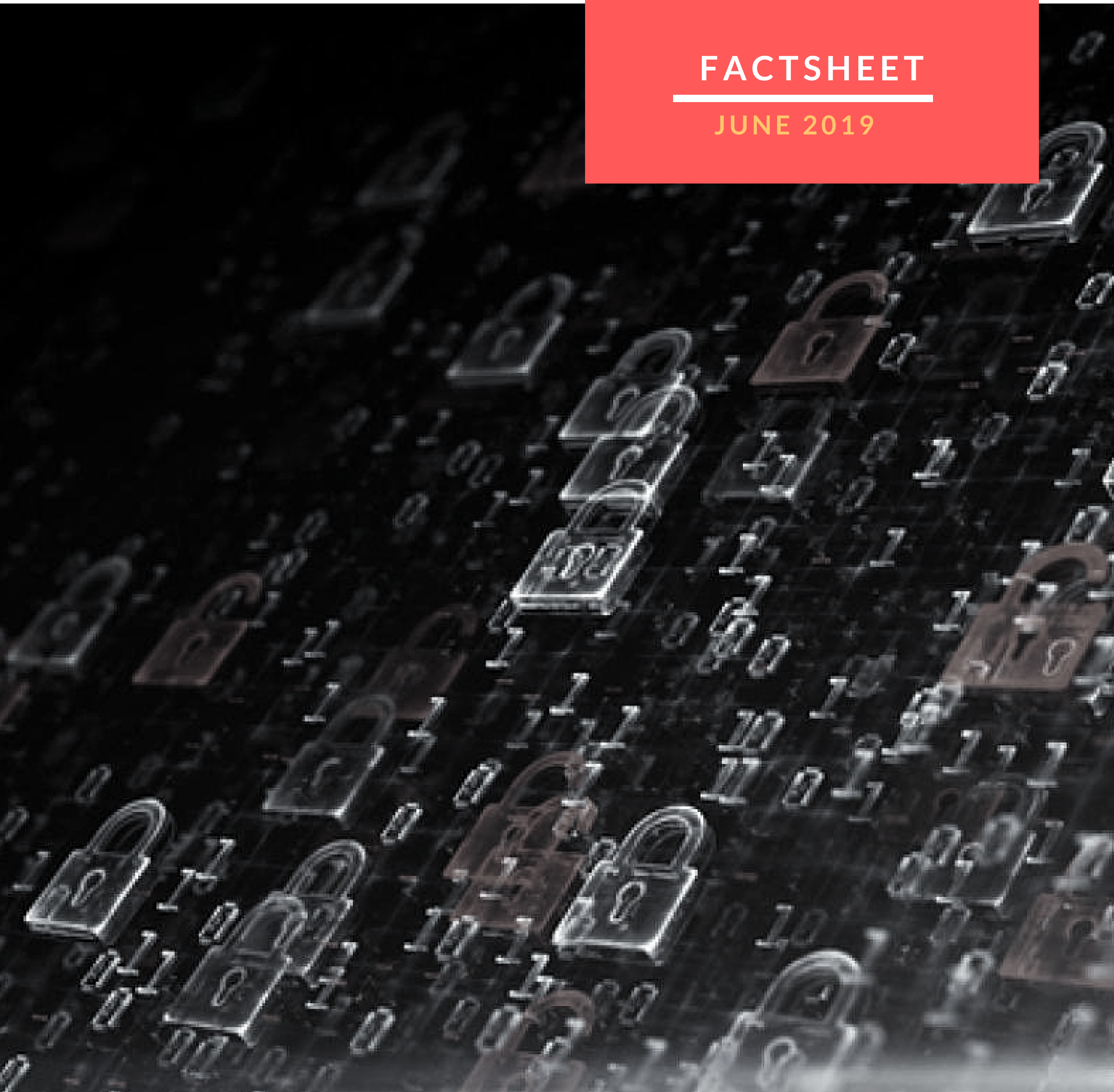
MICROSOFT AZURE SENTINEL - FAQS

CONTEXT

FACTSHEET

JUNE 2019



1 WHAT IS MICROSOFT AZURE SENTINEL?

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Azure Sentinel delivers intelligent security analytics and threat intelligence across an enterprise, providing alert detection, threat visibility, proactive hunting, and threat response.

Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) tool.

2 HOW DOES AZURE SENTINEL WORK?

The platform uses built-in AI to help analyse large volumes of data across an enterprise. It aggregates data from all sources, including users, applications, servers, and devices running on-premises or in any cloud.

By using scalable machine learning algorithms, the platform correlates millions of low-fidelity anomalies to present a few high-fidelity security incidents to the analyst.

AZURE SENTINEL USES AI TO TRIAGE ALERTS AND PERFORM CORRELATION ACROSS VARIOUS PRODUCTS AND SERVICES.

3

HOW DOES AZURE SENTINEL DIFFER FROM OTHER SIEM TOOLS?

Azure Sentinel aims to stand out from other SIEM tools by leveraging the scalability and flexibility of the cloud – and by tapping artificial intelligence to reduce cyberthreat noise.

Because the tool is built on Azure, enterprises can take advantage of significant cloud speed and scale, investing time and money into security instead of servers and hardware.

Users can also connect data from various sources – across devices, servers, applications, and users, both on-premise and remotely.

For many, SIEM systems tend to be client-server based while also being focused on a specific security niche.

> "The use of AI in Azure Sentinel has helped to enable a 90% reduction in “alert fatigue” among early users"
>
> Ann Johnson, Corporate Vice President for cybersecurity at Microsoft

As a result, most enterprises have more than 50 security solutions in place – creating a complex environment where it is difficult to react quickly to security alerts.

Azure Sentinel, on the other hand, classes itself as a true SIEM-as-a-service claiming it can potentially reduce the number of security solutions required by many enterprises, leading to cost savings and therefore a new class of intelligent security technologies.

4

AZURE SENTINEL - WHO IS IT FOR?

Microsoft Azure Sentinel has been designed to help security operations teams across companies of all sizes and differing industries, improve detection, protection and data security.

Early partners working with Azure Sentinel include global technology companies - Accenture, Insight, F5 and New Signature.

Launched in March earlier this year, it comes at a time when vast volumes of data have created issues for security professionals, who are often too overwhelmed by alerts to focus on solving complex security problems.

5

HOW DOES IT USE AI AND MACHINE LEARNING?

The ML models in Azure Sentinel are based on Microsoft's work in protecting customers' cloud assets.

There are three ML toolkits available that can be tailored to the security community; 'Fusion', 'built-in ML' and 'build your own ML'.

FUSION

Microsoft's Fusion technology, currently in public preview, uses scalable learning algorithms to correlate millions of low-fidelity anomalies into tens of high-fidelity cases.

Azure Sentinel integrates with Microsoft 365 solution and correlates millions of signals from different products such as Azure Identity Protection, Microsoft Cloud App Security, and soon Azure Advanced Threat Protection, Windows Advanced Threat Protection, O365 Advanced Threat Protection, Intune, and Azure Information Protection.

BUILT-IN ML

Currently in limited public preview, Built-in ML is designed for security analysts and engineers, with no prior ML knowledge to reuse ML systems designed by Microsoft's fleet of security machine learning engineers.

It uses principles of model compression and elements of transfer learning to make the model developed by Microsoft's ML engineers ready to use for any organisation's needs.

BUILD-YOUR-OWN ML

For companies who need to delve deeper and customise the analysis further, there is the option of build-your-own ML.

Azure Sentinel will offer Databricks, Spark, and Jupyter Notebook detection's authoring environment, in order to take care of data plumbing, provide ML algorithm in templates, code snippets for model training and scheduling, and soon introduce seamless model management, model deployment, workflow scheduler, data versioning capabilities and specialised security analytics libraries.

6

HOW DOES IT FIT INTO AN ORGANISATION'S SECURITY ORCHESTRATION?

Until recently, the one thing that seemed to be lacking for many organisations was a central orchestrator. Enterprises have been linking alerts generated by Microsoft security solutions back to their on-premise SIEM solution, but with the increasing volume of data, it has become apparent that many SIEMs are unable to scale accordingly.

This is where Azure Sentinel classes itself as different to other traditional SIEMs, providing a central place to analyse security data, across all parts of the environment, at scale.

Azure Sentinel can ingest events from several Microsoft and non-Microsoft platforms, including:

Azure AD Identity Protection, Microsoft Cloud Application Security, Azure Security Center, Microsoft Graph Security API, DNS, Syslog and third-party telemetry including F5, Palo Alto Networks, Checkpoint, and Cisco ASA.

7

CAN IT WORK ALONGSIDE OFFICE 365?

Many organisations are using Office 365 and are increasingly adopting the advanced security and compliance offerings included in Microsoft 365. In just a few clicks organisations can bring data into Azure Sentinel from Office 365, where it can be combined and analysed alongside other security data from users and end point applications to understand a complete attack.

The Office 365 activity log connector provides insights into ongoing user activities and provides information about various user, admin, system and policy actions and events.

By connecting Office 365 logs into Azure Sentinel data can be used to view dashboards, create customer alerts and improve the investigation process.

8

CAN IT INTEGRATE WITH AN ORGANISATION'S EXISTING TOOLS?

Azure Sentinel can be integrated with an organisation’s existing tools, whether business applications, other security products or home-grown tools along with independent machine learning models.

Organisations can optimise for their own needs, by bringing their own insights, tailored detections, machine learning models and threat intelligence.

9

WHAT IS THE COST?

Azure Sentinel is currently available in public preview only, during this preview stage it is **free to use**.

Microsoft hasn’t yet communicated how it will be priced once it goes live. Pricing will be announced in the future and a notice will be provided prior to the end of the preview.

10

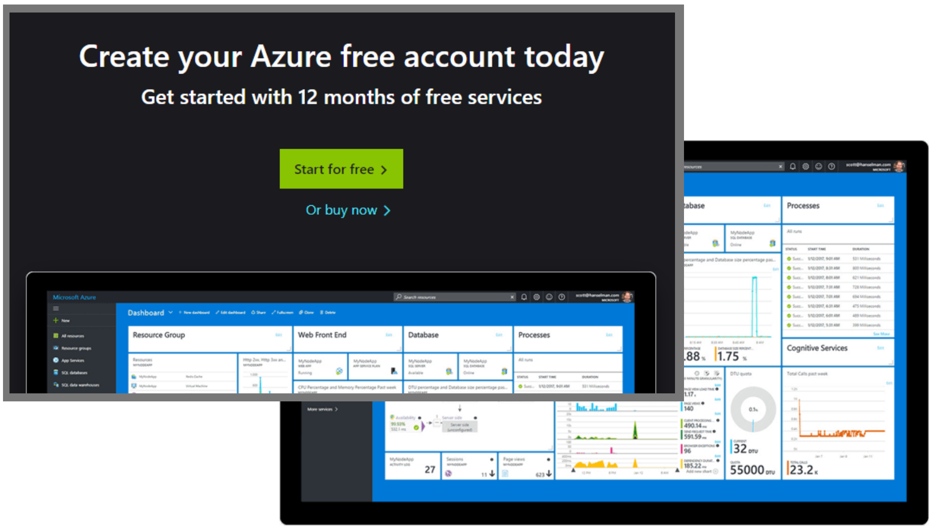
HOW DO I GET STARTED?

To get started, you need a subscription to Microsoft Azure.

If you do not have a subscription, you can sign up for a **free trial**.

For more information about Azure Sentinel, or to find out about our recruitment services please contact us:

info@contextrecruit.com
T: 023 8168 0400



Create your Azure free account today

Get started with 12 months of free services

Start for free >

Or buy now >

The above is intended as an overview only and is in no way comprehensive.
It is not a substitute for legal or business advice.