open systems

WHITEPAPER

Leverage the Power of Multi-cloud Infrastructure and Software as a Service Solutions using SASE and MDR

swiss safety center ISO 27001 certified system

Open Systems
services are
ISO 27001 certified.

Across almost all industries, today's IT professionals need to support digital transformation, a sudden growth in remote workers, and the move to cloud and multi-cloud. Traditional hub-and-spoke networking and security models – revolving around physical data centers and endpoint detection and response (EDR) – are failing to keep up with these trends.

To address the limitations of old-school architectures, enterprises began adopting a more modern approach to networking and security with software-defined wide area networks (SD-WAN). Some people think SD-WAN is about cost-savings. But it is about much more than moving expensive communications connectivity to less expensive connectivity – such as, for example, moving from MPLS to internet and accessing cloud. The SD-WAN fabric forms a software overlay network that runs over standard network transport services such as the public Internet, MPLS, and broadband.

This overlay network also supports next-generation software services, which enables you to accelerate your shift to modern compute environments and workflows such as cloud networking, remote and mobile, and IoT and the intelligent edge.

SASE, a transformational next step

The next step in this direction is secure access service edge, or SASE (pronounced "Sassy). In its recently published report, The Future Network Security Is in the Cloud, Gartner defined SASE as "an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS, and ZTNA) to support the dynamic secure access needs of digital enterprises."

Gartner also called SASE "transformational" because it inverts the traditional networking and network security model by turning the data-center-centric approach inside out. By distributing security across the entire SASE stack, you can eliminate mundane aspects of the network and network security operations.

Gartner sees 40% of enterprises adopting SASE strategies by 2024.

So, it should come as no surprise that, in addition to continued strong growth in SD-WAN adoption, Gartner sees 40% of enterprises adopting SASE strategies by 2024.

MDR, the key to containment

Companies can also gain significant benefits by integrating SD-WAN and SASE with a managed detection and response (MDR) service that incorporates a cloud-native SIEM. This combination can answer chronic problems facing security teams such as increasingly complex security stacks, challenges securing of cloud and multi-cloud environments, and a chronic shortage of trained analysts.

An effective MDR should also be designed with the assumption that all networks are in a constant state of breach. The viable solution to this challenge, and to stopping incidents earlier in the cyber kill chain is continuous monitoring. Security experts should staff the service's security operations center, providing eyes on your environment 24x7. Using sophisticated detection tools, these experts can detect only credible threats and quickly run the most urgent incidents to ground.

A managed service keeps data secure while improving access and availability

More importantly, an effective MDR solution should leverage input from all the components of a SASE stack as well as legacy firewalls and external endpoint detection and response solutions such as Carbon Black and Microsoft Defender ATP. By bringing in log data, including context, from these elements it can deliver access without latency, global security policies, and data protection with:

- Unified Threat Protection & policy enforcement
- Automated remediation
- Threat Intelligence

The integration of the SIEM and the SASE stack further provides improvement over an endpoint security model because it can contain threats at the web proxy. Plus, with the addition of SOAR (Security Orchestration, Automation and Response) such an MDR solution allows an organization to collect threat data from multiple sources and respond to less-critical security events without human assistance.

Accessing a security operations center (SOC) as a service further ensures consistent and effective central policy management as well as the capability to rapidly react to business changes. In particular, SD-WAN and SASE help to solve problems that you find in most traditional networking and security architectures.

One example is the speed-bump effect of security controls. If developers have to wait days for IT to update firewall policies whenever they bring up a new app in the cloud, for instance, productivity will take a hit, and users may adopt shadow IT workarounds. If users can download and upload data to any SaaS or cloud app (vetted and authorized by IT or not), you surely have data leakage taking place. Enabling millions of employees working from home to remotely access corporate networks, as we have during the current pandemic, has also increased the vulnerability of enterprises to cyberattack. This is true even in instances where enterprises have employed full security stacks with up-to-date software.

Overcoming the critical shortage of experts

However, staff performance/usability and security issues will always vie for the attention of your limited IT staff. We all know the cost of and difficulty of recruiting and retaining skilled security and networking experts. In a major 2019 study, the certifications organization (ISC)2 found the number of unfilled security positions then stood at 4.07 million professionals, up from 2.93 million in the previous year. This included 561,000 in North America and a staggering 2.6 million shortfall in APAC.

So, how do you meet the demand to deliver your users fast, secure access to applications and services no matter where they are or what device they are using to access it? First and foremost, having security built into the network – not sitting in a data center – takes security to the edge and to your branch offices and remote users.

The next step is to face the reality of a chronic worldwide shortage of skilled security professionals. Finding these experts and integrating the expensive tools required to build a SOC could take years. The realistic choice is to outsource the function. This will give you around-the-clock overview of your security posture by experts – skilled professionals that would be difficult if not impossible to recruit, train and retain in the numbers needed.

Get the force-multiplier effect of networking and security as a managed service

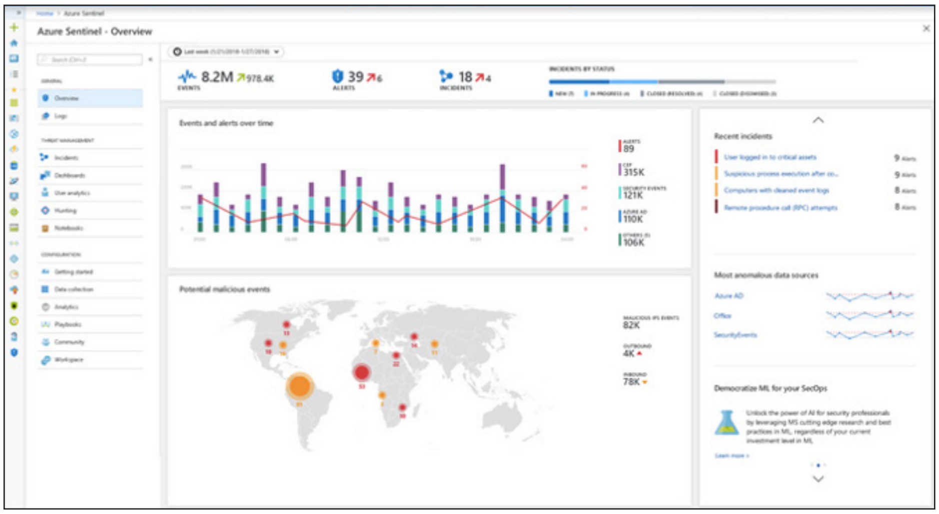
By delivering threat detection and incident response together as a managed service, MDR provides huge benefits. The synergies between the integrated SASE stack and the MDR service make it possible to detect threats with more accuracy.

Microsoft Azure Sentinel brings world-class SIEM capabilities

A cloud-native SIEM and SOAR solution, Microsoft Sentinel uses artificial intelligence (AI) and machine learning (ML) and a use case library curated by the MDR service operators to look for only the threats that matter. Then, human intelligence tracks threats to ground and advises customers on the most effective incident response.

As a new type of SIEM built for a cloud and multi-cloud native world, it connects to and collects data from all customer sources including users, applications, servers, and devices running on-premises or in any cloud. Its advanced analytics link massive amounts of threat intelligence and security data to provide MDR customers with unparalleled threat detection.

Highly skilled experts staffing the SOC can use Azure Sentinel to see and contain threats. It provides visibility – a single pane of glass – across the customer's entire organization. In addition, it distills decades of Microsoft security expertise into advanced threat detection algorithms that complement the expertise of the SOC's security professionals.



User logged in to critical assets	9 Alerts
Suspicious process execution after co...	9 Alerts
Computers with cleaned event logs	8 Alerts
Remote procedure call (RPC) attempts	8 Alerts

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

SASE also integrates comprehensive security features, which avoids the need to acquire and manage multiple bolt-on/stitched together security point solutions. These built-in security tools also feed log data into the SIEM. Consequently, an MDR service based on SASE and Sentinel collects data at cloud scale – across all users, devices, applications and infrastructure – both on-premises and in multiple clouds.

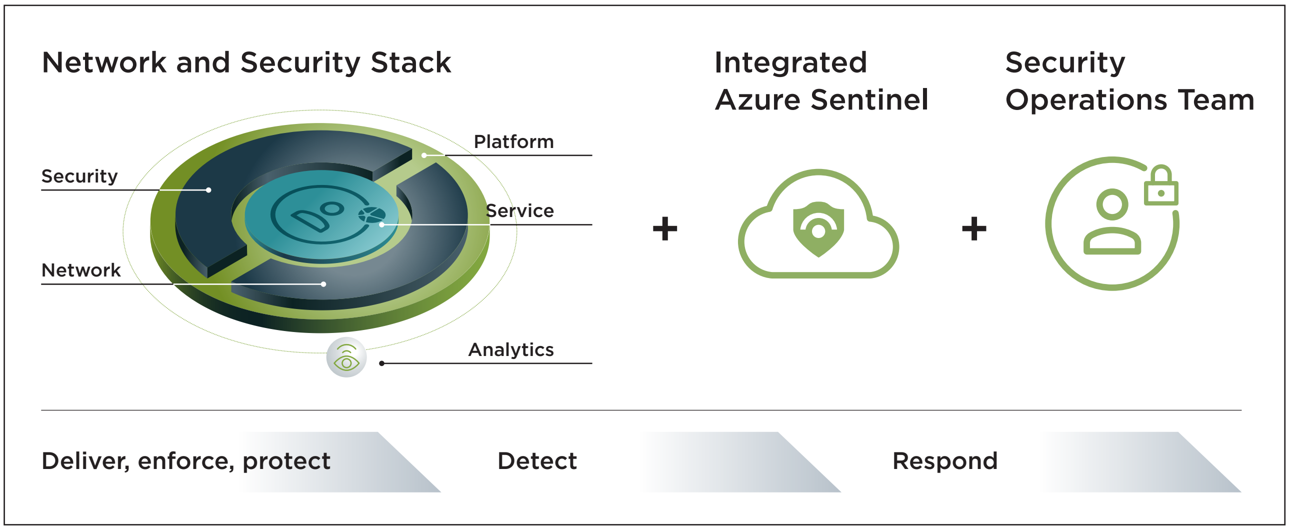
The combined human intelligence and artificial intelligence (Sentinel) enables the MDR service to:

Collect – Easily gather data at cloud scale across users, devices, applications and infrastructure both on-premises and across multiple clouds.

Detect – Sentinel recognizes both zero days and previously discovered threats and minimizes false positives by using analytics and threat intelligence drawn directly from Microsoft. This includes unique vast threat intelligence (gained from millions of unique threat indicators collected worldwide) and Microsoft cybersecurity experience.

Investigate – Machine learning and AI identify threats and hunt suspicious activities at scale. Once surfaced by the machine, security experts run the credible threats to ground.

Respond – Security experts in the MDR service can also acquire an intimate understanding of the customer’s environment and based on the rich threat data delivered by Azure Sentinel, advise customers on the most effective way to contain any threat.



For organizations considering MDR, you should also look for a solution that integrates MITRE recommendations into the threat detection model.

The Open Systems MDR – Advanced threat detection, SASE integration, and the human element

As a leading innovator in SD-WAN and SASE, Open Systems has integrated a world-class MDR capability with its SASE solution. This MDR service takes a world-class SIEM capability (built on Azure Sentinel) and combines it with human experts plus the rich log data and real-time capabilities of SASE.

By effectively combining human and machine intelligence, 90% of all tickets are resolved without customer intervention.

Finding only the alerts that matter – i.e., credible indicators of significant threats – is like finding the proverbial needle in a haystack. There are simply not enough people or person hours in the typical IT organization to run every threat to ground. This is where the power of a machine comes into play. Microsoft Sentinel technology, combined with the threat detection model from Open Systems, reduces noise and amplifies signal for the Security Analysts.

It also accelerates the Open System's analysts' proactive threat hunting ability with pre-built queries based on years of security experience. They can view a prioritized list of alerts, get correlated analysis of thousands of security events within seconds, and visualize the entire scope of every attack. More than 80% of all network problems are proactively detected and ticketed by AI-based automated monitoring technology, which leaves the Open Systems experts free to focus on resolving them quickly. By effectively combining human and machine intelligence, 90% of all tickets are resolved without customer intervention.

The power of having an integrated SD-WAN/SASE platform not only speeds detection and response but can also prevent breaches. For example, once a credible threat is detected in the SOC with the help of Azure Sentinel, you can authorize a block or isolation the compromised system. And since the SD-WAN / SASE service is integrated from end to end – with security controls close to the users – the response can work in real time.

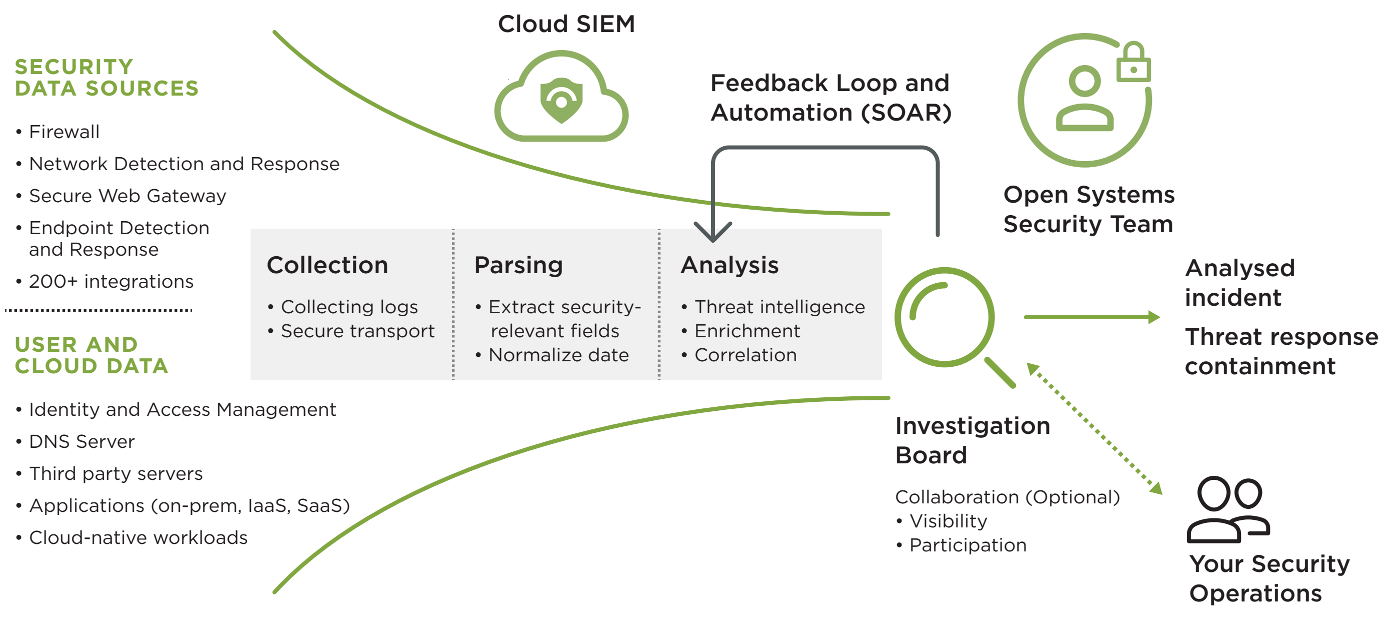
Industry leaders in SD-WAN and SIEM team up to simplify and improve your security posture

The combination of best-in-class technology with the best security and networking experts available simplifies security operations and speeds up threat response.

- Reduces noise from legitimate events with built-in machine learning and knowledge based on analyzing trillions of signals daily
- Accelerates proactive threat hunting with pre-built queries based on years of security experience
- Allows you to view a prioritized list of alerts, get correlated analysis of thousands of security events within seconds, and visualize the entire scope of every attack
- Simplifies security operations and speed up threat response with integrated automation and orchestration of common tasks and workflows
- Incorporates best practices from MITRE

Managed Detection and Response Platform

From data collcetion alerts and threat containment



SECURITY DATA SOURCES

- Firewall
- Network Detection and Response
- Secure Web Gateway
- Endpoint Detection and Response
- 200+ integrations

USER AND CLOUD DATA

- Identity and Access Management
- DNS Server
- Third party servers
- Applications (on-prem, IaaS, SaaS)
- Cloud-native workloads

Cloud SIEM

Collection

- Collecting logs
- Secure transport

Parsing

- Extract security-relevant fields
- Normalize date

Analysis

- Threat intelligence
- Enrichment
- Correlation

Feedback Loop and Automation (SOAR)

Open Systems Security Team

Investigation Board

Collaboration (Optional)

- Visibility
- Participation

Analysed incident

Threat response containment

Your Security Operations

The Open Systems MDR service, with its SIEM capability built on the industry-leading Azure Sentinel platform integrates automation and orchestration of common tasks and workflows. You can also work with Open Systems to optimize the solution for your unique needs by bringing your own insights, tailored detections, machine learning models, and threat intelligence.

Contact us for a free assessment by an Open Systems security engineer.

CONTACT US

opensystems

The digital transformation journey demands agility and defensibility from your IT infrastructure. Open Systems' secure access service edge (SASE) solution unifies security and comprehensive networking capabilities, enabling organizations to connect their clouds, branches, applications and users anywhere in the world, in a secure and flexible way. Open Systems' cloud-delivered Secure SD-WAN and Managed Detection and Response (MDR) services combine 24x7 experts with AIOps and an automation platform to deliver immediate peace of mind, and future-proof your business.

Learn more at **open-systems.com** | Approved for public use.