

The Comtact Guide:
Microsoft Azure Sentinel

Introduction

In a world of increasingly sophisticated and harder-to-detect cyberattacks, the challenges for information security leaders continue to grow.

Digital transformation continues to reshape IT. Information security leaders face growing complexity, diverse attack surfaces and alerts growing by orders of magnitude. Cyberattacks are increasingly sophisticated and difficult-to-detect – and all in the context of exponential growth in data volume. At the same time, IT teams need to find ways to make systems and processes more efficient, while controlling costs and managing resources.

Security Information and Event Management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges – let alone tomorrow's unknown risks. Costly to operate and slow to scale, resource-heavy SIEM infrastructure and tools can easily become obstacles to digital transformation. Ever-growing volumes of data strain the limits of on-premises systems. Managing and staffing those same systems creates a huge operational burden that takes time away from strategic activities. Alert fatigue is reaching all-time highs and traditional approaches simply can't handle the pace of change, with IT departments having limited funds to throw at the problem.

A Next Generation SIEM Solution

In response to these challenges, Microsoft developed Azure Sentinel, a high advanced, fully cloud-native SIEM with artificial intelligence designed to serve all aspects of security operations.

- ✓ **Collect** data at cloud scale – across all users, devices, applications and infrastructure, both on-premises and in multiple clouds.
- ✓ **Detect** previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence from Microsoft.
- ✓ **Hunt** for threats proactively that may not have been discovered by security apps.
- ✓ **Investigate** threats with AI and proactively hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- ✓ **Respond** to incidents rapidly with built-in orchestration and automation of common tasks.

Built on Microsoft Azure, a leading public cloud platform, Azure Sentinel eliminates infrastructure and management complexity. It scales readily to meet dynamic needs and maximises your SOC provider's skills with intelligent, role-based tools, empowering you with insights from Microsoft's extensive multi-billion dollar global security operations.

Comtact are proud to partner with Microsoft, with Azure Sentinel at the heart of our Cyber Defence Centre (CDC), the UK's most advanced SOC service with Microsoft Gold Partner status.



"Azure Sentinel addresses all the foundational SIEM use cases. It addresses data aggregation at scale horizontally forever, and the proof is in the pudding. How do you go from 50 gigabytes to 8.5 terabytes a day in a period of six months? The answer is with Azure Sentinel."

**Senior VP of global threat management,
financial services industry**

Why Microsoft Azure Sentinel?

Improve threat protection with AI on your side

Intelligent correlation helps reduce false positives and alert fatigue by up to 90%, which can detect complex, multi-stage attacks. Built-in intelligence helps automate and orchestrate up to 80% of common tasks, simplifying operations and accelerating the threat response from your SOC team.

Secure your entire enterprise

Allow your SOC provider to integrate with existing tools, whether business applications, other security products or home-grown software. Analyse data from users, applications and infrastructure, both on-premises and multi-cloud. Azure Sentinel helps your SOC provider get started fast and grow with your business as needed with a broad range of connectors and industry-standard data formats.

Invest in security, not servers

Powered by the Microsoft cloud platform, Azure Sentinel delivers near-limitless speed and scale without the operational complexity and overhead of a server-based SIEM. Proven, scalable log analytics delivers insights to your SOC provider in seconds. That means lower cost, more agility and more time for them to focus on real security issues.



"There is no more downtime with Azure Sentinel. It's never blinked. It's never gone down, and when we hit a certain capacity, Microsoft actually gave us our own dedicated cluster and the performance improved."

**Senior VP of global threat management,
financial services industry**

Why Microsoft Azure Sentinel?

Free storage and analysis for Office 365 data

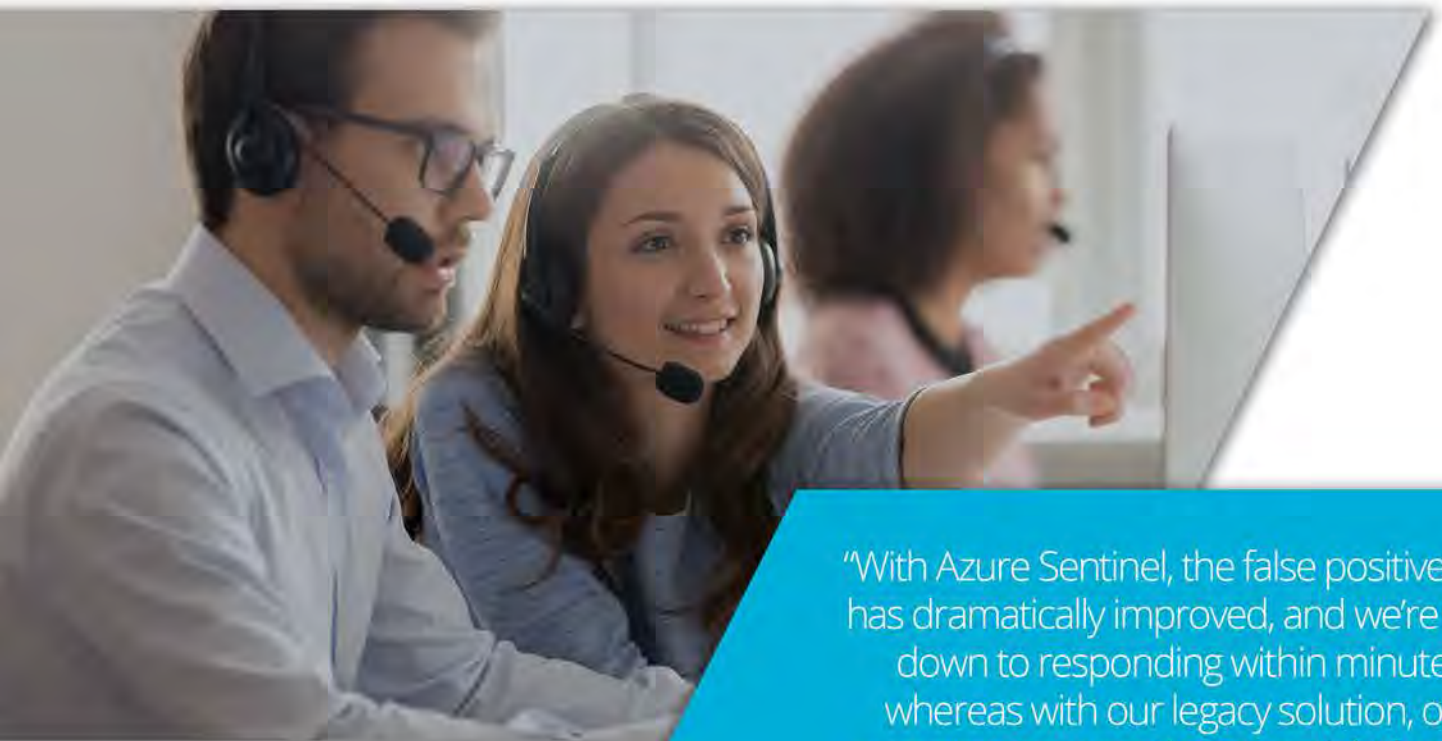
To help you maximise security effectiveness across your enterprise, Azure Sentinel pulls in data from your entire Microsoft estate for analysis without charge. This provides a significant cost saving over third party SIEMs which charge you for each piece of data they ingest.

Build on Microsoft's investment

In security, knowledge and scale is power. With Azure Sentinel, you gain the power of Microsoft's decades of experience managing security at a massive global scale. Microsoft solutions share insights gained from unparalleled threat intelligence that is informed from analysing trillions of signals every day. Their security experts support proactive threat hunting with prebuilt queries based on years of security experience.

Store and analyse massive amounts of data in seconds

Azure Sentinel is built on the highly scalable, high performance Azure Monitor Log Analytics platform, designed to store and analyse massive amounts of data in seconds. It allows your SOC provider to join data from multiple tables, aggregate large sets of data and perform complex operations with minimal code, answering questions at speed.



"With Azure Sentinel, the false positive rate has dramatically improved, and we're now down to responding within minutes whereas with our legacy solution, our average response time was eight hours."

**CISO, eCommerce /
fashion industry**

Serving The Five Key Aspects of Security Operations

1 Collection

Collect data at cloud scale – across all users, devices, applications and infrastructure, both on-premises and in multiple clouds. Microsoft is the core, but the coverage and integration is as comprehensive as any SIEM.

Azure Sentinel includes connectors providing real-time integration with many industry solutions. It enables easy connections to a variety of Microsoft services, such as Office 365, Azure Active Directory, Azure Advanced Threat Protection and Microsoft Cloud App Security. Data can also be collected from existing security solutions such as firewalls, routers, endpoint security and many more using built-in connectors. Plus, your SOC provider can use Common Event Format (CEF), Syslog or REST-API to connect any compliant data source to Azure Sentinel.

After your data sources are connected, your data starts streaming into Azure Sentinel and is ready for your SOC provider to use.

2 Detection

Enable your SOC provider to detect previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence from Microsoft.

After your data sources are connected to Azure Sentinel, the next step is to identify suspicious activities and threats. Azure Sentinel provides built-in templates to enable your SOC provider to do this and get notified of such threats. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors and suspicious activity escalation chains. After you enable these templates, they will automatically search for suspicious activity across your environment. Many of these can be customised to search for, or filter out, activities according to your needs.

Business Benefits of Microsoft Azure Sentinel – Forrester Research*

- Increased SOC efficiency with less false positives and reduced analyst effort to investigate alerts.
- Reduced management effort by 56% with a platform delivered in the cloud.
- 67% reduction in time to deployment with out-of-the box functionality.
- Costs 48% lower than the legacy SIEM deployment with flexible, consumption-based pricing.
- Prebuilt connections to many applications, improving data ingestion, visibility and overall coverage.
- Improved response times by up to 50% with advanced AI and threat intel to spot suspicious event sequences.
- Capital investment avoided for storing logs on-premises.
- Automation of many of the administrative tasks traditionally performed by SOC analyst.

Serving The Five Key Aspects of Security Operations

3 Hunting

Analysts need to proactively look for threats that may not have been discovered by security apps. Azure Sentinel includes built-in hunting queries that guide your SOC provider to ask the right questions to find previously undiscovered threats.

With Azure Sentinel hunting, your SOC provider can take advantage of the following capabilities:

- Built-in hunting queries: Developed and fine-tuned by Microsoft security researchers and the GitHub community on a continuous basis to provide an entry point and help start hunting for the beginnings of new attacks.
- Powerful query language with IntelliSense: Built on top of a query language, this gives the flexibility to take hunting to the next level.
- Create your own bookmarks: Save items for later to create an incident for investigation. Bookmark a row, promote it to an incident and investigate with an investigation graph.
- Use notebooks to automate investigation: Notebooks encapsulate all the hunting steps in a reusable playbook.
- Query the stored data: The data is accessible in tables to query, for example, process creation, DNS events and many other event types.
- Links to community: Leverage the power of the greater community to find additional queries and data sources.

4 Investigation

Investigate threats with AI.

An incident is an aggregation of all the relevant evidence for a specific investigation. Incidents are created based on alerts your SOC provider will define in the Analytics page. The properties related to the alerts, such as severity and status, are set at the incident level. Your SOC provider can now more easily investigate the detected threats and the entire incident, quickly view the status of each incident and manage the full life cycle of this event.

5 Response

Respond to incidents rapidly with built-in orchestration and automation of common tasks.

A security playbook is a collection of procedures that orchestrates a threat response. Playbooks can run manually or automatically. Security playbooks in Azure Sentinel are based on Azure Logic Apps, providing built-in, customisable templates. For example, if you're worried about malicious attackers accessing your network resources, an alert can be set that looks for malicious IP addresses accessing your network and trigger a playbook to stop the attack in real time.

Why Contact for Microsoft Azure Sentinel?

Microsoft Gold Partner

Contact, through our Cyber Defence Centre (CDC), are the UK's premier Microsoft Azure Sentinel SOC provider partner. We have a single platform focus so our expertise is second to none.

Dedicated team

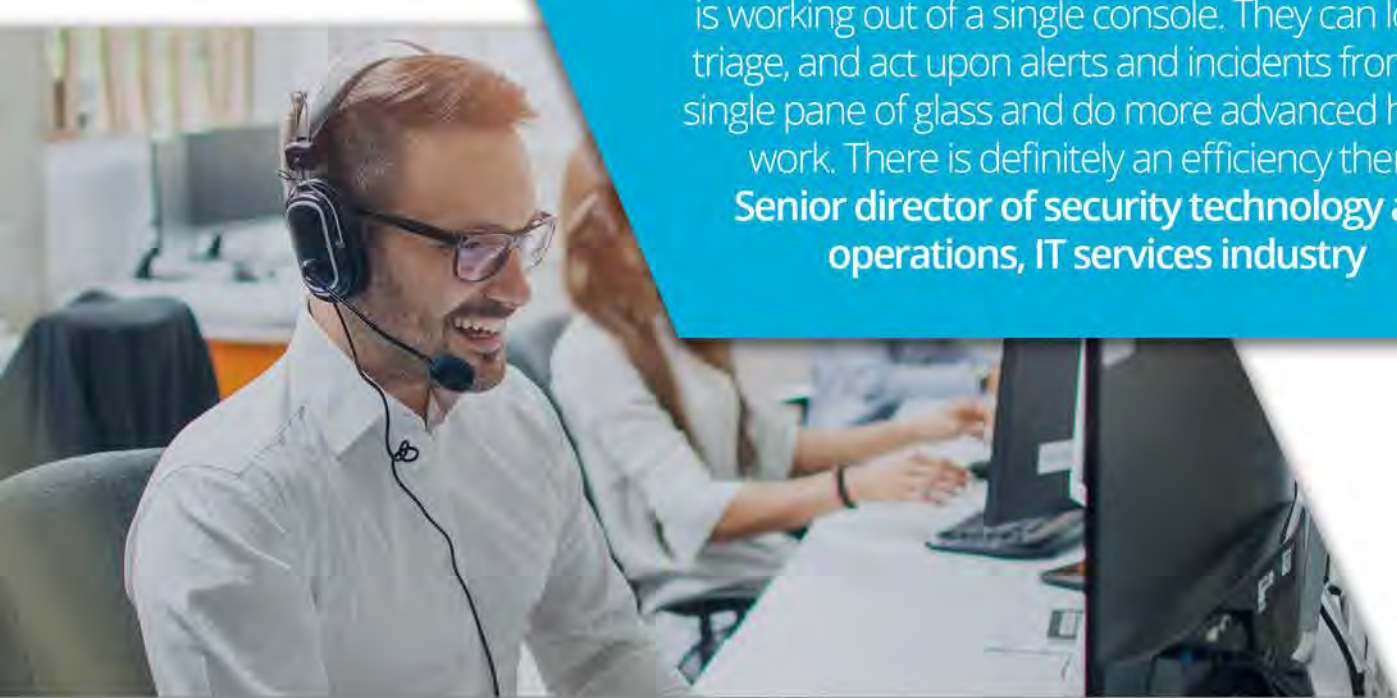
Our experts manage all aspects of threat prevention, detection, analysis and response, taking the tools we deploy well beyond out-of-the-box capabilities. We establish clear and strong lines of communication to act as an extension of your in-house team. Through continuous measuring against strict performance criteria, we ensure the highest levels of service are maintained over the long term.

24x7x365 service

Many competitors pay lip service to "24x7x365". We live and breathe it. If an incident occurs, it will be investigated immediately by our team, leveraging Azure Sentinel and initiating rapid-response escalation procedures as required. We are watching over you at all times and never rest until all issues are resolved.

Scalability

CDC is a flexible solution that can easily be scaled and adjusted in line with your changing business needs and the ever-evolving demands of the cybersecurity landscape. Our team has the breadth to scale and respond rapidly.



"Whether they are Tier 1, 2, or 3, the key is that everyone is working out of a single console. They can look at, triage, and act upon alerts and incidents from their single pane of glass and do more advanced hunting work. There is definitely an efficiency there."
Senior director of security technology and operations, IT services industry

Why Contact for Microsoft Azure Sentinel?

Reduce costs and enhanced productivity

CDC works on a flexible consumption-based pay-monthly subscription model, so you don't pay for any unused capacity. You no longer need to make significant up-front investments in technology, training or resources, with your in-house team free to focus on core objectives. The pricing plan is clear, simple and with nothing hidden.

Threat hunting

CDC includes ongoing, proactive threat hunting which many competitors charge for. We proactively search for cyber threats that lay undetected within your network that could be actively stealing data from right under your nose. This threat hunting service shines a light on undetected attacks allowing and allows for a faster response.

Service reviews

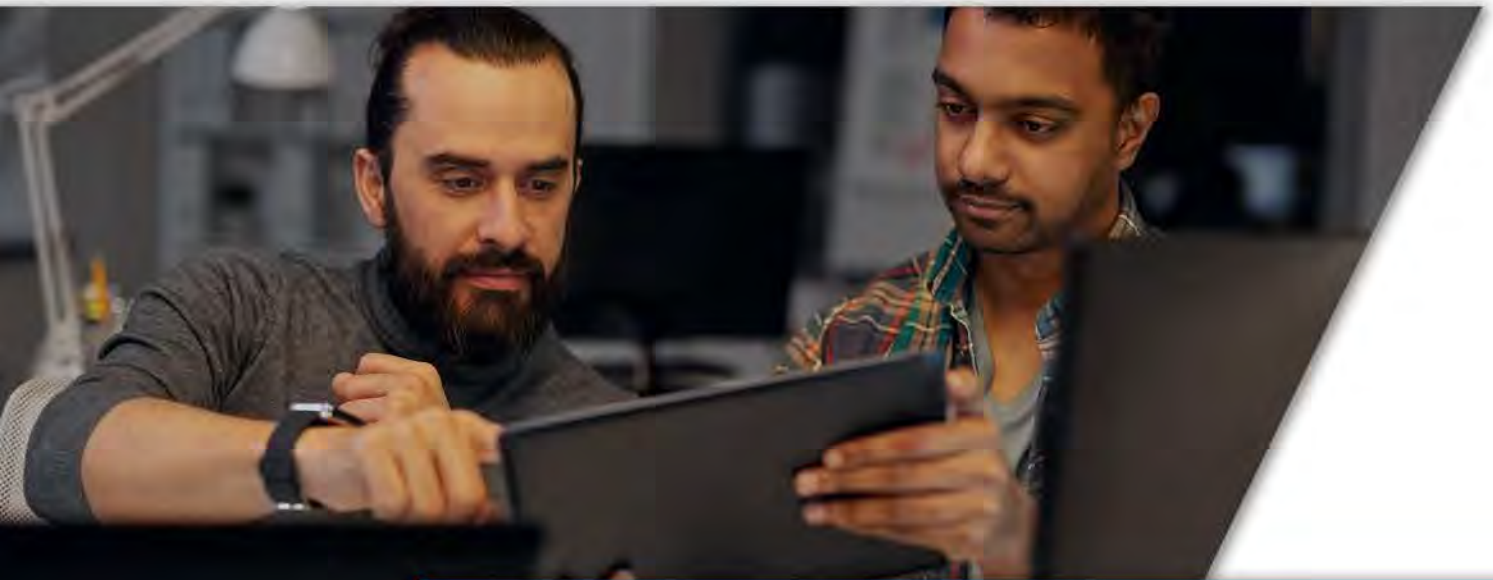
Customer service reviews are regularly carried out to monitor both contract and technology performance. We run a Continuous Service Improvement Plan on all our contracts to ensure you're getting the best out of the solution, and we are keeping up with your business requirements.



TRY AZURE SENTINEL TODAY

No infrastructure investment. Powerful AI built-in. Tools for every role. Virtually unlimited scalability. All backed by Microsoft security research. If you're looking to improve the security posture of your enterprise while simplifying security operations, consider Azure Sentinel through Comtact and our Cyber Defence Centre.

See how fast, easy and inexpensive it is to get started.



Contact us to arrange a free consultation with an Azure Sentinel and SOC specialist.

03452 757575 | enquiries@comtact.co.uk

* "The Total Impact of Microsoft Azure Sentinel", Forrester Consulting, November 2020