Azure Sentinel Service

Stay ahead of threats with intelligent security analytics

Cyber-crime attacks continue to grow. With the increase in remote workers more people are operating from mobile devices and from cloud-based platforms than ever before. Together with the explosion in connect devices through IoT, security is an increasingly complex concern for all organisations.

Microsoft has developed Azure Sentinel, a cloud-based Security Information and Event Management System (SIEM), and Security Orchestration Automated Response (SOAR) solution to help alleviate the stress. It delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

The Azure Sentinel Service from the security team at Zetta will give you an understanding of the solution and a deployed instance in your environment in less than a week, allowing you to gain visibility and take back control of your IT security.

Our Approach

Zetta's Azure Sentinel Service is an onsite, consultancy engagement that provides training and implementation. It will help you take advantage of this cutting-edge technology from Microsoft to strengthen and simplify your security environment. During our engagement we will familiarise your team with the new technology and provide you with a working environment you can begin using right away.

Why Zetta for Azure Sentinel?

WA headquartered

Our team is all based in Perth, so you will be guaranteed to have our A-team as your core team, from start to finish.

Fast

We provide you with a working environment that you can begin using right away.

Agile

Using an agile approach, we continuously incorporate real-time feedback to ensure that Sentinel provides valuable insights quickly.

Microsoft experts

Highly certified, we hold 10 Gold and Silver Competencies including:

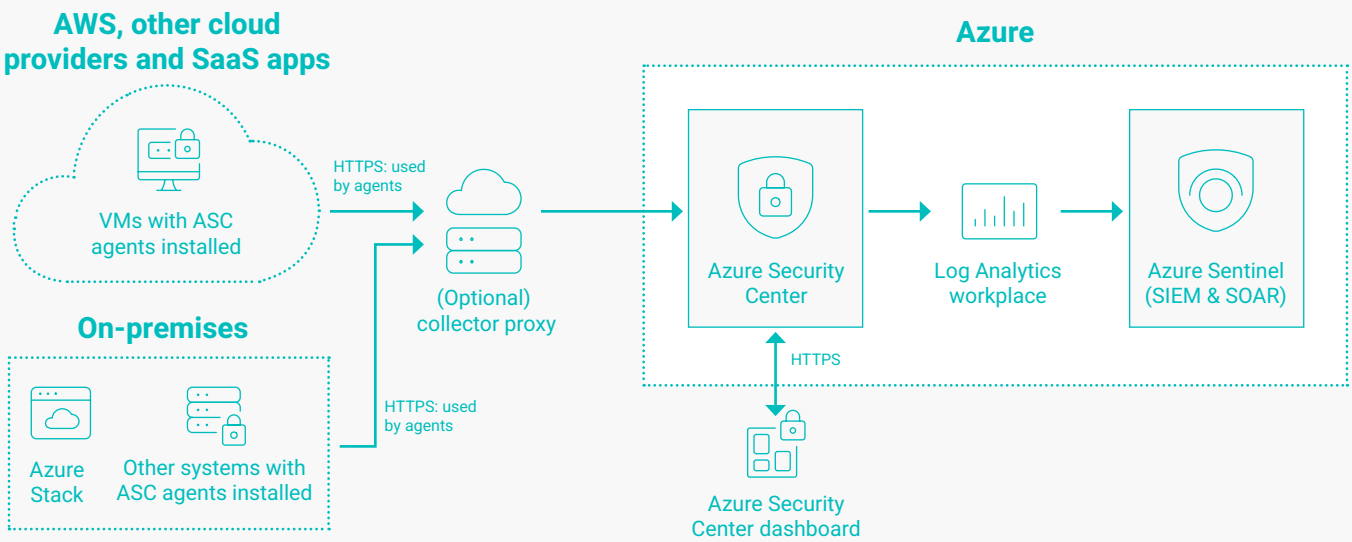
Security | Cloud Platform | Data Centre

Highly skilled

Our dedicated team of security consultants specialise in designing, implementing and managing solutions based on Microsoft technology.

Customer focused

We truly value your business, and the opportunity to become an extension of your team. We listen, and we respond, fast.



About Azure Sentinel

Azure Sentinel was created to provide a whole new level of control and visibility across your entire IT security environment. Centrally managed, you can see all users, devices, applications, and infrastructure deployed on-premises and in multiple clouds. Plus, by using AI and ML to detect, analyse, and investigate threats, Azure Sentinel delivers the intelligence your security team needs to be resource efficient.

Collect data at cloud scale – across all users, devices, applications and infrastructure, both on-premises and in multiple clouds

Investigate threats with AI and hunt for suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft

Detect previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence

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

Service Level Options

We offer 3 service levels to select from based on your environment:

Essentials

- Up to 4 connectors
- Workbooks for each connector

Advanced

Essentials plus:

- Additional 4 connectors
- Workbooks for each additional connector

Premier

Essentials & Advanced plus:

- Custom connectors including non-Microsoft
- Customised workbooks for each connector
- Customised alert responses for each connector

How does the service work?

Our Azure Sentinel Service is a three-part engagement:

01 - Assessment and Set-Up

2-5 days

- Our security consultants identify data sources for your Azure Sentinel Service
- We deploy Azure Sentinel and create a log analytics workspace to analyse your data
- We connect up to four, existing Microsoft data sources into your Azure Sentinel SIEM

02 - Monitoring

1-2 weeks

- Logs are registered in Azure Sentinel

03 - Reporting

1 week

- We review data sources and flow into Azure Sentinel and provide training on how to monitor and visualise this activity
- We highlight the threats and identify the gaps in your security posture
- Together we discuss your long-term strategy for a holistic security practice using Azure Sentinel and various data sources

Simplifying a complex world

We help our clients to digitally transform and manage their ICT infrastructure. Leveraging our unique intellectual property (IP) and the Microsoft 365 platform, our team helps clients from design and architecture to implementation and management. Specialising in Modern Work, Security, Cloud & Infrastructure solutions we enable your journey towards improving workforce productivity and organisational cybersecurity posture.

zetta

Simplifying a complex world

zetta.com.au | 1300 307 710