

INTERFOCUS ADVANCED THREAT PREVENTION

Endpoint Management and Threat Protection in One Integrated Solution

Interfocus Technologies and Cylance® Inc. have partnered to integrate endpoint management and CylancePROTECT®, an innovative artificial intelligence driven malware prevention product.

Uncovering, Analyzing and Preventing Threats

The Interfocus Advanced Threat Prevention (ATP) solution integrates critical security event information into a dashboard that makes it easy for IT managers to gain visibility into suspicious activity across **all** endpoints, analyze that activity, and immediately take corrective action. From management through detection, investigation and mitigation, ATP provides total lifecycle support for managing and securing endpoints.

- Gain centralized visibility into every endpoint – both online and offline -- across the network
- Take corrective action against malware and other threats, both external and internal
- Analyze malware's digital footprint to fully understand and effectively defend against identified threats
- Use event, alert and log data to establish policies that record and prevent suspicious behavior occurring during everyday business activity

With Interfocus ATP, IT managers no longer have to examine a myriad of distinct sources of security data, manually correlate the data, and try to connect the dots to gain the upper hand over suspicious activity across their network, endpoints, and users. By leveraging the state-of-the-art CylancePROTECT® malware prevention technology, Interfocus ATP helps IT managers uncover, analyze, and quickly remediate today's complex and dynamic security threats.

Comprehensive Visibility

Interfocus ATP provides a centralized view of every network endpoint and identifies the applications, plus potentially unwanted programs that exist on each. Its comprehensive dashboard graphically displays data collected from across the organization, enabling IT managers *to know in real-time where a threat came from, what the threat looks like, and where it went.*

Robust Analysis

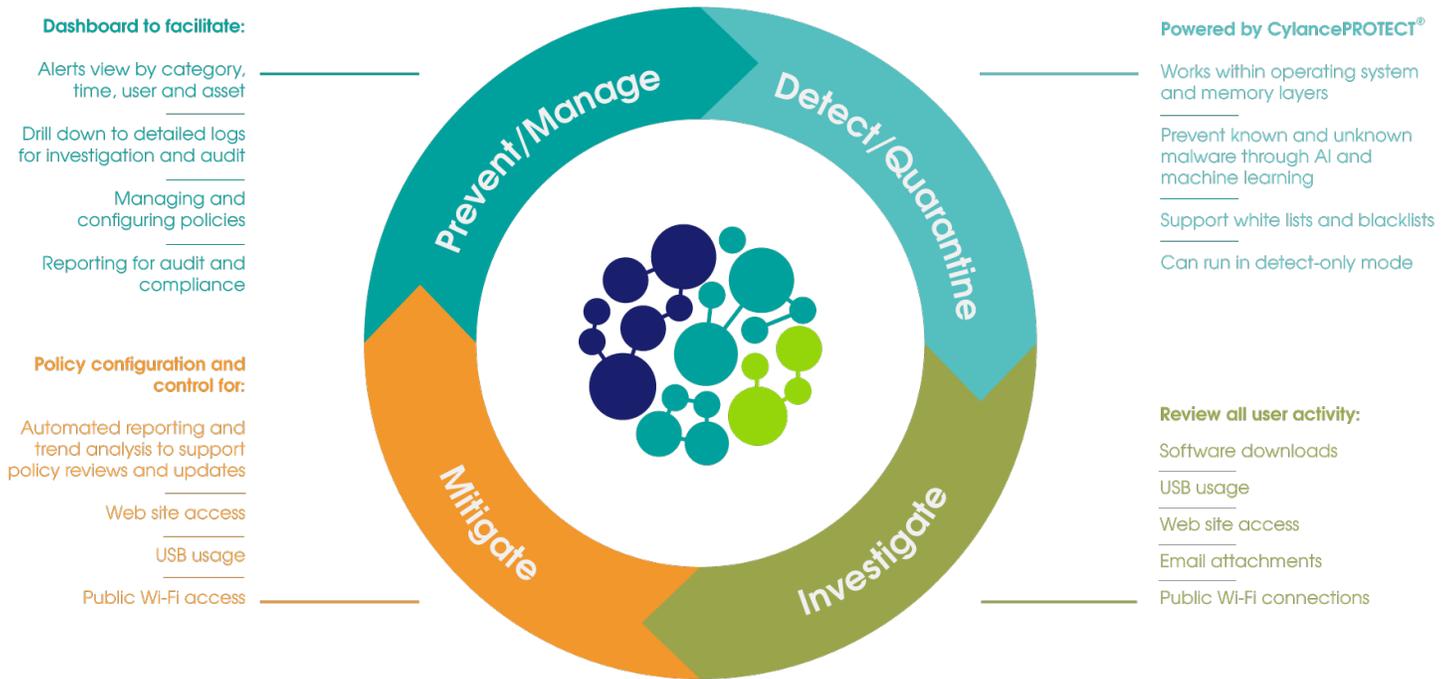
The Advanced Threat Prevention (ATP) dashboard allows IT managers to rapidly explore the extent of a threat and determine how many endpoints – both online and offline – have been infected. The dashboard also identifies files that were detected and quarantined. Detailed threat reports identify threats by category, endpoints impacted and users associated with a given threat. ATP's real-time threat information identifies the *malware's digital footprint*, making it easy to:

- Investigate current threats
- Zero in on just those specific security events of importance
- Develop policies that can prevent identified threats from recurring

Proactive Alerting

Organizations face many threats that originate either intentionally or unintentionally during the course of normal business operations. Using ATP's alerting capability, IT managers will be notified when suspicious behavior occurs in real-time.

- For example, alerts can be triggered when an employee accesses a specific website or downloads a suspicious file.
- The ATP solution provides full visibility of USB and external device usage and makes it easy for IT managers to block specific hardware or autorun files.
- ATP's logs deliver comprehensive email visibility, identifying email title, sender, content and attachment, strengthening phishing prevention and protecting against other common threats.



Advanced Prevention

The Advanced Threat Prevention (ATP) solution integrates CylancePROTECT® within its platform and reports on malware activity within its robust dashboard. Every device connected to the network is regularly scanned in an intelligent, non-performance impacting process to ensure that all endpoints are continually protected by the current version of the Cylance agents. Using artificial intelligence and machine learning, Cylance performs both background and real-time checks to identify and prevent both known and unknown malware and memory based-attacks on both online and offline endpoints.

Easy To Deploy

Interfocus ATP automatically deploys and manages the CylancePROTECT® agents on all endpoints, including Windows workstation and server platforms as well as Apple Mac OS X.

The Interfocus Advanced Threat Protection solution is a cost-effective way for businesses to use existing IT resources to uncover, analyze, and prevent today's ever-increasing security threats across networks, endpoints and users. A comprehensive and easy-to-use dashboard presents detailed security information collected from across the

organization. State-of-the art technology based upon artificial intelligence and machine-learning continually scans for and prevents malware from infecting endpoints. Best of all, IT managers can deploy and begin using the ATP solution to protect their organization within a few hours. Contact us at info@interfocustechnologies.com for more information.

About Interfocus Technologies

Interfocus Technologies is an endpoint management and security solutions provider delivering visibility into user activity, controlling IT assets, enforcing your policies and supporting enterprise compliance at an affordable price through a single console. We offer US businesses exclusive access to a market-leading technical solution that has helped over 10,000 global clients with 8.6M installed users manage and protect their digital property and productivity.

www.facebook.com/InterfocusTechnologies

www.linkedin.com/company/interfocus-technologies-inc

Cylance and CylancePROTECT are registered trademarks of Cylance Inc. All other trademarks are property of their respective owners.