6th of July, 2023

Cyber-immunize your organisation – start by changing your beliefs.

By Zafehouze.com

Introduction

"To be, or not to be secure, that is the question".

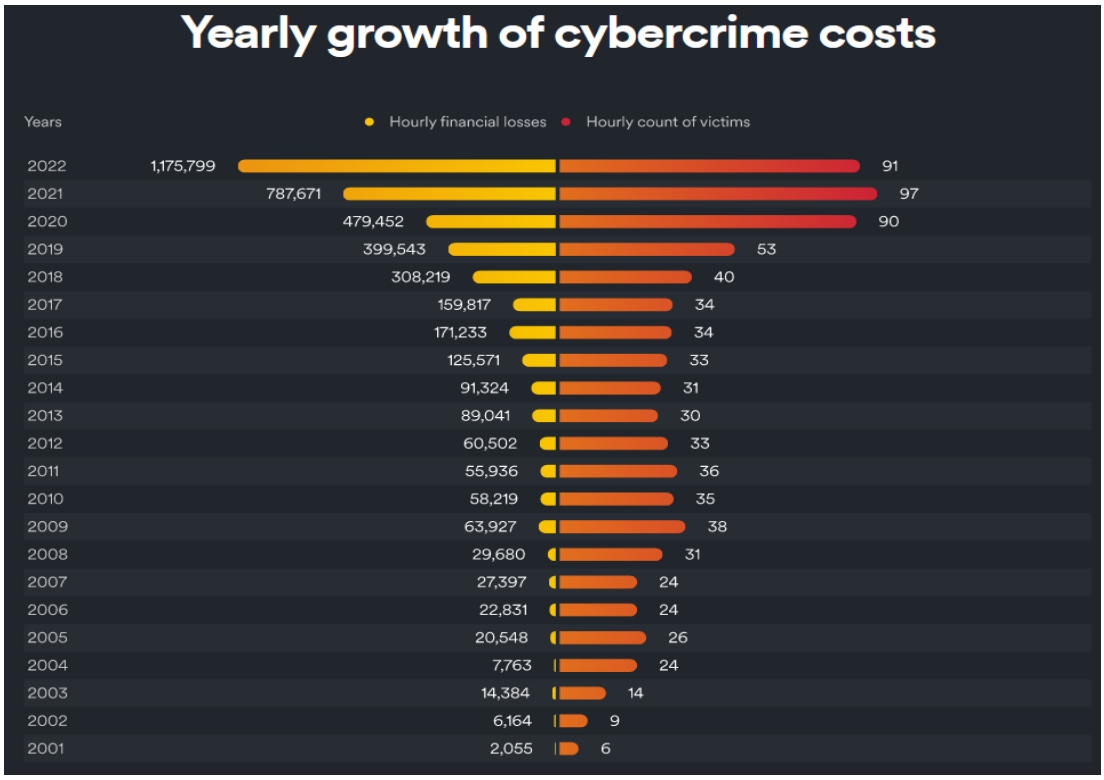
In Shakespeare's Hamlet, the phrase reflects the protagonist's contemplation of 'existing' or 'not existing', the choice of life and death. Similarly, cybersecurity poses an existential threat to modern society. The increasing reliance on technology and interconnected systems exposes organisations to potential cyberattacks, which can disrupt critical infrastructure, compromise personal data, and even endanger lives.

"To secure or not to secure, is NOT the question" anymore. It's "***to change or not to change – which is the question***".

This Zafehouze whitepaper is trying to come up with a few viewpoints to how organisations can keep on existing – and what better start than to face some insights from sources who live and breathe in this space – and whom can hopefully inspire 'change'.

Due to the growing digitization, the value of sensitive data, the economic impact of breaches, the complexity and the velocity of cyber threats, national security concerns, privacy and trust, regulatory requirements, and the rapid evolution of technology, it's crucial for organizations, and governments to take a different approach to cybersecurity **adopting proactive measures** and NOT stick to reactive measures, in order to protect against cyber threats.

FBI, Mandiant, CrowdStrike, Gartner, IBM, PwC, Deloitte and many other organisations publish relevant, but devastating report – one after the other.



Discussion document – comments? Thoughts? Please reach out to frederik@lifutechnologies.co.za

6th of July, 2023

The picture is from the yearly FBI report – no surprise the rate and cost of data breaches have increased since 2001.

- Victim count increased from 6 **per hour** in 2001 - to 97 in 2021 … a **1,517%** increase over 20 years.
- The average cost of a data breach **per hour** has increased from **$2,055 in 2001.** 20 years later the hourly **loss rate reached $787,671** up 383 times. In 2022, it landed at $1.175 million. Using the same growth rate, average losses will reach a **whopping $301.6 million** – ***per hour!*** in 2041.
- In 2022, **data breaches cost businesses an average of $4.35 million** – up from $4.24 million in 2021.
- The increasing threats, force organisations to take cyber security seriously. 73% agree that **cyber security concerns now need action.** 78% say they will increase investment in cyber security in the next 12 months.

But invest in what? more of the same?

Can organisation afford hourly loss rate in the millions range? If **$300 million per hour** is reached, probably both organisations and cyber-crime will be extinct.

The cost of data breaches has steadily increased as changes in the workplace and more advanced penetration methods embolden cyber criminals.

It's roughly 40 years ago, the digitization of the world started. The cost of data breaches has steadily increased as changes in the workplace and more advanced penetration methods and new hunting grounds embolden cyber criminals. Along grew organisations seeing data "as a new natural resource" generating massive profits, and a cyber-security industry, that despite a **market of $250 billion p.a. hasn't succeeded.**

CrowdStrike investigated how fast Nations State Attackers (NSAs) compromise networks and in all fairness, western NSA's are not slow either.

- Russian **NSAs use less than 20 minutes** from initial attack till they move laterally around the network.

CrowdStrike Actor Group Name	Country of Origin/Type	Average Breakout Time
BEAR	Russia	00:18:49
CHOLLIMA	North Korea	02:20:14
PANDA	China	04:00:26
KITTEN	Iran	05:09:04
SPIDER	eCrime	09:42:23

Chinese state-sponsored attacks dominate exploitation of zero-day vulnerabilities. Over 50% of all zero-day vulnerabilities can be linked to known cyber espionage actors or intentions. In 2022, at least 13 zero-days have with moderate to high confidence been used by cyber espionage organizations.

Mandiant's (now Google) insight into Fortune 500 global organisations, servicing more than 900 million customers, show it doesn't really matter how many layers of 'Defending the Castle' (DtC) measures, security controls and solutions, are implemented. The organisations had a total 123 different cyber-security solutions – minimum 30 in full function in combination with a 24/7 Security Operation Center service in place (inhouse or outsourced).

- **Only 9% of attacks generated security alerts – and 53% of successful intrusions remained undetected.**
- **Only 4% of reconnaissance activity generated an alert.**
- **In 67% of mal-/ransomware infiltration cases, the security controls did NOT prevent or detect detonation.**
- **65% of the time, security tools were UNABLE to detect or prevent attempts to bypass security policies.**
- **Malicious file transfers were only detected 29% of the time – half was missed, the rest generated an alert.**

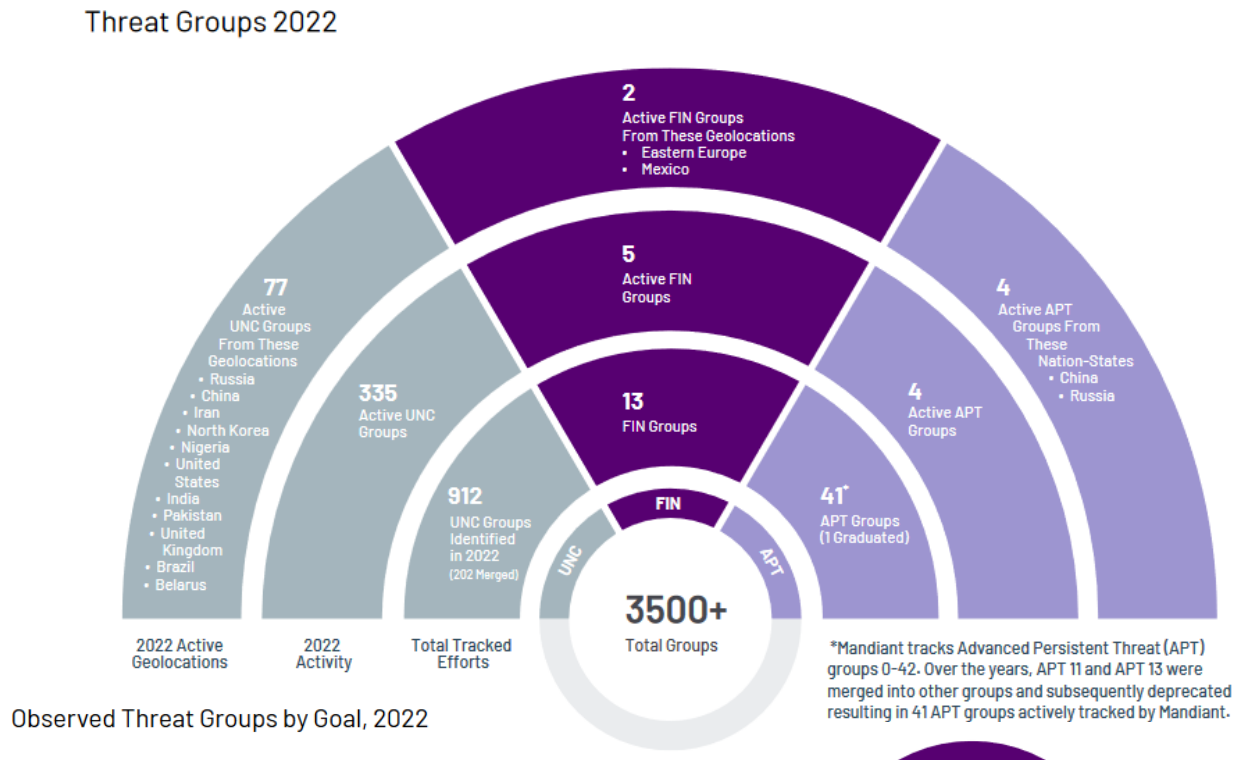
Just over 25% of all attacks were detected by the implemented security tools, AFTER the infiltration was successful.

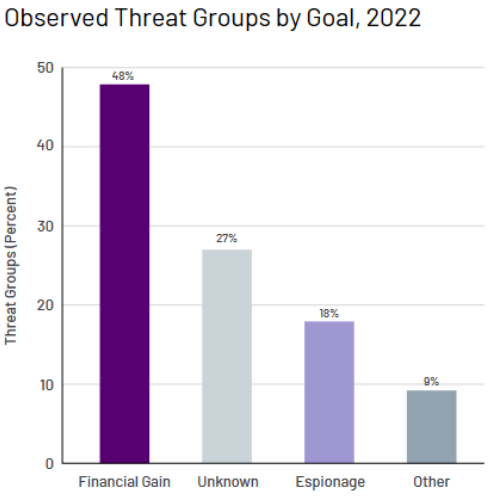
Discussion document – comments? Thoughts? Please reach out to frederik@lifutechnologies.co.za

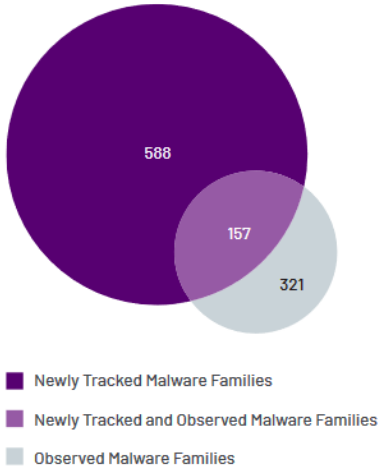
Mandiant experts determined that many of these cases are the result of unchanged default configurations, security events never making it to the SIEM solution, unexpected infrastructure changes, skills shortage, the lack of tuning and tweaking after deployment, and the inability to force controls testing.

Lastly – these numbers have been around for a while – but the World Economic Forum (WEF) reconfirm Cyber-crime being the third-largest economy after US and China, with an estimated turnover of $1,600 billion ($1.6 trillion) p.a.

Cyber-crime **impacts any organisation** and the damage-cost hits $8 trillion in 2023 – expected to rise to $10.5 trillion in 2025. Links can be found in the reference section. Here's a bit more from the 2023, Mandiant report:







What is the background for their 'success'?

Oganisations should understand there are too many threat actors and vulnerabilities to track, mitigate, or otherwise address while maintaining business operations. It's imperative that organisations switch to an approach, prioritizing security efforts based on modern access technology, relative risk and on-the-ground pragmatism.

Cyber-criminals use various TTPs – that is tactics, techniques and procedures to keep detection-rates as low as possible and TTPs form their strategy to breach organizations and their networks.

The most common methods are listed on the next page.

1. **Phishing;** a technique where cybercriminals send fraudulent emails, messages, or website links that appear legitimate to trick users into providing sensitive information; login credentials, financial data etc. With this information, cybercriminals can infiltrate the organization's systems.
2. **Malware Attacks;** such as viruses, worms, trojans, or ransomware, is designed to gain unauthorized access or cause harm to computer systems – often malware is distributed through infected email attachments, malicious websites, or by exploiting software vulnerabilities. Once inside, it will compromise data, steal information, or provide backdoor access for further attacks.
3. **Social Engineering;** involve manipulating individuals into revealing sensitive information or perform actions that assist in a cyberattacks. This can include impersonating trusted individuals, using psychological manipulation, or exploiting human vulnerabilities to trick employees into providing confidential information or granting access to secure systems.
4. **Password Attacks;** using various techniques to crack or guess passwords, including brute-force attacks, dictionary attacks, or using stolen password databases from previous data breaches. Once they obtain valid login credentials, they can gain unauthorized access to sensitive systems or escalate privileges within the network.
5. **Exploiting Software Vulnerabilities:** Cybercriminals actively search for vulnerabilities in software, operating systems, or network devices. They leverage these vulnerabilities to gain entry into systems by using techniques like SQL injection, cross-site scripting (XSS), or remote code execution. Once inside, they can move laterally through the network and access sensitive data.
6. **Insider Threats:** In some cases, employees or individuals with authorized access to an organization's systems may intentionally or unintentionally aid cybercriminals. This could involve sharing sensitive information, misusing privileges, or neglecting security protocols. Insider threats can be difficult to detect, as they often have legitimate access to critical systems.
7. **Supply Chain Attacks:** Cybercriminals may target third-party vendors or suppliers that have access to an organization's network. By compromising these trusted entities, they can gain entry into the target organization's systems. This method has been increasingly utilized to target organizations with robust security defenses and many organisations don't manage third-party access very well.

All 7 relates to the '**legacy network-centric reactive defense model**' aka "Defending the Castle" – focusing on protecting computers and other resources **in networks and associated infrastructures.** This enforce organisations to implement multi-layered defenses – e.g., 'ring-fencing the network' with a firewall (like a castle wall), and includes employee education, strong access controls (guards), regular software patching (fixing the castle wall), network segmentation (more gates), intrusion detection systems (more guards), security operations and services (advisors) for threat detection, analytics and robust incident detect and response plans.

"Are more band-aid solutions, <u>reactive</u> countermeasures and tons of consultancy, the cure?"

A PwC study revealed 2/3 of SMB's feel that they **do not** have the in-house skills to deal with data breaches and turns to Managed Service Providers for mitigating this issue; 89% as of 2022, up from 74% in 2020.

That's 9 out of 10 SMEs – but the PwC study also revealed that 9 out of 10 organisations are breached within a 12-month period. How does that contradiction come around?

It's called 'the shared responsibility model', but it's not so shared. All organisations ARE fully responsible for their own security – it cannot be outsourced or put on any external party!

Management bodies face scrutiny

Directives coming up around the world (e.g., EU's NIS2) emphasize this. They place potential penalties on management bodies, now being held liable for breaches, and temporarily banned from acting in the same job-role. These management bodies don't have the skills either – nor the competences, experience or maybe even desire to understand cyber in-dept.

The PwC study also revealed that almost 1/3 of their 3,500 respondents expected an increase in cyberattacks against manufacturing (OT) environments exploiting vulnerabilities in legacy systems, affecting production-stop, as systems are shut down in order to prevent damage spreading via the supply chain.

.. and 82% of the CIO's stated they don't think the current cyber-security solutions are effective!

4 out of 5 CIO's seems to understand the catch-22 in Cybersecurity.

What management bodies should know

They just want to operate their business with as little, or no risk as possible – and this means, organisations have to take control of their destiny, employing innovative new IT and Cyber-security skills, implement technology that can manage systems, users, data and applications in ways, neither users nor cyber-criminals can subvert, whether by malice, accident or trickery.

The sad truth is – today organisation can spend $1+ billion yearly on Cyber-security solutions and services, and still get compromised in hours. Don't get lulled into 'the false security trap' you've read about above. Don't fall into the 'thanksgiving-turkey' mode, which up until thanksgiving show an increased 'happy index' – which one morning suddenly change.

The threat actors responsible for the majority of cyber based incidents in today's digital economy normally fall into the following categories:

- **Industrial Espionage** – Individuals or organization who seek classified and proprietary information, including market and pricing strategies, corporate financials, client information, product designs or formulas, research data and corporate vulnerabilities.
- **State-Sponsored Cyber Espionage –** Persons who are well-funded and supported by national programs with sophisticated capabilities to compromise and exploit vulnerable systems.
- **Criminals** – Persons who seek any data that can be sold or used for a profit.
- **Hacktivist/Recreational Hackers** – Hackers, both experienced and inexperienced, who operate using the latest techniques and tools to perform a network attack, sometimes for personal gain or as part of an organized group.
- **The Insider Threat** – Individuals already operating within organizations—legitimately or otherwise—can also pose a serious hazard.

'What to do' … that's the real question!

The IT evolution, the technology advancements have made any organisation vulnerable, and it's about time to do something about it. As indicated earlier, there are limitations to the efficiency and effectiveness of how current cybersecurity solutions work. Allow us to briefly cover a few.

Network-based security controls has certain limitations that affect its efficiency and effectiveness.

1. **Centralized Approach:** It relies heavily on centralized security controls and monitoring systems, and when centralized systems are compromised, it imposes severe consequences for the entire network.
2. **Inability to Address Insider Threats:** Network-centric security models often focus on external threats, such as external cyber-threats, malware etc. However, they can't effectively address insider threats, where individuals within the organization may intentionally or unintentionally cause harm to the network and its resources.
3. **Lack of Adaptability**: Network-centric security also struggle to keep up with rapidly evolving cyber threats, which often relies on predefined rules and signatures, which may not be sufficient to detect new advanced attack techniques and may even require manual configuration to stay effective, which is time-consuming and prone to human error.
4. **Blind Spots in Decentralized Environments;** such as cloud computing or distributed networks, the network-centric security model struggle to provide comprehensive visibility and control, leaving certain areas or endpoints vulnerable to attacks.
5. **Over-reliance on Perimeter Defense:** The network-centric model tends to focus on protecting the network perimeter through firewalls and access controls. However, with the rise of mobile devices, remote work, and cloud services, the network perimeter has become more porous and difficult to define. This led to gaps in security defenses and makes it easier for attackers to bypass traditional perimeter-based protections.

A different approach, that is actually not that different

Computers has to be 'connected' in order to communicate, for which two models are being used. One has 7 layers (OSI), the other 4 layers (TCP/IP) and relates to the Internet. The 4-layer model 'squeezed' a few layers together and is widely uses as many applications are browser based, but also opening up for a range of threats and vulnerabilities.

6th of July, 2023

All layers are open to various attacks forms. There are 350+ TTPs… tactics, techniques and precedures defined by MITRA ATT&CK and 950 vulnerable 'holes' to exploit.

(IP-address provided ->)

OSI	Protocol	Attacks	TCP/IP
Application Layer	HTTP, HTTPS, FTP, SMTP, DNS	Malware, DoS, SMTP Attack, FTP Bounce, Data Attack, Insecure HTTP, Browser Hijacking, Buffer Overflow.	Application Layer
Presentation Layer	Data Representation and Encryption	Malformed SSL, SSL Stripping, Unicode Vulnerabilities, Worms.	
Session Layer	WEB Sockets	Session Hijacking, DoS	
Transport Layer	TCP, UDP, SSL	TCP Flood, Desynchronization flooding, TCP Sequence Prediction Attack	Transport Layer
Network Layer	IP, ICMP	Spoofing, Hijacking, Ping Floods, MITM (Man in the Middle attacks)	Internet Layer
Data Link Layer	MAC, Ethernet	MAC Spoofing, collision, switch looping, traffic analysis	Network Access Layer
Physical Layer	Cables, Wi-Fi	Wire Tapping, Jamming, Tampering	

They both follow the same structure – once 'a device' is connecting to a network (the network layer), it receives an IP address, allowing it to 'talk' to all other IP addresses in the same network.

Networks in the 'good old days', resided 'inside' an organisation. This is not the case anymore – ***resources 'are now everywhere' and it has become a complex nightmare restricting everything to a "secure network"!***

Moving security from the network layer to the application layer – the whole security paradigm shifts. Suddenly many of the attacks cannot be successfully carried out. A proactive **Prevent & Protect Guard-Railed and Micro-Perimeter security** – two emerging concepts challenging the traditional security approaches are capable of turning the security paradigm upside down – literally eliminates 90% of all the attack-types – and by separating data, communication, application and services from the layers below, these layers are simply reduced to "connectivity facilitators".

Why hasn't that been done years ago, you might ask. It sure was. Prevent & Protect based technologies has existed since the mid 90'ies.

In recent years, research organisations like Forrester and Gartner – respectively define Zero-Trust (ZT) and Secure Access Service Edge (SASE). Both are frameworks, which are fully incorporated in Prevent & Protect.

In 2004, The Jericho Forum (UK) defined the first real Zero-Trust framework called "deperimeterisation" – this is also included in Prevent & Protect. At the same time a Danish organisation patented a technology leveraging ZT / SASE principles 5-7 years these were defined – and long before Cloud Security Alliance in 2013 defined 'Software Defined Perimeter' – which is also incorporated in Prevent & Protect.

A lot of other elements are incorporated, and some of these we go though below.

What is Prevent & Protect? Gard-Railed and Micro Perimeter-based Security?

Prevent & Protect enable access to any resource in IT, OT and/or IoT environments, automatically enforcing security policies and processes leveraging **guard-railed and micro-perimeter security principles** in order to establish the strongest security posture available and able to easily adapt to the ever-changing threat landscape.

As Prevent indicates – it's a proactive security methodology (not reactive). Protect, indicates that users, applications, data, services e.g., all resources, are protected in ways out-matching existing network-centric security methods.

Let's provide some further insight! – two things need to be visualized;

First: separating data, users, services and applications e.g., resources from the network infrastructure is needed – as one of the 'security first principles' are that 'networks are insecure'. Prevent & Protect should only use infrastructure to **'facilitate connectivity'.**

Discussion document – comments? Thoughts? Please reach out to frederik@lifutechnologies.co.za

Second: in a network-centric security model, segmentation is a key (and important) ingredient, and mainly provided by network-equipment vendors. Moving security to the application layer, software defined perimeter segmentation can now be enforced end-to-end.

Let's walk through these revolutionizing security practices:

1. **Guard-Railed security:** Traditional network-centric security practices have focused on perimeter-based security, where organizations build strong defenses around their network boundaries to prevent unauthorized access. However, with the rise of cloud computing, mobile devices, and remote work, the traditional network perimeter has become increasingly porous and difficult to define. Guard-Railed security takes a different approach by assuming that the network is already breached and focuses on containing potential threats within "security rails" or boundaries.

Guard-Railed security leverages and extends the ZT-framework where every user, device and network is treated as potentially compromised. It emphasizes strict access controls, continuous monitoring, and granular segmentation to isolate and contain potential threats within defined security boundaries.

By assuming that threats can be present both inside and outside the traditional network perimeter, Guard-Railed security helps organizations prevent incidents more effectively as security policies are defined up front and enforced automatically.

2. **Micro-Perimeter security**: Micro-Perimeter security complements Guard-Railed security by creating granular security boundaries around individual applications, services, or data assets. Rather than relying solely on network-level protections, micro-perimeter security focuses on securing specific components, assuming everything is compromised – the PC/device, the network, connections etc.

With Micro-Perimeter security, each user, device, application or service is treated as an independent security zone, with its own set of security controls, access and validation policies. This approach reduces – in fact eliminates attack surfaces dramatically and limits – in fact eliminates the lateral movement of threats within the network.

Prevent & Protect is created around these principles – and should an attacker (highly unlikely) be able to breach an application or service, these are constrained within its micro-perimeter and face barriers accessing other resources.

Prevent & Protect makes access to un-entitled resources impossible and Guard-Railed Micro-Perimeter security is particularly relevant in modern computing environments that rely on distributed systems, containerization, and microservices architecture. It allows organizations to apply tailored security measures to individual components, ensuring that the compromise of one component doesn't lead to the compromise of the entire system. As a non-interruptive, non-invasive and non-intrusive solution, created to meet the need for more resiliency and adaptable security – it challenge the traditional assumption that a strong perimeter defense is sufficient to protect an organization's assets – which it's clearly not.

By turning the security paradigm upside down, shifting the focus from perimeter-based defenses to containment and segmentation strategies, the Prevent & Protect approach provide organizations with enhanced visibility, control, and resilience in order to face even future sophisticated cyber threats and the changing nature of future computing environments.

When it comes to control frameworks, such as industry standards like NIST Cybersecurity Framework, ISO 27001, or PCI DSS, CMMC 2.0 and regulations like GDPR and NIS2, Prevent & Protect's foundation in Guard-Railed Micro-Perimeter security can easily be applied for enhancing the effectiveness of these frameworks.

Here's how you can incorporate Prevent & Protect into an efficient and effective architecture framework:

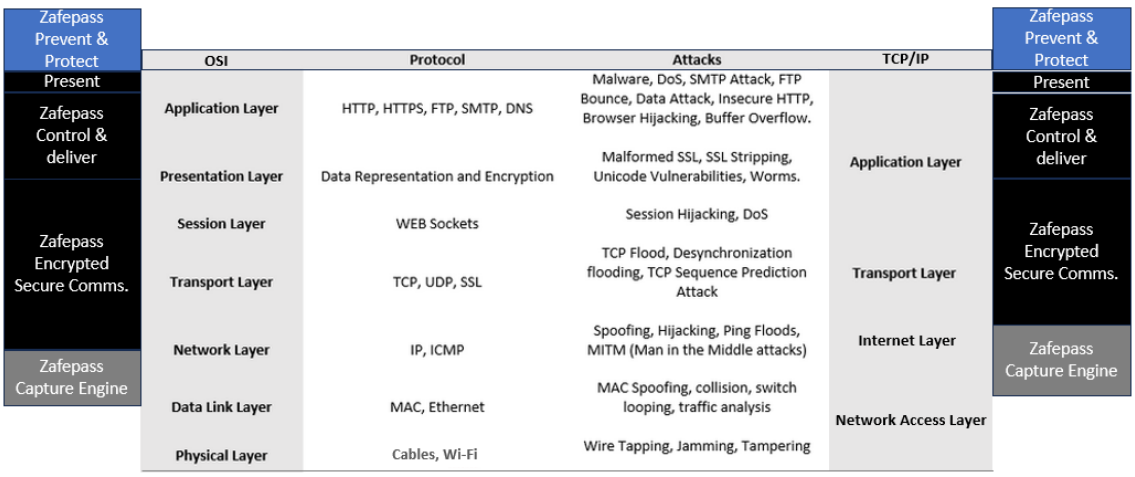
1. **Identify critical assets and risks:** Start by identifying your organization's critical assets and potential risks associated with them. This could include sensitive data, systems, applications, users or even

infrastructure(s). Conduct a comprehensive risk assessment to understand the potential threats and vulnerabilities.

2. **Map control framework requirements:** Review the control framework(s) and identify the relevant requirements that align with your organization's needs. This step helps you understand the baseline security measures and practices recommended by the framework.
3. **Establish security guardrails:** Define security guardrails as specific security policies, configurations, or controls that help enforce security requirements and reduce the risk of non-compliance. In Prevent & Protect based platform(s), guardrails act as automated checks ensuring implementation effectiveness.
4. **Automate guardrail enforcement:** Prevent & Protect enforce guardrails and continuously monitor security controls. Automated guardrails can perform real-time or near-real-time checks, generate alerts or notifications, and provide feedback to system administrators or security teams.
5. **Enhance continuous monitoring**: Prevent & Protect enable setting up a robust monitoring system to track the effectiveness of all security controls and guardrails. This involves regular security assessments, vulnerability scanning, log analysis, and potentially also intrusion detection systems on the network layer for resilient operation (although the infrastructure should be following redundancy guidelines). Continuous monitoring helps identify any deviations from established guardrails and control requirements.
6. **Enhance Incident response and remediation:** Prevent & Protect will benefit incident response plans outlining the steps to be taken in case of a security incident or non-compliance with control requirements. The plan should include preventive incident measures as well as incident detection, containment, eradication, and recovery procedures. Make sure to document lessons learned and apply remediation measures to prevent future occurrences. Learn from events happening and update the security policies in the Prevent & Protect platform.
7. **Periodic control framework review:** Regularly review and update the control framework to align with evolving security threats, regulatory changes, and industry best practices. Conduct periodic audits and assessments to ensure compliance with the control requirements and adjust the policies (guardrails) in the Prevent & Protect platform as needed.

The specific implementation of a Prevent & Protect platform may vary depending on the control framework and the unique organizational requirements.

The Zafepass Prevent & Protect platform is easily implemented – and will overall capture any “communication” on the Network og Internet layer – encrypt as much as possible and use the other layers up to the presentation layer as facilitators getting the data through to the user-screen. How it’s done is too technical to explain in this document.



The point to be made is – that a security-centric culture based on Guard-Railed Micro-Perimeter principles, could prove crucial for organizations to prevent unauthorized usage and the protection of their sensitive data, systems, and even infrastructures from cyber threats. Where other platforms involve everyone in the organization understands the importance of security and actively participate in maintaining security measures, and continuously strive to improve security practices – Guard-Railed Micro-Perimeter security enable the creation of a security-centric culture **without** this involvement.

Discussion document – comments? Thoughts? Please reach out to frederik@lifutechnologies.co.za

Users don't have to become 'min-security-experts' or be 'concerned-they-do-something-wrong' – they can't perform actions that could compromize the entire organisation.

Executives should understand that a preventive mindset also help complying with any upcoming regulations as well as lowering the need for comprehensive programs for education and training in security, raise awareness about security risks, best practices and policies – and the already lost battle trying to constantly being 'on-top, 24/7'.

Prevent & Protect is designed to only provide what is needed for users to do their job , thereby fostering a workplace where employees feel comfortable reporting security incidents, potential vulnerabilities, or suspicious activities without fear of retribution. It helps establish channels for reporting such incidents and ensure they are taken seriously and addressed promptly – as Guard-Rail (security policy) changes are enforced in real-time.

Fighting Cyber-criminals leaves no time for complex update routines and lengthy implication discussions.

Creating a security-centric culture starts by having the right vision. Organisations should select the right solutions for the right job.

Prevent & Protect can significantly reduce the cyber-criminal activity risk, preventing operational damages and protect the organisations valuable assets in any environment.