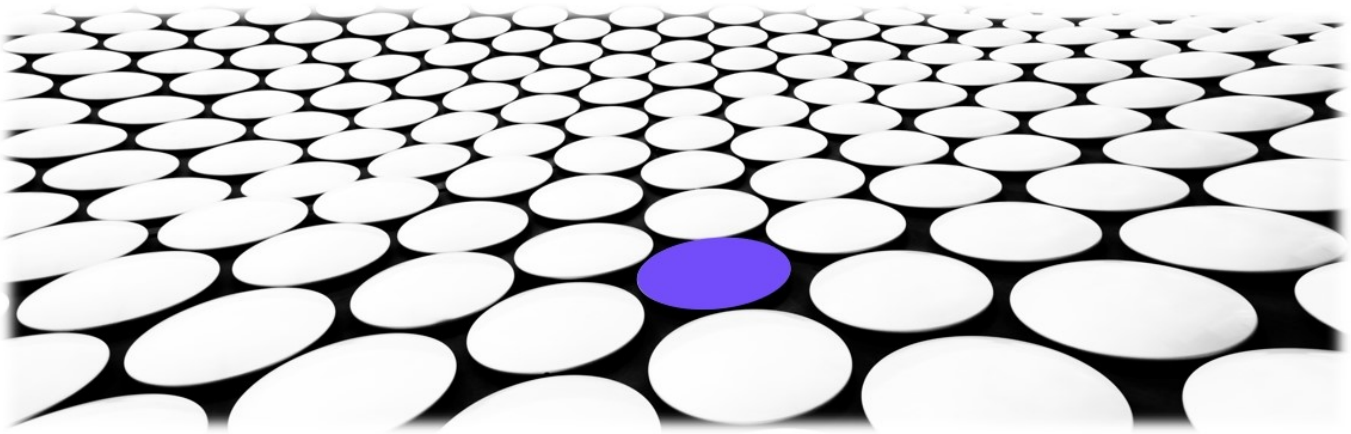
DISRUPTECH
TECHNOLOGY SOLUTIONS

Technology solutions for resellers



We help you stand out from the crowd

EXECUTIVE OVERVIEW

How can your company benefit from these unique Cyber Technologies?

Disruptech prides itself by partnering with the best cyber security solutions vendors in the business.
Many of these solutions are in a cyber category of their own. In other words, there are no other solutions like these on offer anywhere in the world. They are truly unique and cutting edge to protect your business on a whole new level not previously seen in Australia.

Get the competitive advantage with Disruptech.

Security Awareness Training
Our one-of-a-kind Security Awareness Training uses psychology to create individual and custom-made courses for every user in your organisation. Using intelligent automation, the platform combines continuous training with regular phishing simulations, simplified policy management and behavioral risk scores - enabling you to assess and mitigate your organization's human cyber risk with leading technology and a user-first approach.
The first line of defence against hackers and ransomware is through cyber aware employees.
It's cost effective, has rapid deployment (15 minutes per organization) and makes an enormous difference to the company cyber security posture. This needs to be your first line of defence.

NeuShield
Making Ransomware Obsolete. NeuShield's unique patented approach to data protection makes attackers believe they have access to a computer's original data files, but they are in fact only seeing a mirror image. Even Fully undetectable (FUD) and Zero-Day threats can be quickly and easily recovered from.
Bridging the gap between End Point Security and Backups.
Recover your data in minutes without backups.

HOPZERO
HOPZERO is the only solution on the planet that can limit the distance your data can travel.
Stops DataTravel™ — blocking server compromise.

- Limit's server DataTravel to the data centre or organization perimeter.
- Protects your most critical data.
- Stops Ransomware.
- Alarms and catches phishing / ransomware attempts.
- See where your data is travelling live via a world map.
- Map's visualization of exfiltration and attacker activities on a live map.
- Smart Logs provide cogent metrics improving security evidence.

HOPZERO has created a new category of cyber security - The Data Compromise Prevention System.

Harmony IoT
Harmony IOT Keeps your enterprise safe in today's smart connected world.
Harmony IoT delivers an enterprise-grade defense for your airspace that protects valuable digital assets from IoT-born attacks. Harmony IoT analyzes your airspace 24x7 to identify and profile all smart connected devices in and around your environment. With Harmony IoT, you get continuous PROACTIVE THREAT DETECTION and REAL-TIME ATTACK MITIGATION.
The Harmony IoT protectors are connected to the largest wireless computing devices and activities database in the world to give you maximum protection.

Harmony Purple
Harmony-Purple's solution is a Vulnerability Prioritization Technology (VPT) that enables organizations to assess their cyber risks based on asset criticality and advanced analytics. The technology also allows organizations to invest its time and resources on those vulnerabilities that threaten its critical assets and business processes. Powered by Harmony-Purple's patented Attack Patch Scenario (APSTM) technology, the system creates a prioritized list of vulnerabilities. This allows organizations to substantially reduce its attack surface with the least amount of time and effort and with the most efficient use of staff resources. Reduce your vulnerability remediation costs today.

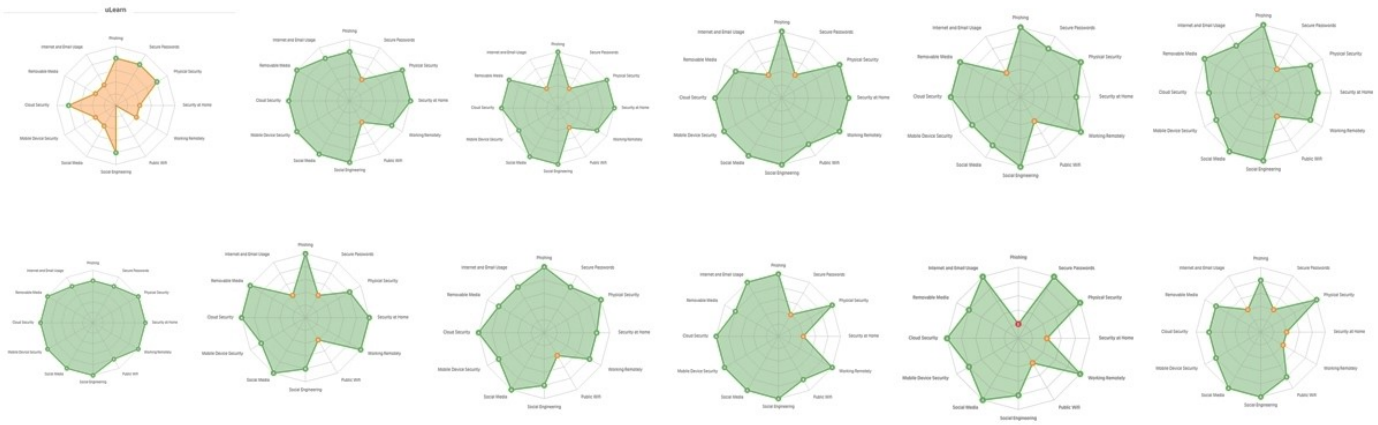
Psychology based Security Awareness Training with Policy Management

Summary of solution

- White labelled security awareness training solution to brand as your own.
- Uses psychology to give each user a unique and custom training modules starting with their weaknesses first.
- Setup time is around 15 minutes per client and can then provide them with 3 years of continuous training.
- The use of intelligent automation speeds up the user learning process in the right areas needed to rapidly protect your organisation.
- Human Risk Report to visualize the human threat to your organisation.
- Dark web scanning exposes employee accounts exposed in data dumps, paste sites and hacking forums.
- Policy management built in. We simplify policy communications and user acknowledgement by automating the process – sending policy changes directly to your user's inbox and tracking who has opened and signed their document.

Below is our typical company risk map for our users.
As you can see, they are all different as each user's cyber security knowledge is different.

Give your staff the custom training they need simply and easily.



Here's how we transform your employees into a cyber security asset

We ensure **ongoing, bite-sized training** that strengthens your users' knowledge in core areas of security, while **measuring your organisation's overall human risk** based on continual phishing assessments, dark web monitoring and policy communications.

Evaluate	Educate	Simulate	Communicate	Calculate
Assess Current Risk	**Drive Secure Behaviour**	**Mitigate Phishing Threats**	**Reinforce Best Practice**	**Measure Progress**
Identify your users' current security knowledge gaps	Develop a security-minded culture with ongoing micro training	Deliver ongoing simulated phishing assessments		...employee and export ...or auditing
Assess employee vulnerability to targeted phishing	Strengthen individual weaknesses with user-tailored programs	Assess vulnerability to a diverse range of phishing attacks	Measure employee acknowledgement with trackable e-signatures	Understand your organisation's human risk at any one time
Locate employee credentials exposed on the dark web	Maximise engagement and retention with video & interactive content	Learn how your employees' phishing vulnerability changes over time	Centralise, edit and create policies in one accessible place	Monitor the dark web continuously for exposed employee credentials
- Dark Web Monitoring - Simulated Phishing - Gap Analysis Quiz	- Computer-Based Security Awareness Training	- Simulated Phishing *(Automated)* - Spear Phishing	- Centralised Policy Management - Automated Policy Acknowledgement	- Custom Reporting - Holistic Risk Score - Dark Web Monitoring

NeuShield Data Sentinel - Making Ransomware Obsolete

Summary of solution

The NeuShield Difference

Why are so many companies getting hit with ransomware even though they have made significant investments in a layered security model? The reason is because ransomware is getting more targeted.

The solution, a new approach to data protection. NeuShield Data Sentinel takes a completely different approach by creating a protective shield between your files and applications. When ransomware or other applications make changes, the original files stay intact allowing users to revert any unwanted change that has been made. While other products create backup copies of your files which, can dramatically increase disk usage and cause a significant performance overhead, NeuShield's revolutionary Mirror Shielding™ technology can preserve the original file without requiring a backup, which allows Data Sentinel to protect files with virtually no additional disk activity (I/O). NeuShield Data Sentinel allows you to shield and protect your data from malware or human error**.**

If your business is time sensitive and cannot afford downtime, NeuShield is the essential layer **of protection your business needs today.**

MIRROR SHIELDING ™

NeuShield's award-winning Mirror Shielding™ technology enables you to recover your data instantly, without relying on backup or rollback, from any kind of corruption, deletion, or encryption due to cyberthreats.
Your data will never be held hostage again.

ONE-CLICK RESTORE

With one simple click you can bring back your entire operating system to a known good state within minutes.
You no longer need to worry about losing time because of undetected malware, faulty patches or operating system corruption.

FILE LOCKDOWN

Let's suppose you are the victim of a ransomware attack and can't afford to have any downtime. No problem!
NeuShield Data Sentinel allows you to lock your data so employees can continue working and using their data until you can use One-Click Restore to recover your operating system.

DATA ENGRAMS™

Leverages Mirror Shielding™ to create copies of modified data at different points in time.
Data Engrams™ work like file revision history, allowing files to be restored to previous versions.

CLOUD PROTECTION

Damage from ransomware can increase exponentially when using cloud drives. NeuShield Data Sentinel stops the spread of ransomware and allows corrupted data to be recovered instantly. We support Microsoft, OneDrive, Google Drive, Dropbox, and Box.com.

BOOT PROTECTION

Protects the boot portion of a drive to prevent aggressive types of ransomware from taking over the boot process and preventing applications from writing to the boot record.

DISK PROTECTION

Monitors all direct disk access preventing malicious programs from destroying data on the hard drive or SSD.
Protects against destructive ransomware or wipers that attempt to wipe the disk.

Supported Operating Systems.
OS: Windows 7, 8.1, 10
OS: Windows Server 2008 R2, 2012, 2016, 2019

HOPZERO – The ultimate data compromise prevention system

Summary of solution

HOPZERO Keeps your most critical servers and data safe.

HOPZERO has the tools and patented technology to stop server compromise.

HOPZERO limits the distance your data can travel to stop data breaches.
It stops the most common security issue, Ransomware.

Our system stops DataTravel™ — blocking server compromise.

- **Limits server data travel to the data centre or organization perimeter at a TCP/IP network layer level.**
- **Reduce your attack surface by 99.9%. Mathematically proven.**
- **Stops the ransomware kill chain, alarms and catches phishing / ransomware attempts.**
- **Limit the distance your IoT device data can travel.**
- **Map visualization of exfiltration and attacker activities.**
- **Map visualization of where your data is located around the world.**
- **Map visualization to see what web spiders can access your critical data.**
- **Map visualization of bottle necks in your network.**
- **Stop the hackers or malicious insiders taking your data.**
- **Not affected by Data poisoning techniques.**
- **No more data breaches to report or loss of reputation.**
- **Extremely comprehensive compliance reports.**
- **Smart Logs provide cogent metrics improving security evidence.**
- **Ai used not to block but to confirm the correct data travel limits.**
- **Has no performance degradation on your network.**
- **No user intervention required to protect your data 24x7.**
- **Is extremely affordable.**

Controls at the network layer level can be applied to all applications, thus, they are not application-specific.

It is the fundamental core design that **future-proofs** against the everchanging behaviour and methods used by cyber criminals.

Harmony IoT – Enterprise-grade defense for your airspace

Summary of solution

Harmony IoT stops:

- **Man in the middle attacks within your airspace.**
- **Ransomware attacks within your airspace.**
- **Monitors what is normal and unusual activity constantly.**
- **Block unusual activity without user intervention.**
- **The option to track a and notify if a specific device enters your airspace.**
- **The protectors are connected to the largest wireless computing devices and activities database in the world.**
- **Total visibility of all devices within your airspace.**

Simple setup without connecting to your network or complicated IT configuration.
Installs in minutes.

SENSITIVE INFORMATION AND ONGOING OPERATIONS FROM IoT THREATS.

- Phones, TVs, watches, coffee makers, air conditioners and lightbulbs are all getting smarter and connected. Your enterprise is likely blind to what all these things are doing, which can be a lot!

- The number of Internet-connected things (IoT) is expected to reach 50 billion by 2021.

- Most of these things communicate via hotspots, unmanaged or public wireless networks, and peer-to-peer wireless connections, making them invisible to traditional management and security systems.

- Most are built with convenience, not security in mind, making them easy targets for attackers.

- As a result, these seemingly innocent things are being used to pierce enterprise defenses to eavesdrop, steal data, and completely compromise digital assets.

IT IS TIME TO SHINE A LIGHT ON ALL THESE THINGS AND PROTECT YOUR ENTERPRISE'S SENSITIVE INFORMATION AND ONGOING OPERATIONS FROM IOT THREATS.

It's time to protect against the not so innocent.

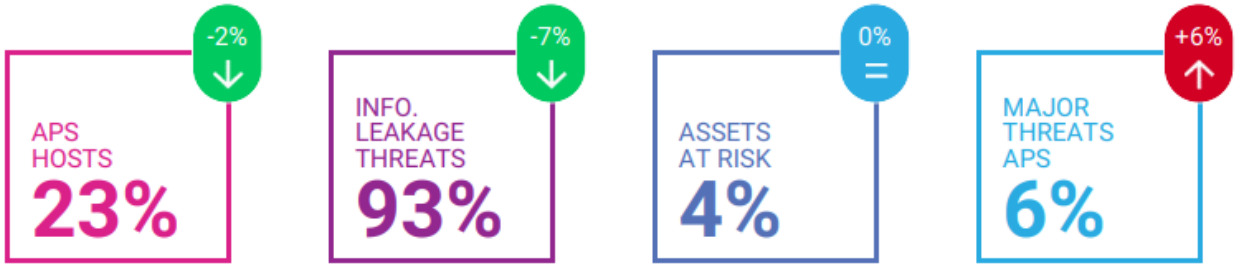
It's time for Harmony IoT.

Harmony Purple – Vulnerability Prioritization Solution like no other

Summary of solution

Automated Grey Hat Penetration and risk-centric vulnerability prioritization test capable of running up to 8 million simulations a day.

- World's first machine-based (Ai patent) penetration testing solution that thinks like a Hacker. Performs around-the-clock penetration testing and predicts Attack Path Scenarios™. Founded 2014.
- A very low network foot print on enterprise operations and critical systems due to silent patented 10 packed scanning technology. Uses less than 3% network bandwidth running 24/7.
- Can be deployed in global, multi-site organization. Information can be shared across all sites to represent “Global Attack Path Scenarios™”.
- Enables GDPR Compliance by offering regular pen testing and vulnerabilities management which greatly reduces the risk of breach to your sensitive data.
- We find and validate Attack Path Scenarios™ that begin in the web and threaten your internal business processes and critical assets.
- Creates actionable insights based on critical vulnerabilities that threaten your business process with immediate alerts.
- On-Premise, in the cloud or hybrid installation for a true global view of your organisation’s cyber security posture.
- Now you can link your cyber security to your company’s business processes.
- Reduced resources needed for remediation.
- Live network mapping
- Create executive summary report for c-level and board members that’s easy to understand.
- Protects your business from ransomwares lateral movement getting to critical assets.
- Perfect for CPS-234 compliance.



About Us

Disruptech Pty Ltd is a proud Australia software distributor offering world class technology solutions.

We offer you some truly evolutionary solutions not seen in Australia before.
Some are so cutting edge, they have created a new category of cyber security of their own.

Having come from the MSSP/MSP world, we understand the challengers' companies face when dealing with distributors. So, here at Disruptech, we go out of our way to make things easier for you.

We offer -

- Cutting edge technology solutions to give you that competitive edge.
- Solutions that are easy to deploy and configure.
- Solutions that are highly affordable.
- And great technical support to back you up.

Rapidly generate more revenue for your business while offering your clients exclusive security solution that are easy to deploy and highly effective.

DISRUPTECH
TECHNOLOGY SOLUTIONS

1300-001-071

info@disruptech.com.au

www.disruptech.com.au