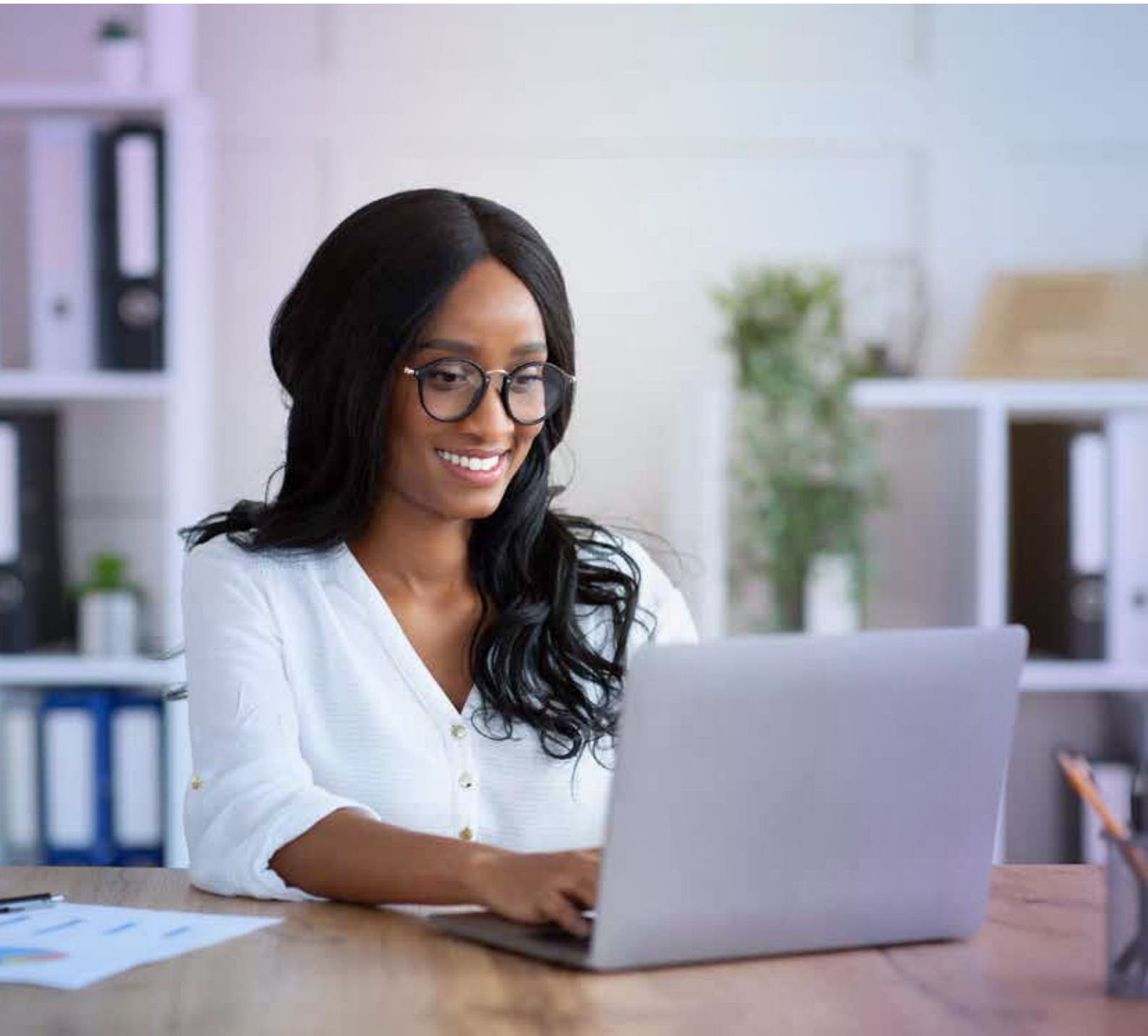
HCLTech | Supercharging Progress™

Fusion endpoint detection and response (EDR)

Through Microsoft Defender for Endpoint



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

Solution overview

HCLTech' 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.

HCLTech Fusion EDR through Microsoft Defender for Endpoint:

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

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

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

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:

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

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

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

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

Service features

End-to-end fully Managed Services

24X7 operational expertise delivered from HCLTech' 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

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

Key features of Microsoft Defender for Endpoint:

HCLTech 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

HCLTech' Credentials

1 Million+ Endpoints managed & protected

Certified engineers and expert analysts

Based-on industry leading Microsoft Defender for Endpoint