

*Limitless
Visibility.
Absolute
Control.*

VM Advisory

Cape Town, South Africa

ADAPTIVE DEFENSE PLATFORM

PANDA
Powered by SECURITY

 **VM ADVISORY**
securing your cyberspace



Next generation protection

Defending the endpoint against attack is hard.

Protection must include a wide range of defences including traditional antivirus & anti-malware, personal firewall, web & email filtering and device control. And, any defence must provide additional safeguards against difficult-to-detect zero-day and targeted attacks. Up to now, IT has needed to acquire and maintain a number of different products from different vendors to defend the endpoint. That's all in the past now.

Adaptive Defense is the first and only offering to combine **Endpoint Protection (EPP)** and **Endpoint Detection & Response (EDR)** capabilities into a single solution. **Adaptive Defense** also automates capabilities reducing the burden on IT.

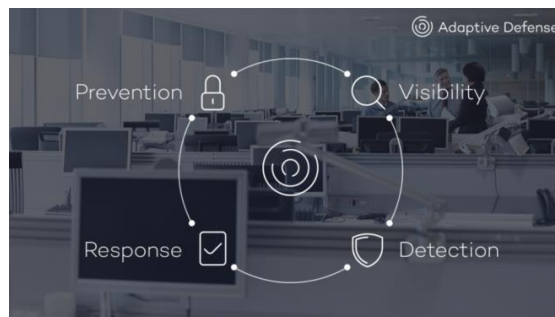
Adaptive Defense starts with the best-of-breed EPP solution which includes simple and centralized security, remedial actions, real-time monitoring and reports, profile-based protection, centralized device control, and web monitoring and filtering.

The present dilemma

The malware and IT security environment have undergone major changes in terms of volume and sophistication. With over 200,000 new viruses appearing every day, and the sophistication of techniques for penetrating defences and hiding malware, corporate networks are more vulnerable than ever to zero-day and targeted attacks.

Besides, current malware is increasingly sophisticated. Traditional Endpoint Protection solutions are efficient at blocking known malware by using detection techniques based on signature files and heuristic algorithms. However, they are no defence against zero-day and targeted attacks that take advantage of the 'window of opportunity for malware' - the time lapse between the appearance of new malware and the release of the antidote by security companies.

This is an increasing gap that is exploited by hackers to get viruses, ransomware, Trojans and other types of malware into corporate networks. Such increasingly common threats can encrypt confidential documents and demand a ransom, or simply collect sensitive data for industrial espionage.



Solution

Adaptive Defense is our solution to these types of attacks as it provides an EDR service that can accurately classify every application running in an organization, only allowing legitimate programs to run.

The EDR capabilities of the **Adaptive Defense** rely on a security model based on three principles:

- 1) **Continuous monitoring** of applications on a company's computers and servers;
- 2) **Automatic classification** using machine learning on a Big Data platform in the cloud;
- 3) The **technical experts that analyse** those applications that haven't been classified automatically in order to be aware of the behaviour of everything that is run on the company's systems.

We combine these capabilities with the best-of-breed EPP solution and our proven **Risk Based Security** and **Cybersecurity Awareness Programme**, closing the cycle of the adaptive malware protection, that now also includes automated prevention, detection, forensics and remediation.

Contact Us

VM Advisory
Cape Town
South Africa

info@vmadvisory.com

Visit us on the Web:
vmadvisory.com