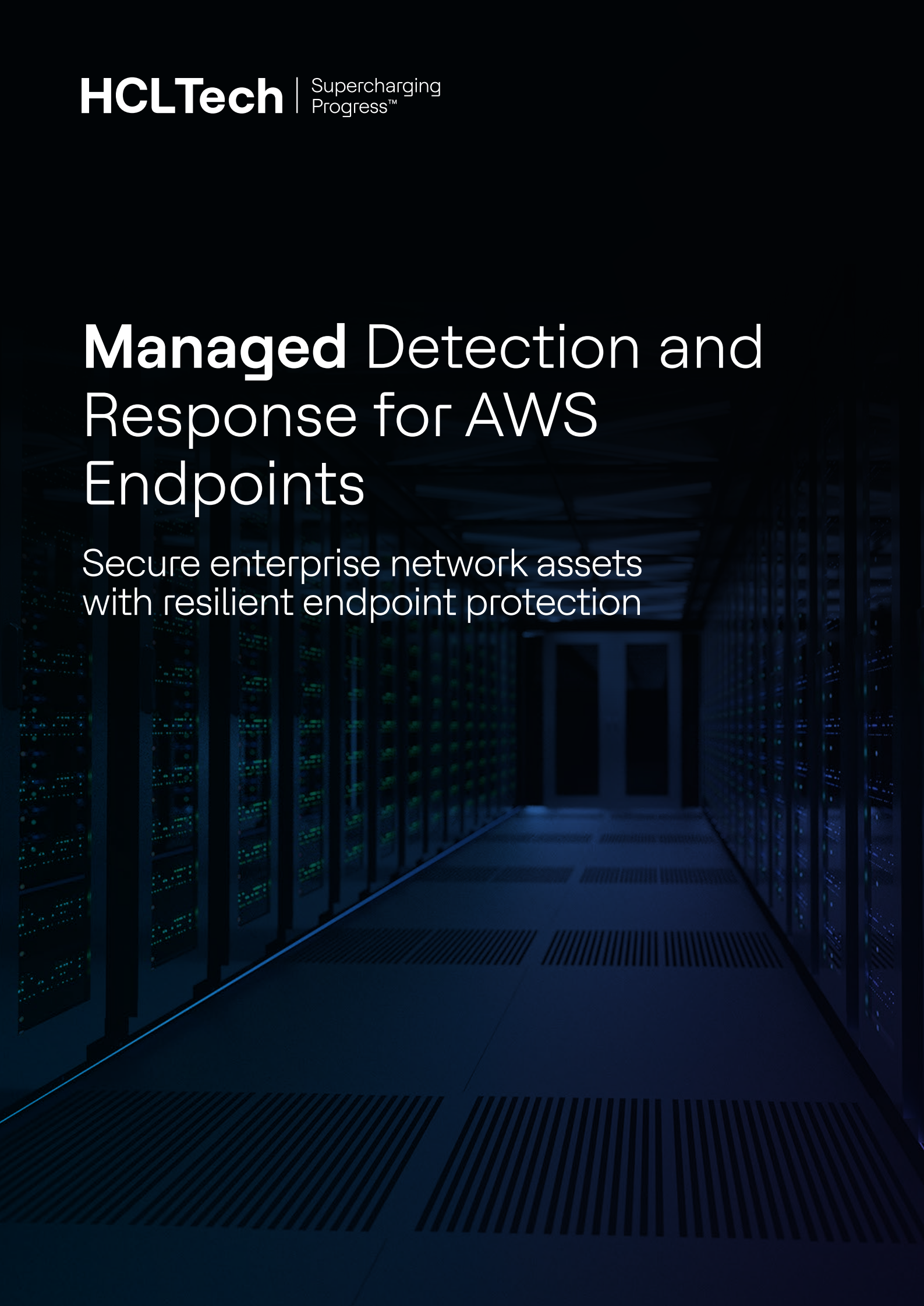


Managed Detection and Response for AWS Endpoints

Secure enterprise network assets
with resilient endpoint protection





Overview

As today's business strives forward with new ways of working, distributed operations, global cloud infrastructure, and third-party access, they must adopt a robust endpoint protection against the rising sophistication of digital threats. Moreover, organizations operating on AWS cloud, need security solutions that can help them scale their operations while seamlessly aligning with their cloud infrastructure ecosystem. More than 70% of network breaches are perpetrated by external actors due to insufficient endpoint security measures. This crucial vulnerability makes endpoint security management a high priority for any cybersecurity strategy. HCLTech Cybersecurity & GRC's Managed Detection and Response for AWS Endpoints could help achieve better customer satisfaction and reduced security risks.

Challenges



Security disrupting the benefits expected from cloud adoption



Lack of Visibility on AWS instances and their security posture



End user Experience disrupted while trying to scale up



Risk with End user data being compromised – the Number of users in B2C also adds to the challenge



Increasing Security Standards and compliances

HCLTech Solution

HCLTech offers enterprises an in-depth solution that leverages best-in-class security technology to prevent breaches by enabling bleeding-edge managed endpoint detection and response (MEDR) across the AWS cloud ecosystem. HCLTech offers four key capabilities for MEDR: detect security incidents, contain the incident at the endpoint, investigate security incidents, and provide remediation guidance. This includes:

- Compatibility and support across every Amazon EC2 operating systems
- Real-time and historical visibility across Amazon EC2 instances for a significantly enhanced security posture.
- Endpoint metadata support that can ingest and display relevant AWS metadata from every EC2 instance that a deployed agent is running on.
- In-depth visibility of the properties of each EC2 instance that showcases key properties such as, VPC ID, Subnet ID, and Region.
- Working agent identification that can easily locate machines without working agents directly from the console.
- Unified console display with personalized alert rules that notifies the detections of events across instances along with respective corrective actions
- Flexible alert rule policies that can either be event-based or policy-based, or a combination of both.
- Integrated container protection with AWS container services such as Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and AWS Fargate.
- Storage device status and protection for S3 buckets in AWS which can be added to the console either manually, or automatically when they are created.

Value Delivered

- Enterprises can leverage AWS cloud securely to achieve their business goals
- Enhanced End user experience
- Better visibility of AWS instance Security
- Ease of operations with centralized management of EC2 security

HCLTech | Supercharging Progress™

BE-112251A11734745820440-EN00GL

HCLTech is a global technology company, home to 211,000+ people across 52 countries, delivering industry-leading capabilities centered around Digital, Engineering and Cloud powered by a broad portfolio of technology services and software. The company generated consolidated revenues of \$11.79 billion over the 12 months ended June 30, 2022. To learn how we can supercharge progress for you, visit hcltech.com.

hcltech.com

