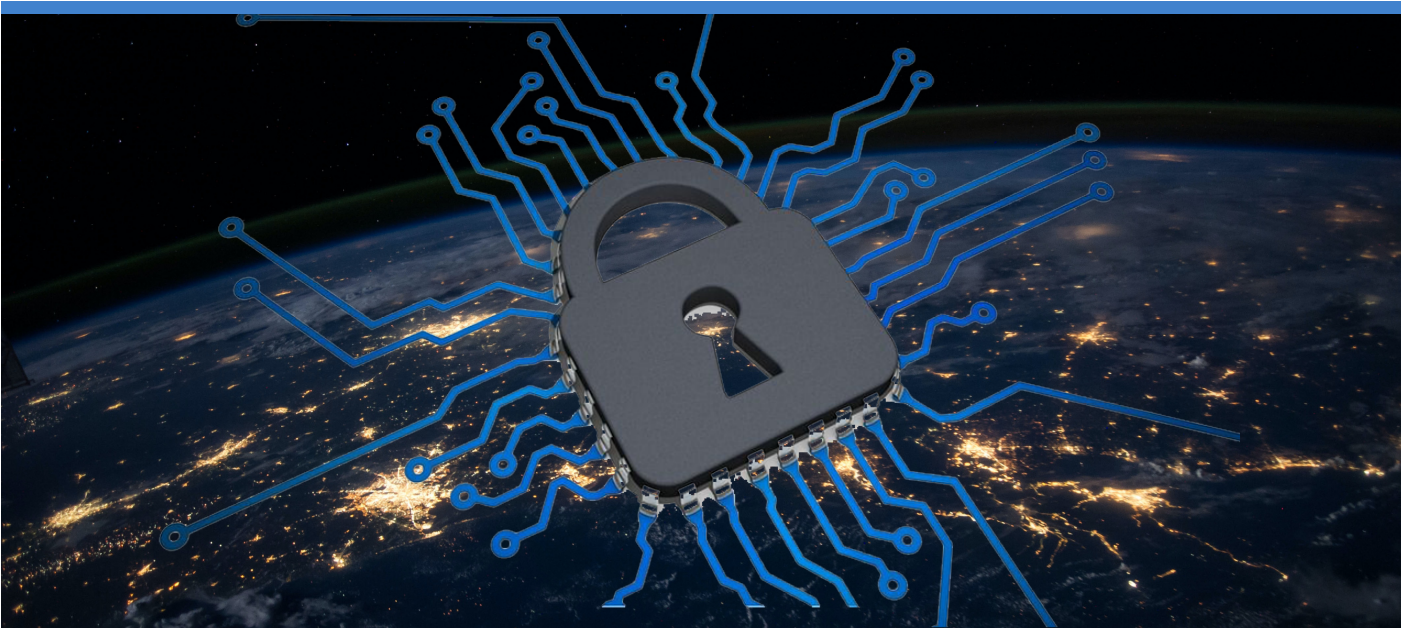# VIGYAN GYAN

Information That Matters

Proactive Endpoint Security - The Modern Solution?

The concept of shift-left is new to software development but revolutionary. The basic principle is that the earlier you identify and tackle an issue, the fewer the troubles you'll face later.

In the context of Endpoint Security, the quicker you anticipate the nature and of external threats, more effective will be your defence to neutralize them.

IoT, big data analytics, cloud sharing, etc have completely changed the sphere of business. Workers have increased mobility and require access to a large amount of data in real time. And owing to the current pandemic situation, large chunks of employees work from home.

And taking advantage of this climate, cybersecurity adversaries have increased in number and sophistication.

Because home networks are easier to corrupt and attack, cybersecurity staff of the organizations have to be constantly on their toes to protect the organization's network and datacenter. They are overwhelmed at the scale of this task. And the traditional Endpoint Security mechanisms are not effective now. The reactive approach, i.e. sit back, wait for an attack and then try to recover from it, just doesn't work anymore.

The most vital component of Proactive Endpoint Security is intelligence or knowledge. Modern tools enable us to gather knowledge about what our adversaries are doing, or are about to do thus putting us in good stead, to structure a defense.

Proactive Endpoint Security means compiling this information and acting upon it by being better informed and prepared. It lends us the ability to anticipate and stop breaches before they happen, and if an attack does manage to infiltrate, to run more effective mitigation steps because we know what is about to happen.

WHAT CAN IPM+ OFFER?

P2

What can IPM+ offer?

IPM+ is here to help you transition from Reactive to Proactive Endpoint Security through our patented Endpoint Security and Remediation
Technology with the following features:

- Vulnerability scanning with standard and out of the box databases
- Automated agentless network discovery - OS, Port, Host & Services
- Brute force analysis
- Deploy out of the box endpoint policies (e.g. CIS Benchmark)
- Real time Policy Audits
- Consolidated Security Health Dashboard
- Policy administration from central console
- Extensible framework for custom policy deployment
- File & Registry Monitoring

IPM+ Corner

Another IPM+ Datacenter product which saves the electricity at Endpoints and Servers is implemented at Fortis Healthcare - leading integrated healthcare delivery service provider in India.

The healthcare vertical of the company primarily comprise hospitals, diagnostic and day care specialty facilities. Currently, the company operates its healthcare delivery services in India, Nepal, Dubai and Sri Lanka with 36 healthcare facilities (including projects under development), approximately 4000 operational beds and over 415 diagnostics centers. They have a huge chain of 56 hospitals and employ 15412 people.

They installed the IPM+ Energy Assistant for Endpoints on 6700 devices. This led to 40% savings in energy, reducing the Carbon footprint by 1297.68 metric tonnes. Monetary savings amounted to INR 1.3 Cr. 123305 cubic meters of water was saved, 33274 trees were planted. The overall energy saved was 1.3 GWh.

IPM+ NEWS & VIEWS

- "Experts Detail A Recent Remotely Exploitable Windows Vulnerability" **- The Hacker News**
- "Sharing ebook with your Kindle could let hackers hijack your account" **- The Hacker News**
- "2021 to bring 'phase two' of remote access investment for enterprises" **- SC Magazine**
- "New cyber council tackles infosec challenges from a tech perspective" **- SC Magazine**
- "Hackers hijacked cloud accounts of high-tech and aviation firms, hid in systems for years" **- SC Magazine**
- "70% of apps for the manufacturing sector spent all of 2020 with at least one security flaw" **- SC Magazine**
- "Look for GDPR fines to increase, extend beyond breaches" **- SC Magazine**
- "Free cyber career training coursework emerges as a perk in tough times" **- SC Magazine**
- "Bot 'FreakOut' leverages three critical vulnerabilities to attack Linux systems" - **SC Magazine**

Fortis Saving With IPM+

www.ipmplus.com   info@ipmplus.com