ARMATA
CYBER SECURITY

_ARMATA WHITEPAPER

Cybersecurity in a New World_

WHITEPAPER CONTENTS

MARKET OVERVIEW

In 2020, instances of malware increased by 358% and ransomware by 435% compared to 2019. As more companies push to embrace digital transformation and equip employees to work in a distributed environment, the focus has been on Cloud enablement. However, business and technology leaders must remain cognisant of how best to secure employee endpoint devices while keeping the impact on productivity to a minimum.

Instances of evolving malware and ransomware are increasing, making it difficult to effectively combat using traditional solutions. Attacks have intensified on corporate networks and endpoint devices given how people are working remotely. Many of the most damaging attacks remain hidden for months, giving the hacker access to sensitive corporate data. Attackers can then encrypt this compromised data at any time, resulting in significant damage to an organisation. And because a breach can stretch back for a long time, it negates some of the benefits of making backups as the restored data could be infected as well.

Then there is the growth of social engineering attacks thanks to the increasing number of people connecting on sites like Facebook, Instagram, Twitter, and LinkedIn. Just as with malware and ransomware, social engineering and password hacks are increasingly sophisticated with any individual or company, regardless of size, country, or industry sector, now a target.

The growing sophistication of all these cyber threats means that it is just as easy for the head of cybersecurity at an organisation to be compromised as the receptionist. And while events of the past two years have resulted in end-users and businesses becoming more cybersecurity savvy, much still needs to be done to curb the threat landscape as we head into 2022 and beyond.

Even prior to the pandemic, organisations had begun putting in place elements to manage distributed employees whether that be through incorporating remote desktop solutions or virtual private networking (VPN) capabilities. But since the start of last year, businesses have had to deal with an influx of connectivity challenges as employees needed remote access to corporate resources to remain productive.

As part of these challenges, organisations had to address common misconceptions around cybersecurity when it comes to remote working environments. For instance, many seem to think that a VPN is an effective defensive measure even though it is not. It is merely a tunnel to the firewall so users can authenticate themselves. During the lockdown, many employees have been reliant on their personal devices for work. The resultant surge in VPN tunnels only exacerbated existing security challenges and meant an increase of people having access to the companies' data remotely as well as increasing the number of potential attack vectors

Without proper endpoint protection in place (beyond simply relying on an antivirus solution), an organisation and employee remain at significant risk especially as remote users are not always connected to the VPN or behind a next-generation firewall.

THE CHANGING CYBERSECURITY LANDSCAPE

The average cost of a cyber breach has risen to approximately R4-million. For many South African small to medium enterprises (SMEs), recovering from this is not possible. Compare this to the minimal monthly costs of maintaining a security strategy that prevents breaches, and the reward far outweighs the potential risk.

South Africa is the 3rd most targeted country in the world when it comes to cyberattacks. In the first half of this year, the number of cyberthreats across South Africa (31.5 million), Kenya (32.8 million), and Nigeria (16.7 million) increased significantly. These threats can be categorised as criminal (80% of attacks), targeted (19.9%), and advanced (0.01%). The advanced grouping is significantly more sophisticated and features increased investment from attack groups. Unfortunately, both criminal and targeted threat vectors learn from the advanced category to enhance their own attack techniques

Ransomware has become the most significant threat vector targeting users and organisations in these countries. For instance, South Africa saw 23 000 different malware threats last year, followed by Kenya (22,000), and Nigeria (5,000). All this is contributing to the Middle East and Africa cybersecurity market predicted to top $23 billion by 2023, growing at an annual rate of almost 12% year-on-year during the 2018 to 2023 monitoring period.

NEW THREATS_

The growth of 5G and Fibre access across the continent means hackers have new platforms to exploit. Furthermore, advanced threat actors will buy network access from other cybercriminals. This will also result in increased collaboration between these cybercriminals and cyber gangs as they look at more effective ways of achieving their objectives. Different gangs will also start specialising in tools and other methods to better advance penetration. As people and companies rely more on technology, the number of threats will continue to increase. People must accept the risks of living a connected lifestyle, but most also embrace the technology and tools available to safeguard themselves.
While cybersecurity currently relies heavily on human input, technology is becoming better at specific tasks than we are. Every technology improvement brings us slightly closer to supplementing human roles more effectively.

Among these developments, a few areas of research are at the core of it all:

- Artificial intelligence (AI) is designed to give computers the full responsive ability of the human mind. This is the umbrella discipline under which many others fall, including machine learning (ML) and deep learning (DL).

- ML uses existing behaviour patterns, forming decision-making based on past data and conclusions. Human intervention is still needed for some changes. This is likely the most relevant AI cybersecurity discipline to date.

- Deep learning (DL) works similarly to ML by making decisions from past patterns but adjusts on its own. DL in cybersecurity currently falls within the scope of ML.

- As we explore the possible implications with security in ML and AI, it is important to frame the current pain points in cybersecurity. There are many processes and aspects we have long accepted as normal that can be treated under the umbrella of AI technologies.

  Despite all the glowing dialogue around the future of this form of security, there are still limitations to be noted:

- ML needs datasets but, may conflict with data privacy laws. Training software systems requires plenty of data points to build accurate models, which does not meld well with 'the right to be forgotten.' The human identifiers of some data may cause violations, so potential solutions will need to be considered. Possible fixes include getting systems to either make original data virtually impossible to access once software has been trained. Anonymising data points is also in consideration, but this will need to be examined further to avoid skewing the program logic.

- The industry needs more AI and ML cybersecurity experts capable of working with programming in this scope. ML network security would benefit greatly from staff that can maintain and adjust it as needed. However, the global pool of qualified, trained individuals is smaller than the immense global demand for staff that can provide these solutions.
- Human teams will still be essential. Critical thinking and creativity are going to be vital to decision-making. As mentioned much earlier, ML is not prepared or capable of doing either and neither is AI. Companies will have to use these solutions to augment their existing teams.

BEYOND THE TRADITIONAL AV SOLUTIONS

The fact is that IT teams must continually adapt to cybersecurity threats. Anti-virus and firewall solutions are no longer sufficient. Things like email security tools that evaluate the content, and endpoint detection and response (EDR) solutions that are designed with artificial intelligence to examine application behaviour have become increasingly important to implement especially with the increased number of remote users. Cybersecurity is now all about adding layers of defence as the threat landscape evolves.

For instance, polymorphic viruses circumvent traditional anti-virus solutions that are signature-based. And then next-generation firewalls provide more effective defence over legacy ones that are rule-based. It is about fighting the proverbial fire with fire. As hackers get access to more sophisticated tools to perpetrate attacks, so too must organisations use more advanced techniques to defend their data, systems, and infrastructure. The right solution also requires the right Managed Security Services. Like EDR and MDR (Managed Detection and Response).

THE IMPACT OF THE REGULATORY ENVIRONMENT

The General Data Protection Regulation (GDPR) of the European Union (EU) and the Protection of Personal Information Act (POPIA) in South Africa requires companies who hold data of their citizens to put sufficient measures in place to safeguard this data. These businesses are accountable in case of a data breach that results in the theft or leaking of personal information.

In South Africa, the penalties for failing to comply with POPIA include a maximum of a R10 million fine or imprisonment for a period not exceeding 10 years or both, for serious offences; and a fine or imprisonment for a period not exceeding 12 months or both, for less serious offences. POPIA was put into full effect on 1 July 2020, with local organisations being given a year's grace period initially. The Information Regulator has stated that there will be no further exemptions, meaning that local businesses have had to be fully compliant by 1 July this year.

And then there is still the cost of identifying the root cause of an attack or compromise to consider. With costs potentially running into the millions, hundreds of millions or even billions, organisations need to do more than pin their hopes on protections built-in within operating systems and basic firewalls and antivirus software. They need to take a holistic and proactive approach to defend their networks, devices, software and data from attacks, loss, or unauthorised access by using people, technology, and processes to create strategies to protect data, ensure business continuity and safeguard against reputational and financial loss.

Over the past two years, local businesses have become more reliant than ever on online and cloud services to interact and engage with customers and even sell their products and services. But threats are increasing daily and have become more dynamic and complex

Defensive Measures_

According to POPIA, companies must take appropriate measures to protect personal information against unlawful access or processing, as well as loss, damage, or unauthorised destruction. In a nutshell, it is all about first getting consent from an individual, and then putting in place policies, procedures, and technologies to ensure proper protection and confidentiality of personally identifiable information, from point of capture to transmission, processing and storing.

Regardless of size or industry sector, companies must become more diligent in identifying all their assets, looking at where and how data is stored, discovering what information sits on every system across the business, and more. Systems are also continually changing as updates are rolled out, and controls and policies need to be put in place to keep track of all information.

Corporate Responsibilities_

From a policy perspective and considering the impact of POPIA and other regulatory aspects, a company must make sure that users only have access to the data and systems central to their job roles. While this has always been important, it was less of a concern as employees would generally only access sensitive data while within the relative safety of the corporate network. But with employees at home becoming easier targets, the risk of lateral movement from one compromised device must be kept as low as possible.

The organisation must therefore understand how its data is being accessed and the applications that are accessing it. By putting endpoint protection and multi-factor authentication in place to enhance existing perimeter solutions, companies can manage remote workers in a more secure way.
For organisations, this means a radically evolved playbook when it comes to cybersecurity best practice. From the traditional firewall, anti-virus, anti-malware, and mail protection, to endpoint, Active Directory, and Zero Trust, they must either extend their in-house security 'battle box' or move to platform as a service to fulfil the security function.

As such, rather than just implement measures and hope it does the work, it is becoming increasingly important for organisations to carry out regular penetration tests to uncover exploitable vulnerabilities and identify the impact to the business - before a hacker does. Ongoing testing militates against future issues and provides assurance of the security of a system, evaluates how a potential threat actor could gain access, prioritise gaps to be dealt with and be better equipped to protect themselves against cyberattacks.

Partner-approach_

Businesses, therefore, need to turn to trusted partners who fully understand the requirements of regulation such as POPIA, as well as cybersecurity, data privacy and more, as well as use trusted methodology – tailored to meet the customer's environment - that considers guidelines from sources such the Open Web Application Security Project (OWASP), Payment Card Industry (PCI), METRE Attack Framework and the Technical Guide to Information Security Testing and Assessment.

At the very least, these tests should encompass the following:

- Gathering publicly available information – using sources such as search engines and websites to map out an organisation's public footprint and point out areas of concern
- Network scanning – performing automated sweeps of IP addresses of systems provided and discovered from on-network and off-network sources
- System profiling – identifying operating systems and version numbers running on the system for further testing
- Service profiling – identifying services and applications running on systems, as well as their version numbers for further testing
- Vulnerability identification, validation, and exploitation – potential vulnerabilities are identified and validated to minimise errors (false reports of problems). This involves attempts to exploit the found vulnerability

There is also a growing need to drive awareness around POPIA to build familiarity with the regulation and to ensure that employees working with personally identifiable information are fully aware of what the Act requires from them.

INTEGRATING CONNECTIVITY & SECURITY

It is easy to think of connectivity and cybersecurity as two unrelated topics. After all, these come across as completely different products. However, they are more intertwined than business decision-makers may expect. Fibre as a connectivity medium is vastly superior in terms of safety and overall security (think the high instances of copper cable theft in South Africa). Furthermore, its fast speeds make data transfer quicker and less prone to interception. It also makes for easier maintenance and a significant reduction in overall costs.

With improved signal quality due to a lack of interference between optical fibres, companies can also enjoy a better quality of service and reliability of information. Faster connections mean quicker access to the vital elements of the business. In the event of a breach, it also allows for easier preventative action to address these threats. When combined with cybersecurity offerings such as firewalls, antivirus, patch management, antimalware, backup, and so on, a company can ensure it is safeguarded against threats, but also backed up with the necessary support to minimise any damage if a compromise occurs.

Many companies, especially SMEs, think cyberattacks will not happen to them. But the reality is very different. Fortune 500 companies do go all out when it comes to their cybersecurity. As such, their international-standard Firewalls and Malware Protection are so hard to breach that many cyber criminals choose to instead prey on easier targets like the average SME.

Factor in that 95% of breaches that do occur do so because of human error, and not only can a business be vulnerable in its defences, but an unprepared workforce can provide an additional avenue for cybercriminals to capitalise on. So, fibre and cybersecurity form the ideal bedfellows to help ensure organisations have the necessary safeguards in place to protect their data and systems.

Many companies, especially SMEs, think cyberattacks will not happen to them. But the reality is very different

DEFINING THE IDEAL CYBERSECURITY SOLUTION

With Vox and its best-in-class cybersecurity solutions, the organisation is making safety a top priority. Its solutions are tailor-made to ensure any business, regardless of size, enjoys the best protection available.

By taking a managed services approach to cybersecurity, it provides SMEs with a full complement of solutions at a small, monthly outlay. To this end, and to help keep local businesses across industry sectors safe from compromise, the recently launched Vox subsidiary, Armata Cyber Intelligence delivers the technology solutions and niche expertise needed to protect data, systems, endpoint devices, and employees against the increasingly complex cyberattack threat surface.

Armata delivers cost-effective intelligent cybersecurity solutions that help achieve zero interruption to existing business systems while maintaining the highest level of protection for data. It follows the NIST Cybersecurity Framework, which provides best practice guidelines around how internal and external stakeholders at organisations can better manage and reduce the risk of cyberattacks.

This framework is built around five functions:

Identify

Protect

Detect

Recover

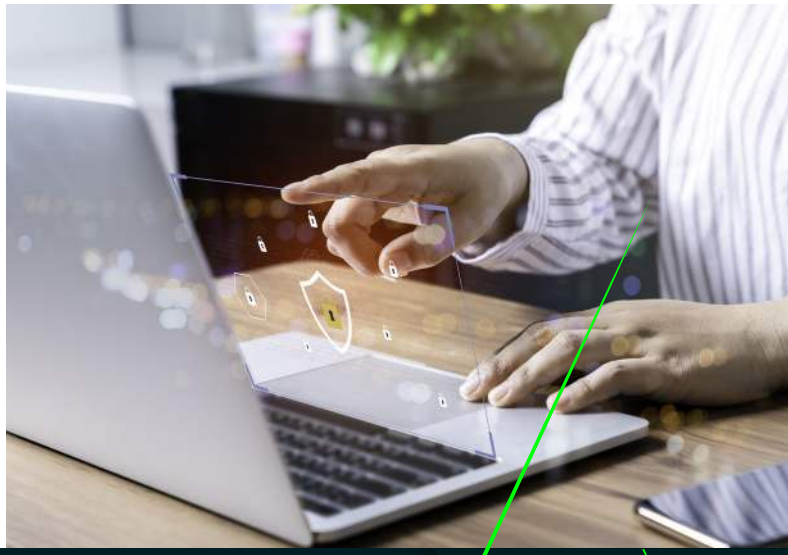
Respond

Cybersecurity is made up of products, people, and processes. Many organisations, especially SMEs, lack the funds to support all three in-house. With Armata, Vox offers an affordable month-to-month value proposition that can scale to any budget and need.

PACKAGED OFFERING

The Armata offerings include cybersecurity solutions, security services, managed security services, consulting services, and audits and assessments.
This will help organisations comprehensively deal with endpoint security, email security, network security, cloud security, application security, digital security (on mobile and Internet of Things devices), Web services security, and network access control.

It further helps organisations in the areas of identity and access management, backup, data discovery, data loss prevention, information rights management, vulnerability scanning, application code review and threat feeds, whereby customers have access to security intelligence collected from a variety of sources that can be used to proactively mitigate against cyber threats. It also provides user awareness testing programmes to ensure that employees are aware of the security risks they face daily.



SERVICES PROPOSITION

Managed Security Services Firewalls

Your business needs a next-generation firewall to protect your local network, company info, and private customer data. This managed firewall solution offers dedicated, best-of-breed security products designed to protect you from malware, intrusions, and other common cyber threats.

Managed Security Services- Endpoint Security

Our antivirus and Endpoint Detect & Response solutions are designed to shield your family and business against online threats. Our endpoint solutions offer award-winning protection for all your connected devices. The Armata Managed Security Services for Endpoint Security additionally adds the people and process aspect to the solution thus enhancing the Endpoint protection to the client.

Managed Security Services Email security

Your company email contains communication records, company and customer information, data, and other valuable resources. Our Email Management combines security, continuity, and archiving to protect your business from malware, spam, phishing, data leaks, and social engineering attacks.

It also provides user awareness testing programmes to ensure that employees are aware of the security risks they face daily

Managed Security Services Vulnerability Management

With a Web attack occurring once every 39 seconds, an average of 30 000 small business Websites gets hacked every day. Our Vulnerability management solutions are designed to proactively prevent such dire outcomes by scanning for vulnerabilities and then patching them. This gives your business the ability to keep both system and computer software up-to-date and capable of combating any low-level cyberattack.

User awareness Training

Your employees can either be your greatest asset or your biggest liability when it comes to cybercrimes – the difference is training and awareness. Our User Awareness Training programmes are designed to circumvent this risk entirely, by empowering and enabling your staff in the fight against these attacks.

THE OUTLOOK FOR 2022

Business growth today is driven by technological innovations. SMEs are more interconnected than ever, especially considering how their networks connect with mobile and Internet of Things (IoT) devices. IT is also becoming more software-defined, and more of it is moving to the cloud to meet expectations of seamless remote working, making cybersecurity critical.

Looking at the landscape for the new year, businesses must focus on conducting comprehensive risk assessments that help identify the threats that they face and highlight what controls need to be put in place. They can deploy various technologies - such as network and infrastructure security as well as endpoint security - to prevent or reduce the impact of cyber risks, depending on what they deem to be an acceptable level of risk.

To achieve this, they need specialised technical staff who are equipped with the latest skills and qualifications to ensure that appropriate controls, technologies, and practices have been implemented. However, not all organisations have access to such skills though, and it is imperative that they work with a trusted partner - that can enable businesses and remote workers with connectivity, hardware, software, and managed services - to be able to fight off the latest cyber threats.

A company's employees are critical to the success of its cybersecurity efforts. Everyone in the business needs to be aware of their role in preventing and reducing cyber threats, whether it is handling sensitive data, understanding how to spot phishing attacks - data shows that 95% of hacking attacks start with phishing or spear-phishing emails - and ensuring that security policies are adhered to when working from their own devices.

Despite best efforts, data breaches and losses still do happen, and companies need to be adequately protected. More recent offerings in the market such as cyber insurance cover businesses against financial loss, disruption, and reputational damage that result from cyberattacks.

It covers software and data, and it protects against liability arising from the misuse of, and third-party attacks on, IT infrastructure. This includes data breach expenses, extra costs, and loss of income, because of insured incidents.

Heading into 2022, we will start seeing biometrics becoming more accepted as the means to safeguard devices and data. Combine that with a Zero Trust approach where people will not trust anyone until they can prove they are who they say they are, and the environment will automatically become more secure.

Artificial intelligence and machine learning will also be used to build up patterns of user behaviour to protect systems. For example, if you are logging in to your online banking profile in Johannesburg and twenty minutes later a login request from Russia takes place, access will automatically be blocked.

Multi-factor authentication and one-time passwords, while frustrating to some as they create additional steps in the process, will also become more prevalent. Ultimately, the password landscape of the future will be one where a combination of tools and strategies will be used to protect people and companies.

CONCLUSION_

If the past two years have taught us anything in the digital world, then it is the need for constant vigilance against an increasingly sophisticated threat landscape. Malicious users are capitalising on lockdown conditions and the uncertainties created by the global pandemic to compromise business and personal systems and access critical data.

It is no secret that local entrepreneurs and SMEs have been hard hit by the global pandemic. Of course, this is not unique to South Africa. Research conducted by the International Organisation for Economic Co-operation and Development shows that up to 90% of small companies in several countries have been negatively affected. But even the ones that have managed to keep their doors open and who are preparing for a semblance of normal operating conditions for the rest of the year, the rise of cyberattacks targeting entrepreneurs and smaller companies cannot be ignored.

In addition to secure connectivity and cybersecurity solutions, companies need to consider the following interventions to help keep employees safe from cyberattacks:

- Open and honest communication. Employees seek cues from their managers on how to react to crisis situations. Organise 'Ask Me Anything' sessions with the company's top management so that they can talk to employees about how your business will continue working in the new circumstances.

- Run surveys to understand the emotional state of your employees, their workload, if they have everything they need for remote working, and if they have clarity on the business processes. This gives a better understanding of specific circumstances people are in today and helps to make more balanced decisions.

- Help your employees manage information overload and the feeling of being overwhelmed at this uncertain time. Keep your teams informed of the facts and current situation, as well as on how to stay safe and healthy.

- Create HR and IT online communication channels so that everyone can easily solve their issues. Provide guidance for all employees on how to enable remote working and use certain software. It can be done through webinars or group calls.

- Educate employees, continuously, about sound security practices when working remotely, including how to avoid becoming a victim of email or web phishing, or how to manage accounts and passwords.