INFOSYS MANAGED ENDPOINT DETECTION AND RESPONSE (MEDR) SERVICE POWERED BY PALO ALTO NETWORKS

paloalto® NETWORKS

Infosys® Navigate your next

Overview

Endpoint security is the process of protecting devices like desktops, laptops, mobile phones, and tablets from malicious threats and cyber-attacks. Endpoint security software enables businesses to protect devices that employees use for work, either on a network or in the cloud, from cyber threats. Today's workplace model comprises of a combination of office-based, remote and hybrid workers who increasingly use the Bring Your Own Device (BYOD) option. This adds security risks and requires endpoint protection that therefore lays the groundwork for an effective security strategy for any organization.

The modern business landscape is witnessing a rise in the volume of cybersecurity threats from sophisticated cyber criminals. Endpoints are one of the most common targets, given the sheer number of them in use to connect to networks. According to Strategy Analytics insight, endpoint devices will reach 38.6 billion by 2025 and 50 billion by 2030.

Also, a recent study by the Ponemon Institute indicates that 68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. The same report stated that 68% of IT professionals found that the frequency of endpoint attacks had increased since the year before.

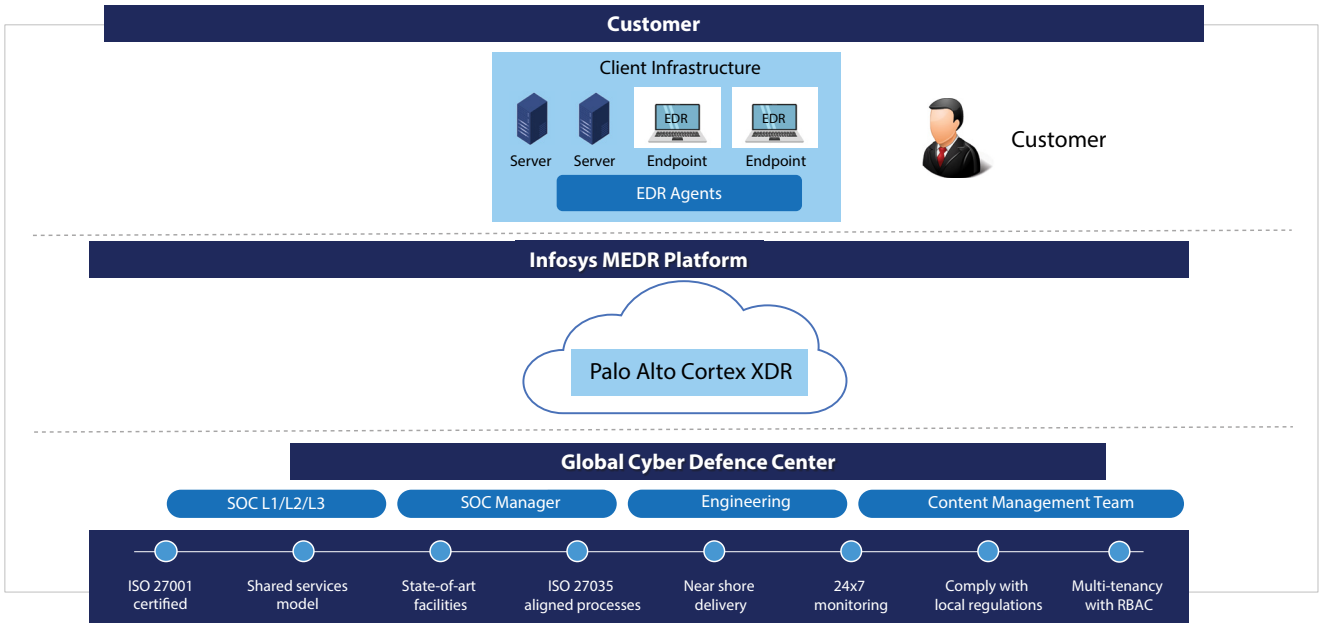
This is where a fully managed security-as-a-service from Infosys helps enterprises in providing a comprehensive package of security products and associated services that provide ready-to-use solutions. With Endpoint Detection and Response services, organizations will be able to collect and inspect event information from all endpoints in real time to prevent and detect attacks. All activities of interest on endpoints will be recorded for deeper inspection, and accordingly security teams can quickly investigate and respond to incidents that evade standard prevention measures.

Infosys MEDR Services

Infosys offers pre-engineered, packaged and fully Managed Endpoint Detection and Response (MEDR) services delivered 24x7x365 from Infosys Global Cyber Defense Centers. Infosys Managed EDR solution and services are delivered based on Palo Alto Networks NexGen Cortex Extended Detection and Response (XDR) technology platform. Infosys MEDR solution ensures core elements of an Endpoint Protection by integrating Next Generation Antivirus (NGAV) for prevention and Endpoint Detection and Response (EDR) of threats. The solution records activities and events on endpoints and workloads, providing security teams with a better visibility to uncover incidents that would otherwise remain invisible.

Infosys MEDR Service:

- Eliminates blind spots and provide comprehensive visibility.
- Simplifies security operations and reduces Mean Time To Respond (MTTR)
- Harnesses the scale of the cloud for AI and analytics
- Enhances cost efficiency by consolidating tools and improving SOC operations productivity



Infosys MEDR – A Complete Lifecycle

Onboarding

This stage covers the whole journey from deployment and onboarding the Customer to MEDR platform and enabling access to Infosys Cyber Central portal.

Stabilization

Infosys implements the detection policies based on OEM recommendation and industry best practices. The detections are validated during the stabilization phase and the configured rules/ policies will be fine-tuned for reducing the false positives and for enhanced detection.

Assurance/BAU

Infosys provides 24x7x365 Endpoint Detection and Response services, which helps in triaging and analysis of potential security alerts, publishing incident reports and maintaining the stipulated SLA/KPI.

Optimization/ Continuous Improvement

Infosys optimizes the services by deploying new policies and finetunes the existing policies deployed.

Service Renewal

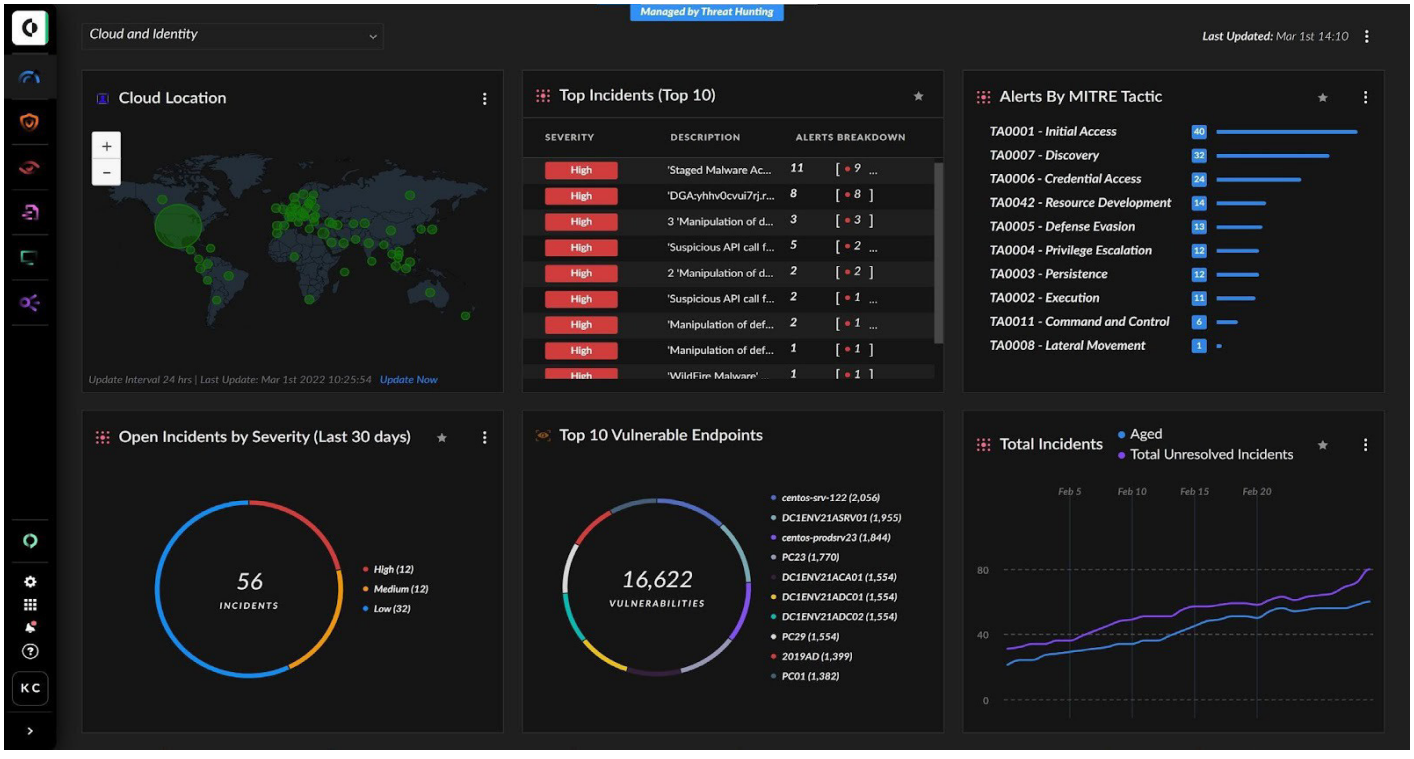
After expiry of the service agreement, customer can renew the services to a mutually agreeable duration. License to services will be renewed as per the renewal agreement.

Business Benefits

Enhance your organization's security from breaches with Infosys MEDR Platform services:

- 24x7 Service with skilled team delivering services from state-of-the-art global Cyber Defense Centers
- Cloud native solution with behavior-based and AI-powered next-generation antivirus
- Verify threats quickly by getting complete picture of attacks with reduced MTTR
- Faster time to value with pre-engineered and tested platform powered service
- Consolidate tools and simplify SOC operations to maximize ROI
- Subscription-based and outcome-oriented pricing model

Customizable Dashboard



Customer Case Study

Implementation of Infrastructure Security Endpoint Management (ISEM) for an investment giant

About the client

A leading financial investment company wanted to secure the endpoints within their environment by following security guidelines for Palo Alto Networks Cortex XDR. As a trusted partner, Infosys developed, provisioned, built, configured and deployed the security architecture across environments, networks, infrastructure, software, and tools. Thereby providing security services for the modernized environment to comply with client's security policies and standards.

Client Challenges

- Absence of tools to secure endpoints from behavior-based, signature-based, ML-based threats and exploits
- Lack of a real time verdict update mechanism and integration with cloud-based malware analysis service
- Unable to identify malicious activities in client's environment due to no threat detection engine updates

Value Delivered

- Prevented malware, exploits and suspicious activities across multiple systems
- Uncovered attacks by implementing Palo Alto Network Cortex XDR
- Protected critical stages of the attack lifecycle for online and offline users

Infosys Solution

- Deployed Cortex XDR agent, the best-in-class endpoint protection, that fulfilled the most rigorous endpoint security needs, including EDR, next-generation AV, and legacy AV replacement
- Detected stealthy threats with Cortex XDR
- Cortex XDR natively integrated endpoint data lake in client's environment
- Analyzed the data with machine learning-based behavioral analytics and with custom rules to generate high-signal alerts
- Integration of Cortex XDR solution with Palo Alto Networks Wildfire to automatically prevent threats found on the network/ endpoint (from tens of thousands of customers) across the globe
- Deployed Cortex XDR agent, part of Cortex XDR, to detect and response to security threats across network, endpoint, and cloud
- Established a secure connection with XDR, routed endpoints from Airgap Subnet, collected and forwarded logs and files for analysis

For more information, contact askus@infosys.com

Infosys®
Navigate your next