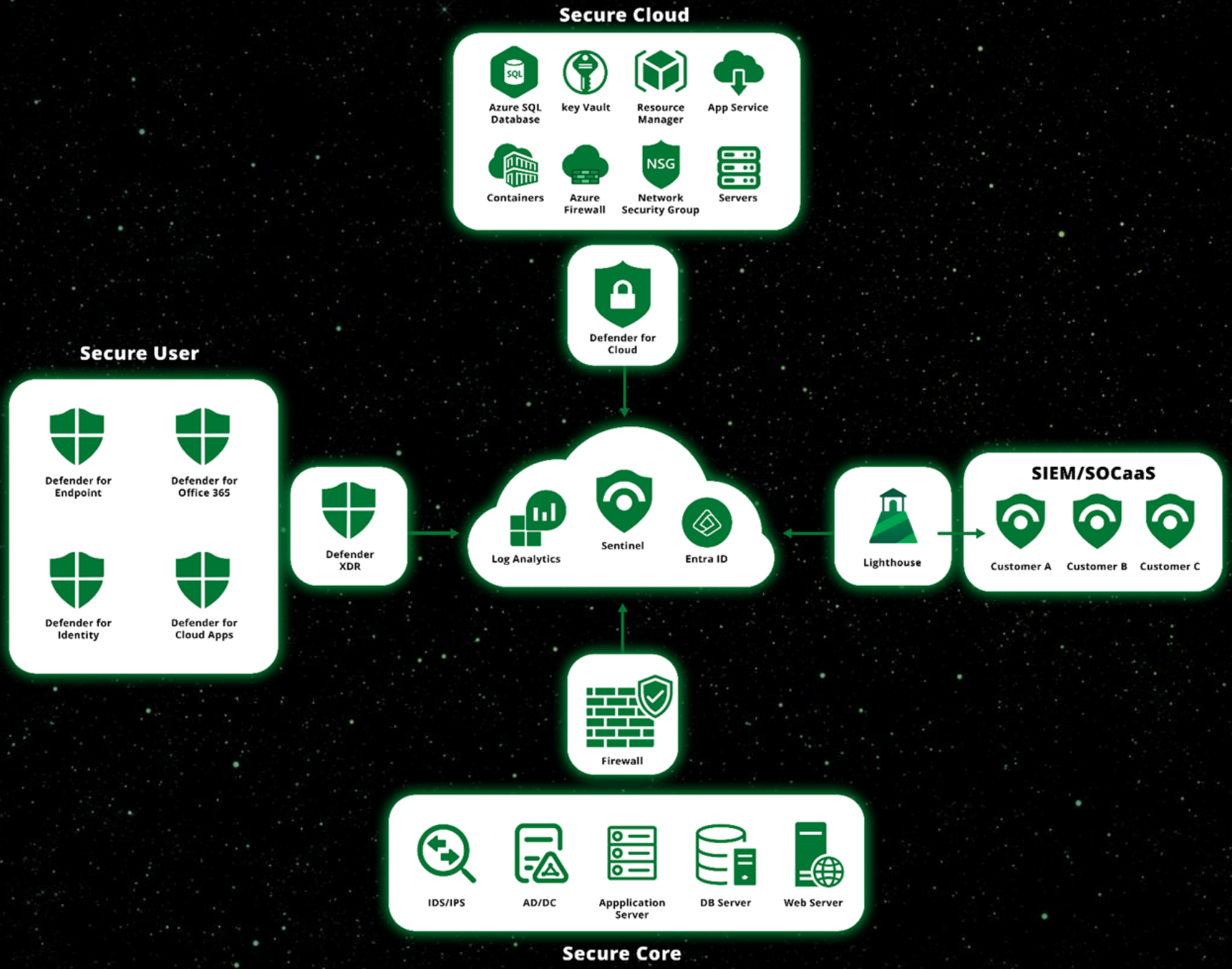
Security service

centric
connect.engage.succeed.

SOC as a Service (SOCaaS)

Focuses on analyzing alerts from all customer environments and escalating to incident response team.

- 24/7 Monitoring: Round-the-clock monitoring capabilities to detect threats in real-time.
- Advanced Threat Detection: By staying ahead of emerging threats and leveraging sophisticated technologies, we ensure proactive defense measures and strategic response strategies, safeguarding your digital assets against even the most sophisticated adversaries.
- Incident Response: Our service will support your IT and Security teams in incident response.
- Meet compliance requirements: By monitoring and responding to incidents of highest risk and most critical infrastructure your organization will cover NIS 2, ISO 27001 and ISAE 3402 compliance requirements.
- Trend Analysis: By performing daily dashboard checks, the security team will investigate discrepancies, raise requests for information, and provide suggestions for possible fixes.
- By utilizing Microsoft tooling: security suite we managed to increase efficiency within our daily workloads.
- When you choose our SOCaaS solution, you also have the option to enhance your cybersecurity with Vulnerability Management and Employee Training. These additional services come at extra cost but provide added layers of protection for your business.


Secure Cloud
Azure SQL Database
key Vault
Resource Manager
App Service
Containers
Azure Firewall
Network Security Group
NSG
Servers
Defender for Cloud
Secure User
Defender for Endpoint
Defender for Office 365
Defender for Identity
Defender for Cloud Apps
Defender XDR
Log Analytics
Sentinel
Entra ID
Lighthouse
SIEM/SOCaaS
Customer A
Customer B
Customer C
Firewall
IDS/IPS
AD/DC
Appplication Server
DB Server
Web Server
Secure Core

Benefits

NIS2 sets a baseline of cybersecurity risk management measures and reporting obligations.

The good news is that NIS2 compliance aligns to the same Zero Trust principles addressed by Microsoft Security solutions, which can help provide a solid wall of protection against cyberattacks across the entire attack surface.

The key to effectively cyber attack protection is choosing the right security information and event management (SIEM) and extended detection response (XDR) systems. Based on the Microsoft Security suite, you will get a fully integrated approach to security—and streamlined security threat investigation and response.

Reduced likelihood of a breach by 72%

- Ensure the security of your critical IT infrastructure with Microsoft's innovative security products, featuring integrated AI (Artificial Intelligence), Threat Intelligence, and Machine Learning capabilities. By proactively blocking threats, drastically minimize the risks of hacking and reduce the potential for prolonged downtime.

Increase by 50% in IT and security team efficiency.

- Microsoft Security solutions seamlessly integrate with most products by reducing workload, integrated AI reduces incident triage time.

Peace of Mind

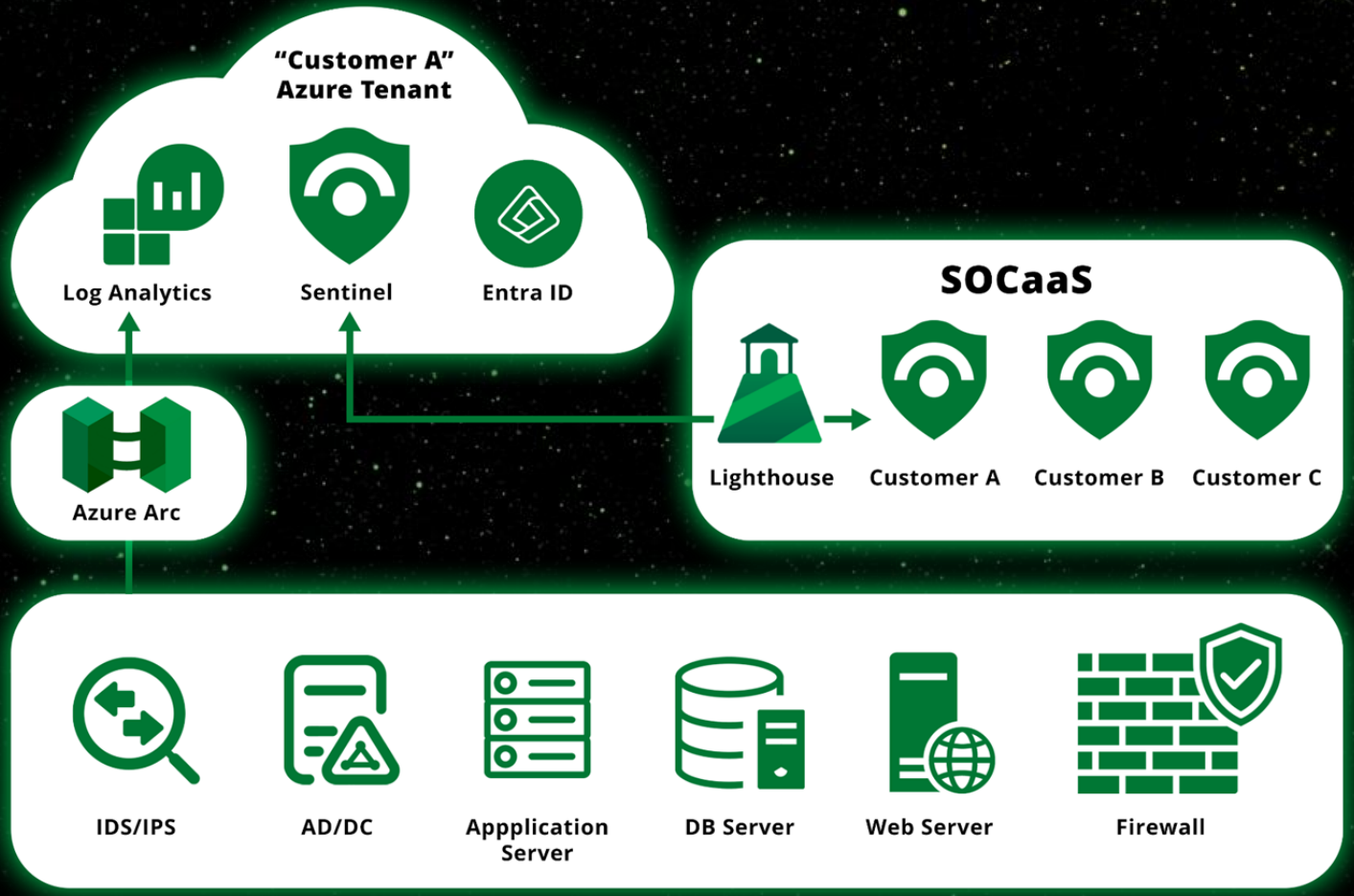
- Our round-the-clock monitoring will notify you on time so you can act without waiting. Sleep well knowing that we are watching your back.

Compliance with NIS 2 & ISO

- Microsoft Security solutions are designed so organizations can better manage security risks, protect against cyberattack, and minimize the impacts of cybersecurity incidents.

Plan 1 - Secure Core

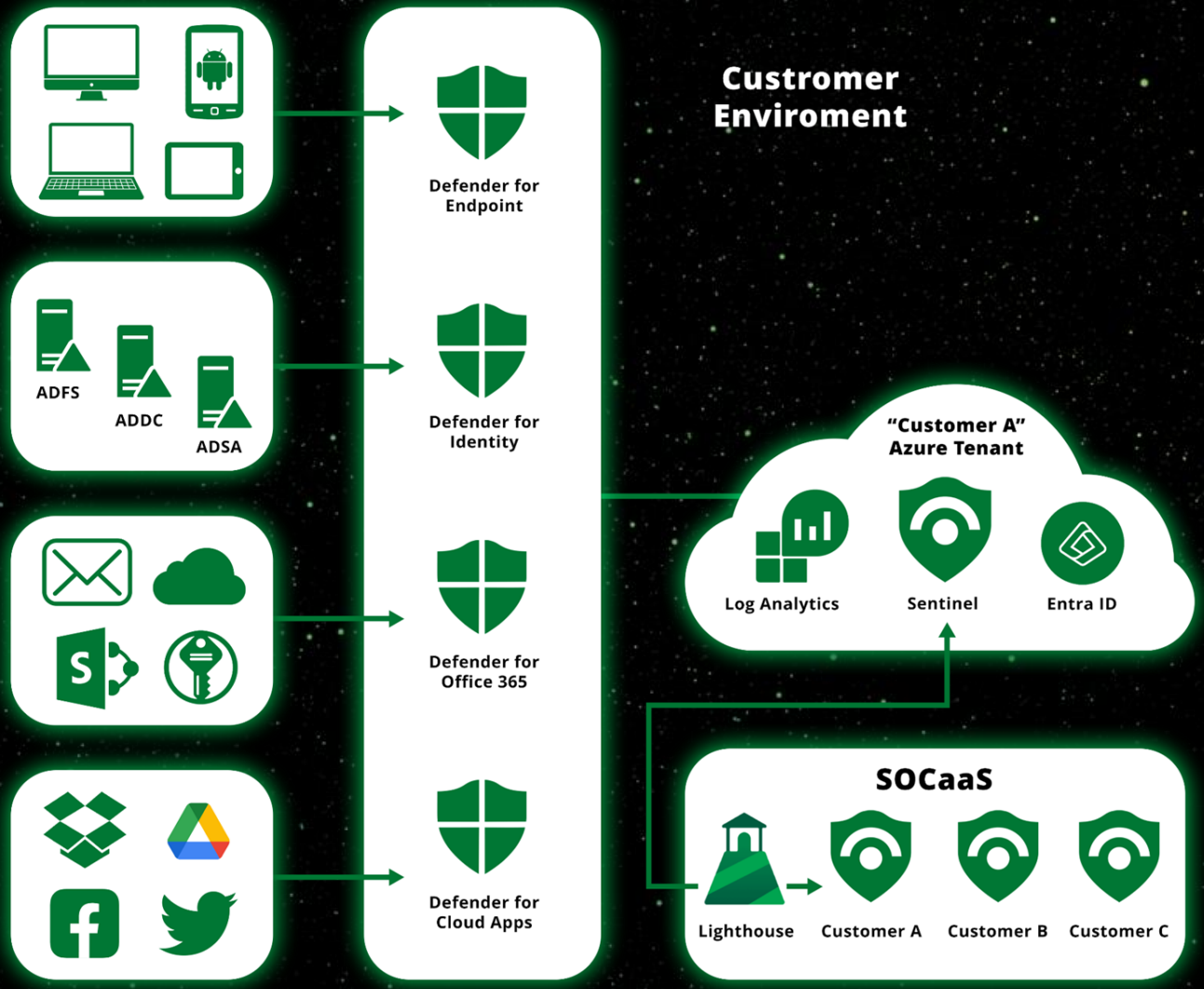
Utilize your log data and send it to Sentinel SIEM solution for Triage. We have 200 + Use cases that will cover the most important aspects of your security and compliance.



Plan 1 - Secure Core Options

	Basic	Advanced	Pro	Pro +
Identity Protection				
Network Protection				
App Security WAF				
App Security IIS				
App Security Syslog				
App Security Database				
Infrastructure size (CI)	5	22	75	154
Analytics rules	Up to 48	Up to 118	Up to 200	200+

Plan 2 – Secure User



Choose products in any order you like:

Defender for Endpoint

Secure endpoint devices across your enterprise.

Defender for Office 365

Protect your email and collaboration tools from advanced cyberthreats, such as phishing and business email compromise.

Defender for Identity

Manage and secure hybrid identities and simplify employee, partner, and customer access.

Defender for Cloud App

Get visibility, control data, and detect cyberthreats across cloud services and apps.

Centric’s Endpoint Monitoring Services provide 7x24 monitoring and alerting of your organization's endpoints, including desktops, laptops and mobile devices.

Our services include:

Real-time Threat Detection:

- Monitor and investigate threats in real time 7x24. Triage and escalate incident to a customer’s response team.

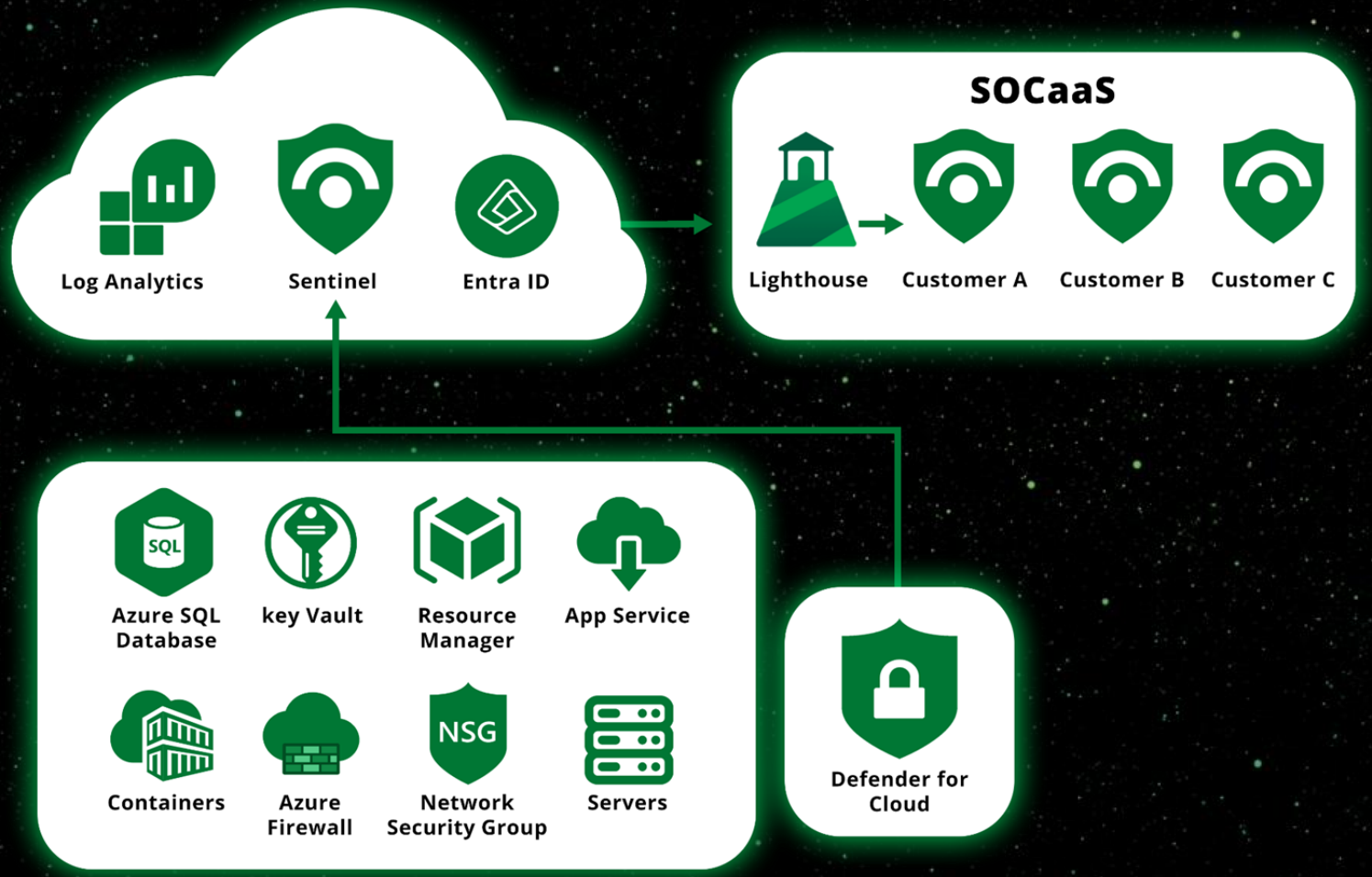
Incident Response:

- Our Security Operations Center (SOC) in Kaunas provides robust support to empower your IT team in promptly addressing security incidents, minimizing any impact on your business.

Endpoint Protection Configuration:

- We optimize and configure Microsoft Defender to ensure maximum protection against known and emerging threats.

Plan 3 - Secure Cloud



Scope:

- **Azure Firewall**
- **Network Security Group**
- **Web Application Firewall**
- **Defender for Server**
- **Defender App Service**
- **Defender for Database**
- **Defender for Storage**
- **Defender for Kubernetes**
- **Defender for Key Vault**
- **API Manager**
- **Resource Manager**

Protect your cloud workloads

Monitor and investigate threats in real time 7x24. Triage and escalate incident to a customer's response team.

Incident Response:

Our Security Operations provides robust support to empower your IT team to promptly respond to security incidents, minimizing any impact on your business.

Endpoint Protection Configuration:

We will assist you in interpreting and recommending best configuration practices within:

- Centralized policy management,
- Secure Score,
- Cloud Security Posture Management (CSP)

Contacts