CyberSecurity & GRC Services by HCL Technologies

Gold Microsoft Partner

HCL

# Fusion Endpoint Detection and Response (EDR)

## Through Microsoft Defender for Endpoint

www.hcltech.com

## 1. Business challenges

Cyberattacks today are not just restricted to malware or virus anymore. Determined threat actors and APTs are sophisticated and resourceful in their efforts to evade and breach cybersecurity defenses. Post breach they often lurk in an enterprises IT infrastructure and potentially undermine an organizations credibility through credential theft, system, software & hardware exploits, all combined into a malicious tactics that exploit the shells, CMDs, and apps which are the foundational parts of the OS of an enterprises' asset. Malware, ransomware, on disk, on memory, etc. the list goes on with below business challenges:


Cyberattacks are costly and ever evolving


Traditional antivirus can't detect and stop both known and unknown malware


Lack of skilled in-house resources


Absence of a proactive threat detection process


Multiple agents to meet next-gen endpoint security problems


Weak integration among di erent point solutions lead to vulnerabilities


Accelerated adoption of the remote workforce model

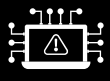

Manual/ decentralized approach to contain threats is often time consuming and costly

## 2. Solution overview

HCL Technologies' Fusion EDR service delivers 24X7X365 malware detection monitoring, proactive hunts for emerging Indicator of Compromises' and stealthy threats by experts and provides time-bound notifications and recommend response actions. This fully managed service delivers endpoint-based threat protection & detection through Microsoft Defender for Endpoint, which provides a comprehensive security to the endpoint by detecting threats at an early stage while reducing the attack surface through in-built policies and provides an automated investigation and remediation of security alerts/ incidents.

**HCL Fusion EDR through Microsoft Defender for Endpoint:**

1 **Protect & detect**
Protects against known malicious attacks and detects any malicious system activity and identifies any active endpoint-based attacks



2 **Investigate**
Investigates & quickly analyzes all alerts, performs threat hunts as well as remote RCA and focuses on adversarial behavior-based on MITRE ATT&CK® framework

3 **Respond**
Quick response including containment of suspected incidents through quarantine and other actions

4 **Investigate**
Remote remediation of malware from compromised assets and restore endpoint to a pre-infection state. Also record all stages of attack wherein automatic blockage of attack and remediation of a ected assets based-on MITRE ATT&CK® framework is provided.

## Deployment and Enablement Journey:

1 **Design-** Basis the requirements and endpoint environment, design the architecture with the valid components, configuration, and security policies

2 **Integrate-** Enablement of endpoint security suite and the tenant while integrating with the right security alert management & ITSM tools

3 **Modify and develop-** Modify any endpoint security policies as per compliance and develop custom queries for effective threat hunting

4 **Analyze and mitigate-** Threat analysis and investigation to detect and mitigate even the zero-day cyber threats

## 3. Service features

- End-to-end fully Managed Services
- 24X7 operational expertise delivered from HCL Technologies' CSFC's
- Experts led threat hunting to uncover stealthy attacks in progress
- Automated investigation & response through Microsoft Defender for endpoint
- Detection of advanced attacks based on MITRE ATT&CK® framework

## 4. Service benefits

- Proactively secure assets holding customer data, PII, IP info. & PHI
- Single platform-based detection & response combined with skilled security experts leads to quick incident response
- Proactive threat hunting reduces stealthy attacks' dwell time
- Enabled by next-gen protection and behavioral monitoring, detects known and unknown malware-based attacks on endpoint
- An integrated approach with Azure Sentinel and MCAS along with Microsoft Threat Protection provides best protection with zero delays or configuration changes

## 5. Key features of Microsoft Defender for Endpoint:

HCL Technologies has chosen Microsoft Defender for Endpoint as its lightweight client, speed of operation, and unique modeling of adversarial activity that's closely aligned with our own methodologies. Rather than relying on artifacts found in the wake of a breach or breach phase, Microsoft Defender for Endpoint can detect indicators of attack in real time.

- Threat & Vulnerability Management
- Attack Surface Reduction
- Next Generation Protection
- Endpoint Detection & Response
- Automated Investigation & Remediation

## 6. HCL Technologies' Credentials

- 1 Million+ Endpoints managed & protected
- Certified engineers and expert analysts
- Based-on industry leading Microsoft Defender for Endpoint

To know more visit: **http://www.hcltech.com/cyber-security-grc-services**
or write to us at Cybersecurity-GRC@hcl.com

BI-112251AII745819826307-EN00GL

HCL

HCL Technologies (HCL) empowers global enterprises with technology for the next decade today. HCL's Mode 1-2-3 strategy, through its deep-domain industry expertise, customer-centricity and entrepreneurial culture of ideapreneurship™ enables businesses to transform into next-gen enterprises.

HCL offers its services and products through three lines of business - IT and Business Services (ITBS), Engineering and R&D Services (ERS), and Products & Platforms (P&P). ITBS enables global enterprises to transform their businesses through offerings in areas of Applications, Infrastructure, Digital Process Operations, and next generation digital transformation solutions. ERS offers engineering services and solutions in all aspects of product development and platform engineering while under P&P. HCL provides modernized software products to global clients for their technology and industry specific requirements. Through its cutting-edge co-innovation labs, global delivery capabilities, and broad global network, HCL delivers holistic services in various industry verticals, categorized under Financial Services, Manufacturing, Technology & Services, Telecom & Media, Retail & CPG, Life Sciences, and Healthcare and Public Services.

As a leading global technology company, HCL takes pride in its diversity, social responsibility, sustainability, and education initiatives. As of 12 months ending on December 31, 2021, HCL has a consolidated revenue of US $ 11.48 billion and its 208,000 ideapreneurs operate out of 52 countries. For more information, visit www.hcltech.com

www.hcltech.com