AVANTGARD

Cyber Security

WHITE PAPER

Version 1.0
Released: Jan 30, 2017

The worm is turning

For more than a decade, the hackers have mostly had it their way. There has been more to hack as information and business assets move almost completely on-line, more ways in as connections proliferate and every device you can imagine is joining the internet of things, and more smoke for concealment in the huge amount of technology noise jamming our environments.

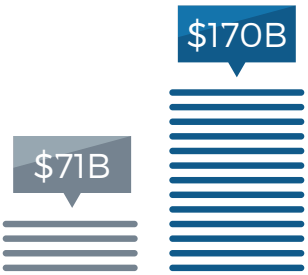
Finally, the empire, might just strike back.

Enter
ASSERTIVE DEFENCE

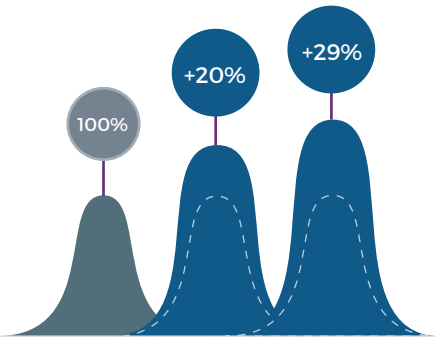
The battle of cyber-security has been tilted toward the hacker. Defenders in IT and infrastructure design have to monitor or block every door or window, every moment. The hacker only has to find one hole, once. This has led to cyber-defenders building thicker walls, more granular analysis and more and more agents to vet traffic on the system.

The effect of this is making cyber-security more and more expensive, more complex and harder to manage.

Deloitte[1] predict that the global spend of **$71B** on cyber-security in 2014 will grow to **$170B** by 2020.



Yet the number of successful attacks is growing.



The Australian Signals Directorate is reported as saying attacks on Australian businesses and government increased **20%** last year[2]. The amount of financial loss per breach is also increasing (globally up **29%** since 2013[3]). We are paying more to defend while suffering more successful attacks with higher losses.

1 http://www.smh.com.au/business/banking-and-finance/cyber-security-spending-to-grow-stevens-20151124-gl77e2.html
2 http://www.abc.net.au/news/2015-04-23/cyber-attacks-on-australian-businesses-rise-20-per-cent/6415026
3 IBM Ponemon 2016 Cost of Data Breach Study

This pattern is obviously not sustainable on cost alone, but has other managerial consequences besides money.

Cyber-defence has become **so complex** that very few really understand it including the practitioners and the sector is flooded **with jargon** and **myth**.
The definitions of success for an IT department are not well aligned to the board's and they can lead to self-protection, under-reporting and even concealment. **They often revert to simplistic strategies such as just spending more or buying from the larger (and more expensive) companies to trade on their reputations.**

For example, if you were a car manufacturer, how would you quantify the potential liability where an unfriendly actor might be able to hack your vehicles and kill your clients or even just track them? Yet your customers demand products loaded with interactively and embedded sophistication.

Most business managers are also not able to make good decisions about their own products, their infrastructure and their path to market. As well as generating a whole new suite of business risks, the possible reach of product liability continues to expand and is very untested at the edges.

The current approach just isn't working.

But the hacker has something to lose too

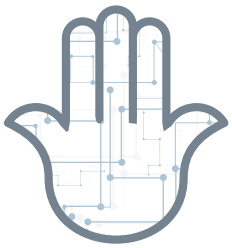
Contrary to common thinking, serious hacking is an **expensive business**. It takes time to assemble information on a target and a toolset to attack with. In many cases, the hacker has to probe the borders of the target gaining information about the defences and slowly building up a methodology or building up information for a credible spear-phishing attack. **These things take typically hundreds of hours, purchase of stolen data such as credentials and assembly of a customised toolkit**.

The effect is that hacking teams are very protective about what they have.

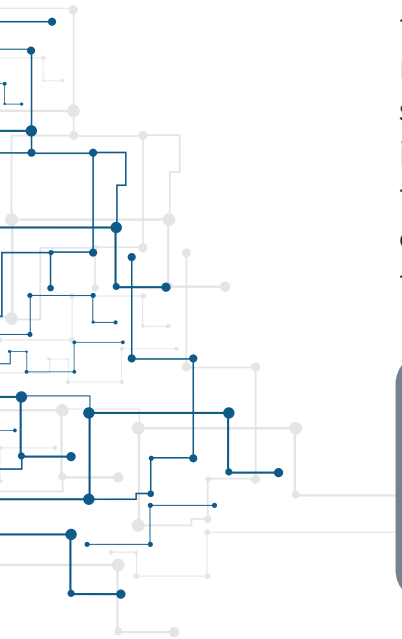
Assertive defence

Assertive defence means the defender **WANTS** to find evidence of an intention to attack, or an intrusion, because that can provide the means to characterise how the hacker will go about it and who the hacker might be. It will probably mean that the defender will know **where to look and what assets are in jeopardy**, and if an attack occurs, detect it more easily and provide the ability to find other areas of penetration even outside the organisation, such as compromised bot – armies. It will also help to trace the path back to the hacker, as the hacker will want to exfiltrate the information assets they are trying to steal.

There will be winners and losers here. Organisations adopting an assertive stance are more likely to successfully defend, but they will also be a less attractive target than the next organisation that is still just busy thickening the walls. **The devil takes the hindmost**. Having some big dogs that could get off the leash at a burglar might just mean he goes down the road to try the neighbours instead.



More than anyone else, we have the **Israelis** to thank for this new posture. This is clearly because their nation state is under perpetual threat for its very survival, but also because it has invested so heavily in it for decades. In the mandatory national service that every young citizen must undertake, the cream of those with maths & hacking skills are streamed into the intelligence and security services.



Israel probably produces more cyber-security sophisticates per capita than any other developed country. In our decade, it is responsible for by far the most number of technology and security start-ups per capita in the world.

The USA has heavily invested in **'elint ' – throwing electronic processing muscle and artificial intelligence at the problem to sift, detect and learn**. Smart routers, machine intelligence and software agents are the order of the day to detect threats, analyse patterns and intervene in suspect data flows.

ELINT	electronic intelligence
HUMINT	human intelligence

The Israeli approach has been more **'humint' - to analyse the mind of the hacker to understand how he/she thinks and go about their work**.

As a result, a number of new approaches have begun to appear from the Israelis that are starting to make a difference. The first is the outward-looking threat assessment. Rather than 'thickening the walls of the castle' or sniffing the air inside for a bad odour, **they stand on the parapet with telescopes and infrared to look at what the enemy is doing and they aggressively patrol outside the perimeter into the dark and deep webs where the hackers live and operate.** The anonymity of the criminal web that protects the hacker enables the savvy defender to also move like a hacker, untraceable and undetected. This allows a client to get a real, unvarnished evaluation of what has **already been stolen from them** – saleable data, credentials, URL's, etc.

It will also show up signs of **an exploit** being planned through exchange in knowledge of weaknesses and exploit opportunities or a call to arms to assist. If you own a brand, chances are things have already been extracted from you and black hats are comparing notes about what they learned.

Knowledge of activity in the hacker community focused on your organisation not only tells you where to look in your own systems, **it helps you shape your security posture with maximum effect**. Even better, it works for insider and collusion threats as well as external hackers.

Next, there is the concept of a deception.

Concept of a deception

The deception strategy assumes that a proficient hacking team will find a way in, often through just **one machine, network share or database**. They will then begin to move laterally to explore the environment, looking for the valuable assets which may be repositories of data or points of control they can seize. This lateral movement occurs through examining network **share tables, network traffic breadcrumbs, cookies between machines, contacts, identities or other tables of access control**. Each time they breach another machine or share, they will look to see what that machine can connect to and continue to explore.

If network shares can be set up that are in every sense genuine, and are linked and '**breadcrumbed**' across the network, but in fact only exist to be visited by hackers, we have the potential for an irresistible decoy trap.

Since the only reason for anyone to be on that machine or share is to explore as a hacker, it creates a unique **opportunity to perfectly fingerprint a hacker's approach and toolkit**. This means you can not only find where else they have penetrated in your system, it may allow you to find their other targets across the internet, and also makes them vulnerable themselves to a counterattack.

The Israelis LOVE to counter attack.

Exfiltration

Another area of focus is exfiltration. **Most hackers want to extract valuable data from your environment.** This means outbound traffic that otherwise would not occur and will have different characteristics. The defender seeing it, following it or modifying it on-the-fly to destroy its commercial value and make it easy to find in the wild (to prosecute), changes the risk proposition to the hacker completely.

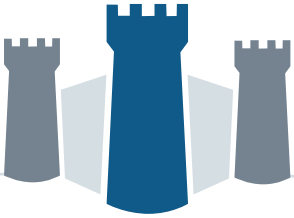
A whole new set of outcomes **become possible**

- Zero false positives, due to a combination of outward-looking threat assessments and decoy fingerprinting
- Realtime blocking of ransomware attacks through obfuscation technology
- Exposure of hacker's tool kits, thus neutralising attacks
- Effective blocking of all unauthorised data exfiltration
- Effective trans-national apprehension, prosecution and penalisation of cyber criminals

HOW IT HAS BEEN	WHERE WE'RE GOING
Passive/reactive blocking of threats	Assertive intelligence reaching out into the hacker's world. Active deception & decoys that expose and destroy the value of hacker tool kits
Rely on off-line backup to recover from Ransomware attacks	Obfuscation techniques that stop ransomware from initiating
Advanced Persistent Threats (APT) are invisible to all but the most sophisticated defenders	Deception and decoy tools that expose even the most sophisticated APTs
Victims find out what was stolen only after the hacker hits their bank account or the scandal hits the media	Dark web intelligence that hacks the hackers and exposes their attempts to sell stolen assets and credentials

This is not all just a distant hope

The Israelis have made these tools **real** and **survive** by them. They are used now by the **Israeli National CERT**. What is new is making them available in productised form to parts of the wider world, and the case studies of deception & decoy solutions that have already uncovered multiple previously unknown APT's are building up. So are the successes in discovering an attack intention before it launches and effectively neutralising it.



Several Israeli vendors are actually providing a warranty up to a million dollars against a breach where their product was correctly installed and maintained.

The question is whether Australian risk leaders can adapt to the new philosophy take the fight back to the hackers.

That way, we might just win some rounds.