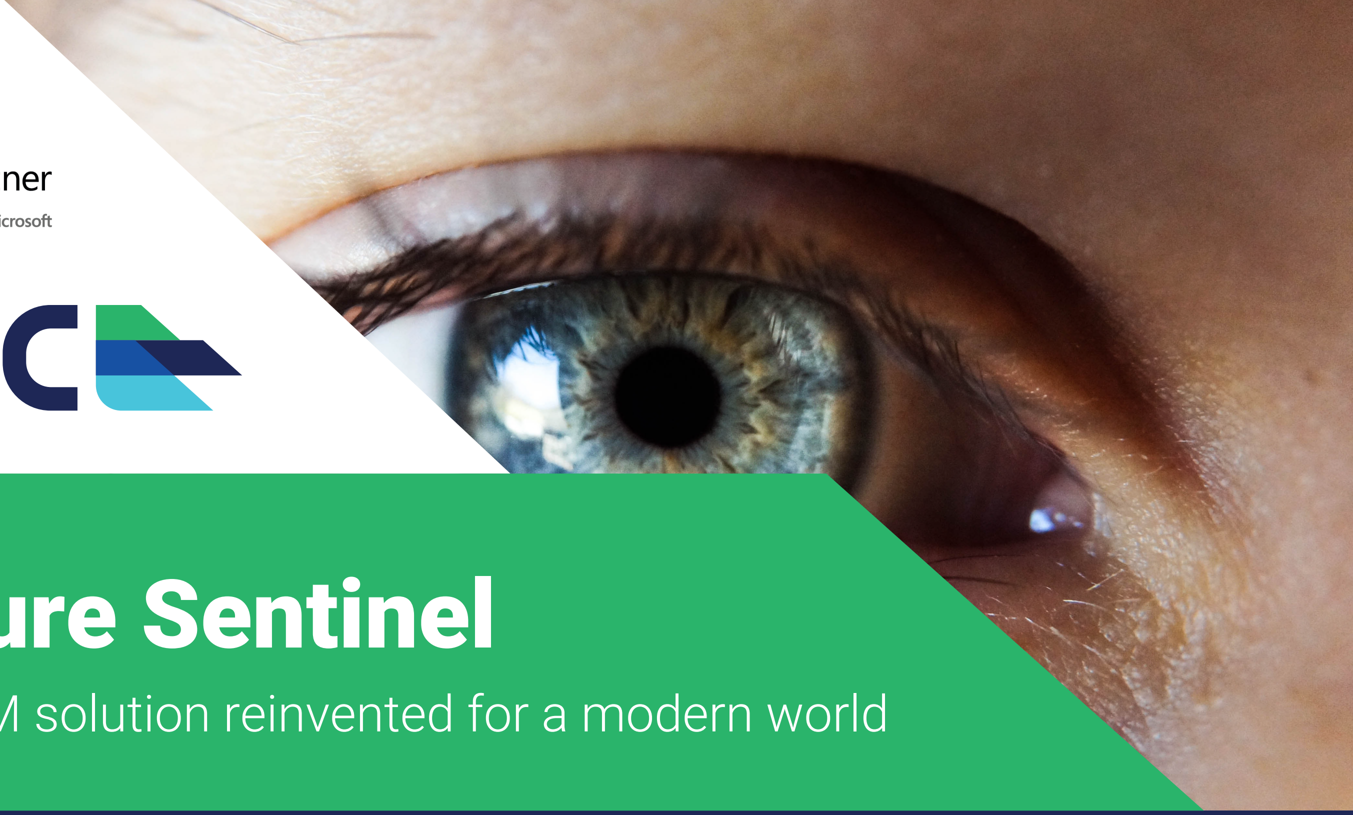
Gold
Microsoft Partner
Microsoft



# Azure Sentinel

## A SIEM solution reinvented for a modern world

Get smarter, faster threat detection and response with the cloud and AI. Gain access to intelligent security analytics and unlimited compute and storage. Azure Sentinel is your birds-eye view across the enterprise. Detect and eliminate threats before they cause harm using artificial intelligence - with a SIEM solution reinvented for a modern world.

### What is Azure Sentinel

Azure Sentinel is a cloud-native security information and event manager (SIEM) solution that uses built-in AI to help analyze large volumes of data across an enterprise—fast. Azure Sentinel aggregates data from all sources, including users, applications, servers, and devices running on-premises or in any cloud, letting you reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of popular security solutions. Collect data from any source with support for open standard formats like CEF and Syslog.

### Using Azure Sentinel with LDC

Delegate combating all kinds of cyber threats to our security specialists, we will help you detect and eliminate cyber crime, protect your business data, manage your devices and minimize compliance risk. As an Azure Sentinel super partner LDC can manage your enterprise security using the best in-class SIEM best practices and know how.

## The LDC Guarantee

### Customer-Led Infrastructure Designs

We provide expert professional services, as cloud innovation advocates, trusted technology advisors and infrastructure specialists we are able to tailor, develop and service complex systems and structures in the way that best suits your unique business needs.

### 24/7 Dedicated Expert Support

We offer dedicated support services around the clock, rest assured you will receive technical assistance anytime you need it via multiple reach out channels as well as, through dedicated expert teams assigned to your specific project.

## Integrating with existing enterprise tools

Azure Sentinel integrates with many enterprise tools, including best-of-breed security products, homegrown tools, and other systems like ServiceNow. It provides an extensible architecture to support custom collectors through REST API and advanced queries. It enables you to bring your own insights, tailored detections, machine learning models, and threat intelligence.

## Reaping ROI benefits

Based on *Forrestor's Total Economic Impact (TEI) Study*, surveyed organizations who have invested in Azure Sentinel, have seen increased SOC team efficiency, including reduced MTTR, avoided legacy SIEM costs,and improved management efficiencies.

Azure Sentinel drove an increase in SOC efficiency by reducing the number of false positives and the effort required by analysts to investigate alerts, leading to **$2.2 million** in efficiency gains.

Azure Sentinel was less expensive than the legacy SIEM solution, saving on licensing, storage, and infrastructure costs totaling **$4.9 million**.

## Features

| | |
|---|---|
| **Data Collection** | Collect data at cloud scale – across all users, devices, applications and infrastructure, both on-premises and in multiple clouds. |
| **Threat Intelligence** | Detect previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence from Microsoft. |
| **AI & Proactive Hunting** | Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft |
| **Orchestration & Automation** | Respond to incidents rapidly with built-in orchestration and automation of common tasks |

## About LDC

LDC is a cloud innovation specialist and renowned managed IT services provider (MSP) leading in IT and digital transformation in the Middle East since 1996. Partners with the world's top technology platforms, LDC is home to certified technology experts and infrastructure specialists with 100+ years of combined regional and local experience.

☎ + 202 2529 5832