micro: Profile of a Global Leader in IT Security

Trend Micro, a global cybersecurity leader, helps make exchanging digital information safer. Fuelled by decades of security expertise, global threat research, and continuous innovation, their unified cybersecurity platform protects hundreds of thousands of organisations and millions of individuals across clouds, networks, devices, and endpoints.

With 7,000 employees across 65 countries and the world's most advanced global threat research and intelligence, Trend Micro has the resources to protect your business.

Trend Micro has been continually recognised by leading analysts, with highlighted accolades including:

- Having the leading market share for hybrid cloud workload security;
- Being named a leader in the Forrester New WaveTM for Extended Detection and Response (XDR) Providers, Q4 2021;
- Being named a leader in the 2021 Gartner Magic Quadrant for Endpoint Protection Platforms;
- Being named a leader in the Forrester Wave™ for Enterprise Email Security, Q2 2021;
- Being named a leader in the Forrester Wave™ for Endpoint Security SaaS, Q2 2021;
- Being in the top three for Visibility and Telemetry in Mitre Engenuity™ ATT&CK Evaluation, Q2 2021;
- Being recognised as meeting 8 of 8 recommendations for securing cloud workloads, 2021;
- Being number one in Gartner IDPS Market Share worldwide, with 23.5% share for 2020; and
- Being named the leader in Global Vulnerability Research and Discovery since 2007.

2.1 Staying a Step Ahead

Over the years, Trend Micro's proven foresight has enabled them to deliver many security innovations, including being the first to secure virtualisation, hybrid cloud, and containers. Now, they are using an innovative platform strategy to help their customers secure the new realities of a remote and hybrid workforces and IoT/OT environments in the wake of a global pandemic and geopolitical unrest.

With Trend Micro's unified cybersecurity platform, there is a continual focus on innovation and addressing the challenges of today and tomorrow. It helps customers see their full security picture so they can quickly detect, protect, and respond to known and unknown threats across evolving attack surfaces. Powered by industry-leading XDR, modern protection across IT layers, global threat intelligence, and expert threat response services, Trend Micro helps its customers better understand, communicate, and mitigate cyber risk, while freeing them to drive their businesses forward.

2.2 Global Threat Intelligence and Research

Smart protection begins with global threat intelligence. Trend Micro's mission is to protect its customers, which is why they mine data around the clock and across the globe by leveraging over 250 million sensors through the Trend Micro™ Smart Protection Network. Receiving over five trillion queries in 2021, the Smart Protection Network enabled its cybersecurity platform to block over 94 billion threats like ransomware across cloud, endpoint, IoT and network environments.

It's not just an amazing amount of threat data – it's global threat intelligence that uses artificial intelligence and predictive analytics to help protect against the most likely threats.

Trend Micro's global research division, Trend Micro Research, uses its worldwide network of 16 threat research centres to continually analyse and identify new security challenges like Log4j, as well as malware, ransomware, malicious URLs, command and control (C&C) locations, and domains that could be potentially used in attacks. The team's broad research agenda helps their offerings defend millions of customers around the clock from attackers like REvil and Conti ransomware.

Trend Micro's vulnerability research is anchored by Trend Micro™ Zero-Day Initiative™ (ZDI), the world's largest vendor-agnostic bug bounty program. Powered by over 10,000 threat researchers, ZDI allows them to identify and disclose the greatest number of new vulnerabilities to help improve the security of both their customers and the broader industry.

Delivering Cyber Security with Trend Micro XDR

3.1 XDR with 24/7 Security Operations Centre as a Service

With traditional endpoint protection, detected malware shows up as a statistic on a monthly report; when a user clicks on a link or opens a suspicious attachment nothing is tracked, nothing happens and no one is watching.

To deliver on the next generation of business security, we're partnering with one of the largest security vendors in the world to deliver enterprise-grade eXtended Detection and Response (XDR) backed by a 24/7 Security Operations Centre.

The XDR platform collects sensor data for security incidents and suspicious changes across your organisation's laptops, desktops, servers, and cloud platforms. This sensor data is then correlated using artificial intelligence and machine learning to provide actionable intelligence to the dedicated security analysts at Trend Micro.

Where threats aren't instantly neutralised, we will work with you and the security services team to contain the breach and neutralise it at its source.

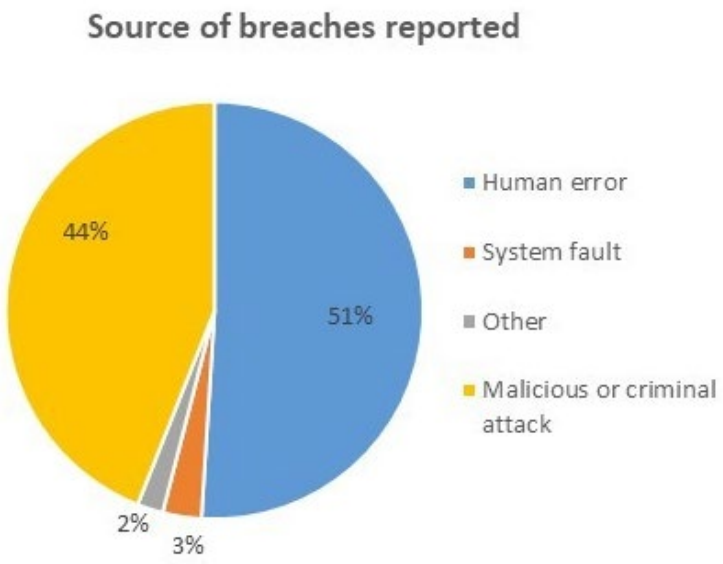
3.2 XDR Threat Hunting

Threat actors can enter your environment from difficult-to-detect vectors and lurk for days and weeks, hiding in plain sight behind legitimate remote tools or on obscure, forgotten windows devices while they prepare to take control of your environment.

Security analysts will leverage the XDR platform to actively perform indicator-of-compromise (IOC) sweeps of your email and environment to hunt, detect, investigate and respond to threats faster.

3.3 Data Loss Prevention

The XDR platform can prevent leaks of sensitive banking, cardholder and other private information from your business. While it might seem unlikely that a data leak will occur, and while anti-malware protection might seem like enough protection, your business is more at risk of a data leak from an unintentional act than a malicious act or criminal attack.



With increased regulation, privacy laws and mandatory reporting of breaches or data loss to the government and your customers, protecting your business with these platforms is becoming more important. Data loss prevention capability is also one of several categories noted during cyber insurance applications or renewals.

We'll work with you to configure DLP policies for your business, so, whether by web, email, instant messaging or a USB drive, the DLP protection will block unauthorised attempts to egress sensitive data from your business.

3.4 Cloud App Security

In the small business sector, on-premises infrastructure has rapidly given way to cloud services that provide better performance and reliability, but this has left a gap in security, allowing threat actors to exploit the opportunities presented.

With the XDR platform, we can now extend threat protection to the most popular SaaS platforms, including:

- Microsoft 365: Exchange Online, OneDrive, SharePoint and Teams;
- Google: Gmail and Google Drive;
- Dropbox;
- Box; and
- Salesforce.

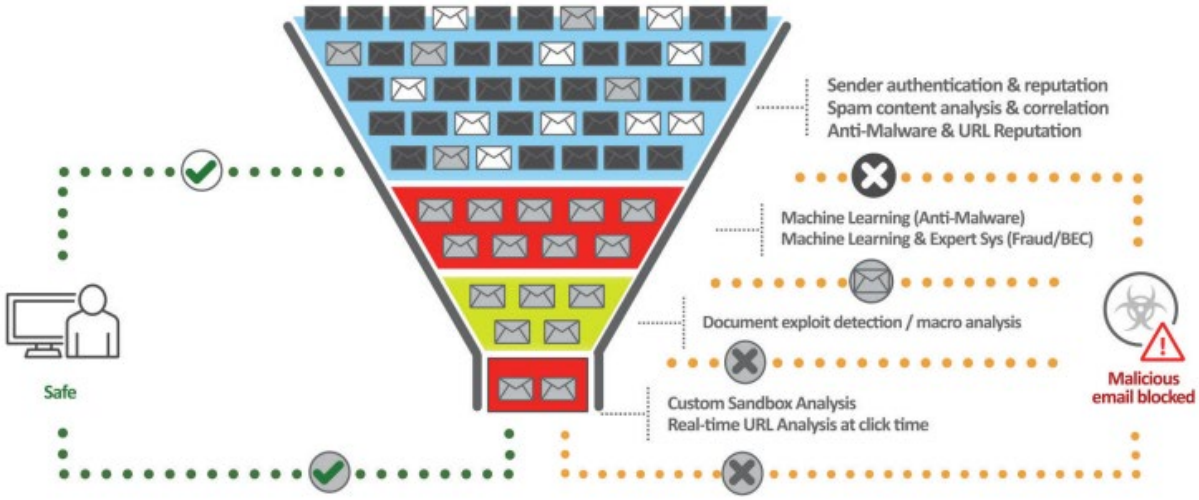
3.5 Advanced Spam Filtering

Traditional spam filters rely upon rigid patterns and rules to detect malicious emails. They have no visibility into the links inside emails, and can't even open a password-protected attachment if the password is in the email.

These weaknesses, among others, allow targeted phishing and other malware attacks to pass through unhindered. Worse still, if one of your accounts is compromised, malicious emails can be sent within your organisation without being scanned for threats.

The next generation of anti-spam will:

- Open and review all the websites linked in the email, analysing logos, pictures, and the given address to detect websites posing as Microsoft, Google, Facebook, and other major brands;
- Open suspicious attachments in a sandboxed environment, so never-before-seen malware can be discovered and blocked;
- Scan password-protected Office and ZIP files where passwords are provided in current or future emails; and
- Scan the content of all emails sent internally in case of a compromised account.



The XDR platform is not only more secure, but is also easier to use and provides a contingency if your email provider has an outage.

- Email continuity: when Outlook or Gmail is unavailable, you may be waiting for hours before Microsoft or Google restore services. Now, you can log on and respond to emails while your provider resolves their issues.
- Quarantine self-service portal: with multiple digest emails a day, and often hours between them, you may be left waiting or need to call our service desk to check if an email you're waiting for has been intercepted. Now, you will be able to quickly log in using your single-sign-on credentials.

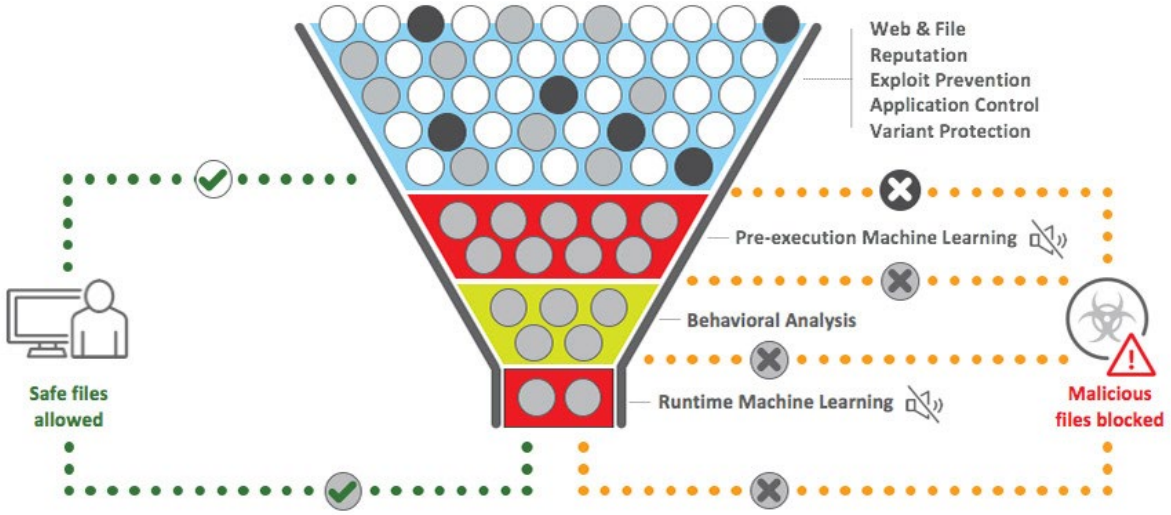
With the advanced enterprise-grade technology delivered by Trend Micro's global team of developers, researchers, engineers they were able to catch 16.7 million high-risk threats that built-in cloud protection was unable to defend.

3.6 Advanced Endpoint Protection (Anti-Virus)

Even with the best email filtering available, one virus getting through can cause havoc and disrupt your business for days or weeks. Modern malware can adapt and change every 15–20 seconds, making traditional AV incapable of coping.

Trend Micro's Endpoint Protection delivers not just traditional Anti-Virus and Anti-Malware features, but delivers on the Web / URL protection and content filtering, and can be used to enforce strict application usage for enhanced security if required.

Trend's security goes beyond the current protection employed and adds high-fidelity machine learning and other detection techniques for the broadest protection against ransomware and advanced attacks



These defences include:

- AI and machine learning techniques running before and after the execution of programs for accurate detection;
- Crypto rollback, where malware attempting to encrypt your local or cloud files will be terminated, and the files rolled back to their original state;
- Virtual patching, where exploit prevention applies 'virtual patches' to your servers and computers, protecting them from common exploits even if they're not yet patched; and
- Cross-layered sharing, where threat intelligence is automatically shared across security layers, enabling protection from emerging threats across the whole organisation.

Beyond the advanced technology, the Security Operations Centre leverages advanced endpoint agents to investigate, contain and resolve threats in your environment when an incident occurs.

3.7 Advanced C-suite Protection

Threat actors use a combination of stolen and public data from social media and websites to gather the names and positions of those in your company, focusing their attacks on those able to authorise or transfer money, such as chief executive officers, vice-presidents, and general managers.

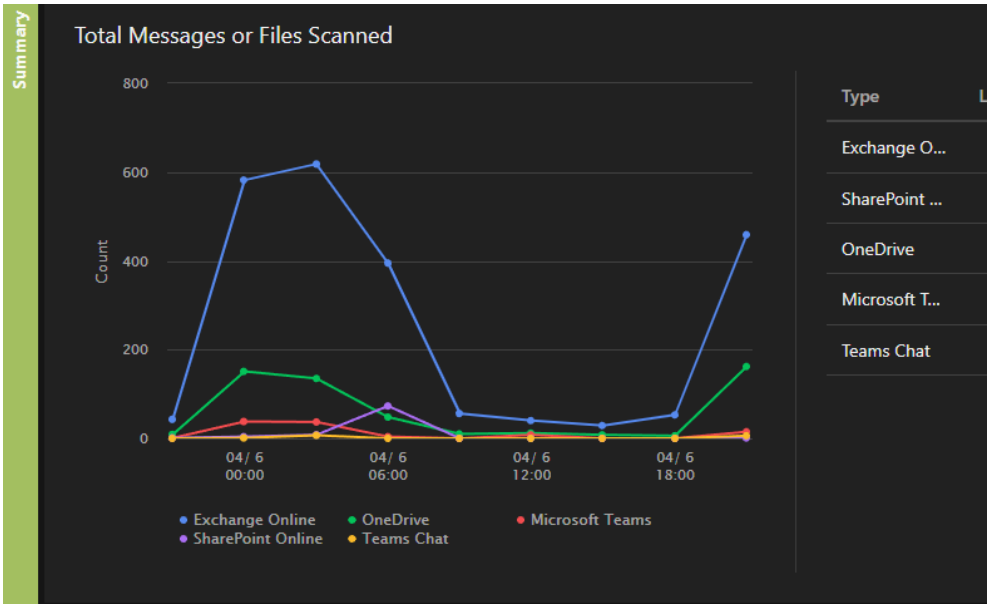
Trend's XDR platform has the most advanced business email compromise (BEC) protection in the industry, including AI-driven writing style analysis that learns how you and your team write emails, allowing it to detect attack behaviours and email intention.

We'll work with you to gather the list of VIPs to upgrade their protection against targeted threats during onboarding.

3.8 Cyber Security Detection and Reporting Portal

Whether your managers are trying to better understand risks against their company or need more control of their email systems, many of our customers often request more insight and control into IT and security.

With the detection and reporting portals, you'll have visibility into activity and defended threats across your email, Teams, SharePoint and OneDrive workloads.



Nominated managers can also be granted access to their company quarantine so they can review and release intercepted emails for their company without needing to wait for digest emails or contact helpdesk.

Security Assessment Reports

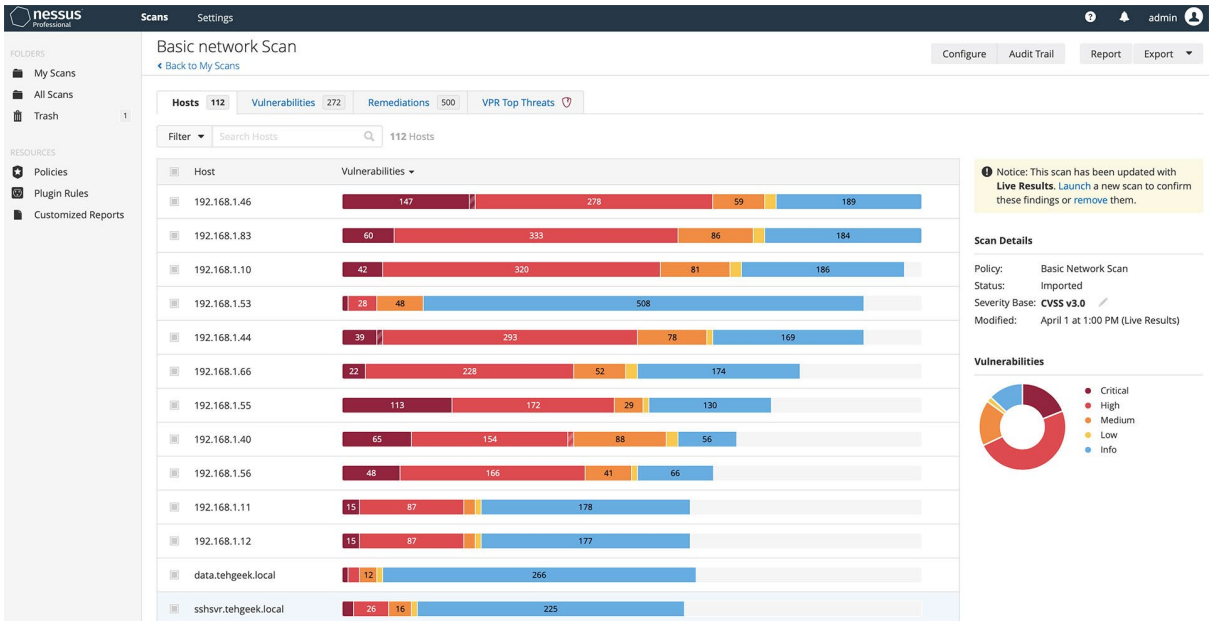
There are many proactive components to the Trend Micro XDR solution, but our goal is to mitigate the security risks to your company by performing further proactive steps to identify vulnerabilities in your organisation before you are attacked.

4.1 Vulnerability Scanning

We've invested in the technology and training for Nessus, the industry standard in vulnerability scanning, to provide you with yearly assessments of your internal infrastructure and services beyond the scope of the Trend Micro XDR platform.

Performing a vulnerability scan is an essential part of mitigating your organisation's security risks. By using a vulnerability scanner to identify the points of weakness in your systems, we can reduce the attack surface that criminals might exploit, focusing our security efforts on the areas that are most likely to be targeted.

Criminal hackers use automated tools to identify and exploit known vulnerabilities and access unsecured systems, networks or data, so it's important that we find risks before they do.



4.2 Dark Web Assessment

Users often utilise their business email for personal accounts across a variety of commercial and consumer platforms, and, almost every other day, we're seeing data breaches across third-party platforms like Microsoft and Facebook.

Often referred to as 'dark web' scanning, it involves using our resources to discover all data breaches that a given email address or domain has been included in. We'll report any

other information that was included in the breach, such as usernames, passwords, and credit card information.

4.3 ACSC Essential Eight Alignment

While no set of mitigation strategies is guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the Australia Cyber Security Centre's (ACSC) Strategies to Mitigate Cyber Security Incidents as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

As part of the risk assessment, we'll score the maturity level of your company's security against the Essential Eight strategies and provide recommendations for changes to increase your security posture for:

- Application control;
- Application patching;
- Microsoft Office settings;
- User application hardening;
- Administrative privileges restrictions;
- Operating system patching;
- Multi-factor authentication; and
- Regular backups.

Mac OS Support

Apple Mac offers a variety of mobile, laptop and desktop platforms to a mostly consumer customer base; their Mac OS platform is also a popular platform for a small number of content creators, web developers, and executives.

We currently offer 'best effort' support to Apple Mac devices; providing further support has been challenging due to a combination of issues with Apple's support model and technical platform issues that make Apple Mac devices unreliable to manage at scale.

In 2022, we're refocusing our efforts on the Apple Mac OS platform and will now be providing additional limited support to include:

- Trend Micro XDR endpoint protection with 24/7 SOCaaS;
- Remote management and monitoring and inventory management;
- Microsoft Office and Microsoft 365 support; and
- DNS and URL monitoring and filtering.

We have plans to further expand our Apple support and endpoint management capabilities to help bring it closer in parity to the full support enjoyed by Microsoft Windows platforms. We will provide details on the planned expansions later in the year as details are finalised.

New Customer Portal Experience

As part of our initiative, we will aim to provide a more modern user experience, streamline common interactions that you have with us, and provide greater insight into all your organisation's service tickets and projects by allowing you to log in with your Office 365 single sign-on credentials.

At launch, we will have available to our primary contacts:

- Create service requests and view those created by all other staff;
- View professional service requests; and
- Utilise the 'New User' and 'User Termination' service request forms.

Within the year, we also plan to add:

- Monitor the progress of your managed IT projects with Gantt chart views; and
- The ability to view invoices and pay for them online.

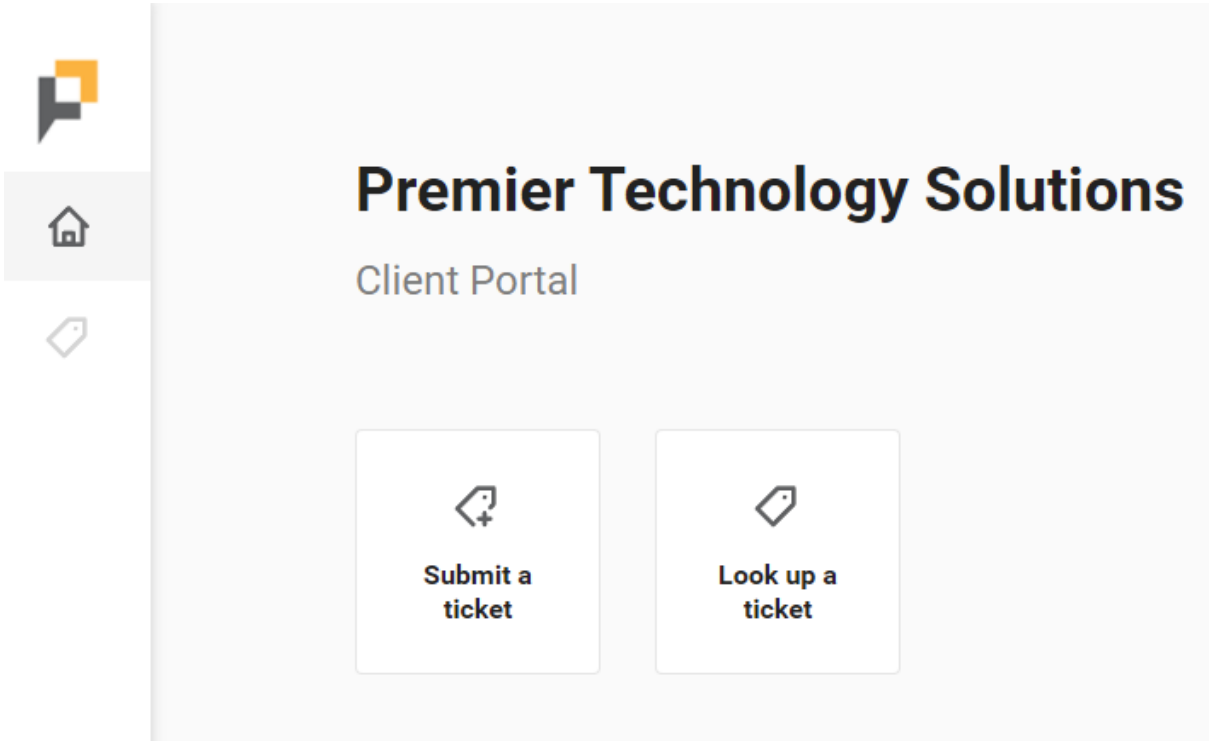
All of your company staff members will be able to log in and create, update or review service requests that they have created with their 365 or G Suite credentials.

The customer portal will also be an important component of our Premier Aware program and security queries, as spam or malware queries by email are frequently being intercepted by our anti-spam, delaying our responses; the new portal will allow customers to upload attachments directly.

6.1 Log In to the Customer Portal

To access the new customer portal:

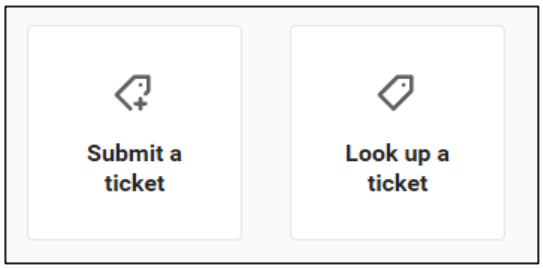
- navigate to https://premiertech.myportallogin.com.au/ from your computer or your mobile phone, or following the helpful link on the https://premiertech.com.au/ website;
- if you have a Microsoft or Google account, choose the appropriate single-sign-on option, or click 'Sign Up' to create a free ConnectWise account; then
- wait for the Customer Portal home page to load. Depending on your level of access, the page displays a variety of options.



Navigate the Customer Portal

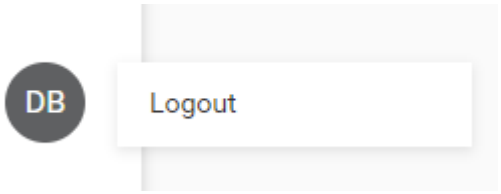
7.1 Service Tickets

- **Submit a ticket:** Click to create a new service ticket. After you select this option, you are presented with different ticket categories. Select the category of ticket you would like to submit.
- **Look Up a ticket:** Click to review all open and closed tickets in the Customer Portal. Search by ticket number or filter by ticket summary.



7.1.1 Log Out

- To log out, click on your initials in the bottom left-hand corner of the screen and select 'Log Out'.



Third Party Application Patching

Applying patches to applications and operating systems is critical to ensuring the security of systems. As such, patching forms part of the ACSC's *Essential Eight* from the Strategies to Mitigate Cyber Security Incidents guide.
To better align our customers with the Essential Eight we'll be delivering additional patching to 57 common third party applications and platforms.

This list includes:

- Adobe Acrobat 2017
- Adobe Acrobat 2020
- Adobe Acrobat DC
- Adobe Acrobat DC (64-bit)
- Adobe Reader 2017 MUI
- Adobe Reader 2020 MUI
- Adobe Reader DC
- Adobe Reader DC MUI
- AdoptOpenJDK 11
- AdoptOpenJDK 8
- Audacity
- Ccleaner
- Chrome
- CiscoJabber
- CiscoWebex
- Dropbox
- Eclipse Temurin JDK 11
- Eclipse Temurin JDK 8
- Firefox
- Firefox ESR
- Foxit Reader
- Google Drive
- Google Earth
- GoToMeeting
- iTunes
- Jabra Direct
- Java 6 (32-bit)
- Java 6 (64-bit)
- Java 7 (32-bit)
- Java 7 (64-bit)
- Java 8 (32-bit)
- Java 8 (64-bit)
- KeePass
- KeePass Password Safe
- Malwarebytes v4
- Notepad ++
- OneDrive
- OperaChromium
- PDF24 Creator
- PDFXChange Editor
- PuTTY
- Safari
- SeaMonkey
- Seven-Zip
- Skype
- TeamViewer 12
- TeamViewer 13
- TeamViewer 14
- TeamViewer 15
- Thunderbird
- Treesize Free
- VLC Media Player
- WinRAR
- WinSCP
- WinZip
- Wireshark
- Zoom

New Applications are frequently being added, with another 4 apps being added next week. If you have applications you would like updated we'll work with our partner to include it.