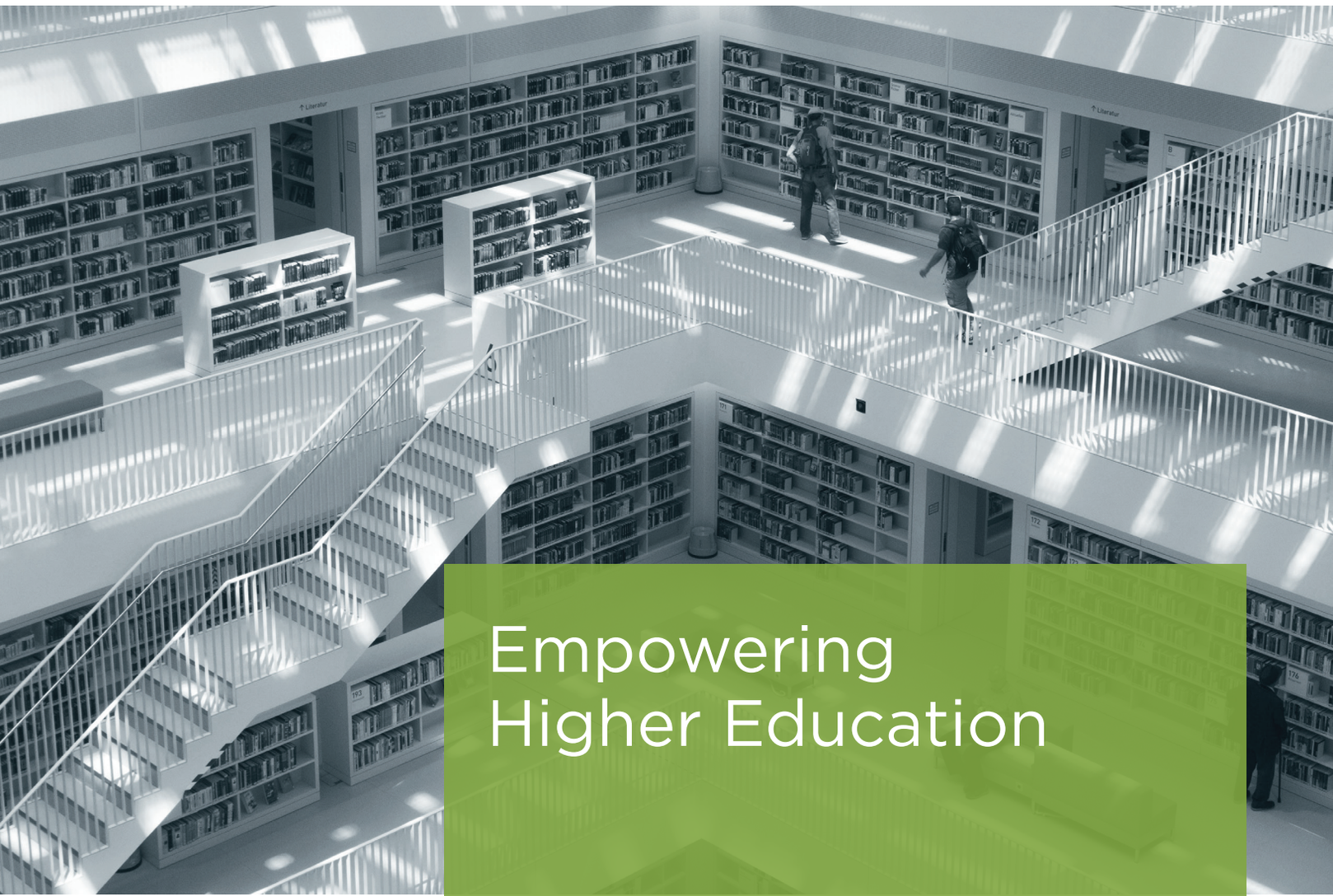


Empowering Higher Education

A cost-friendly approach to managed security operations on and off campus

INDUSTRY SOLUTION BRIEF

Open Systems services are ISO 27001 certified.

What are some of the current IT operations challenges in a higher education setting?

Inhomogeneous environment

Securely interconnect a zoo of gadgets and devices, ensuring consistent strategy and policies in a zero-trust environment.

Understaffed IT and outdated skillsets

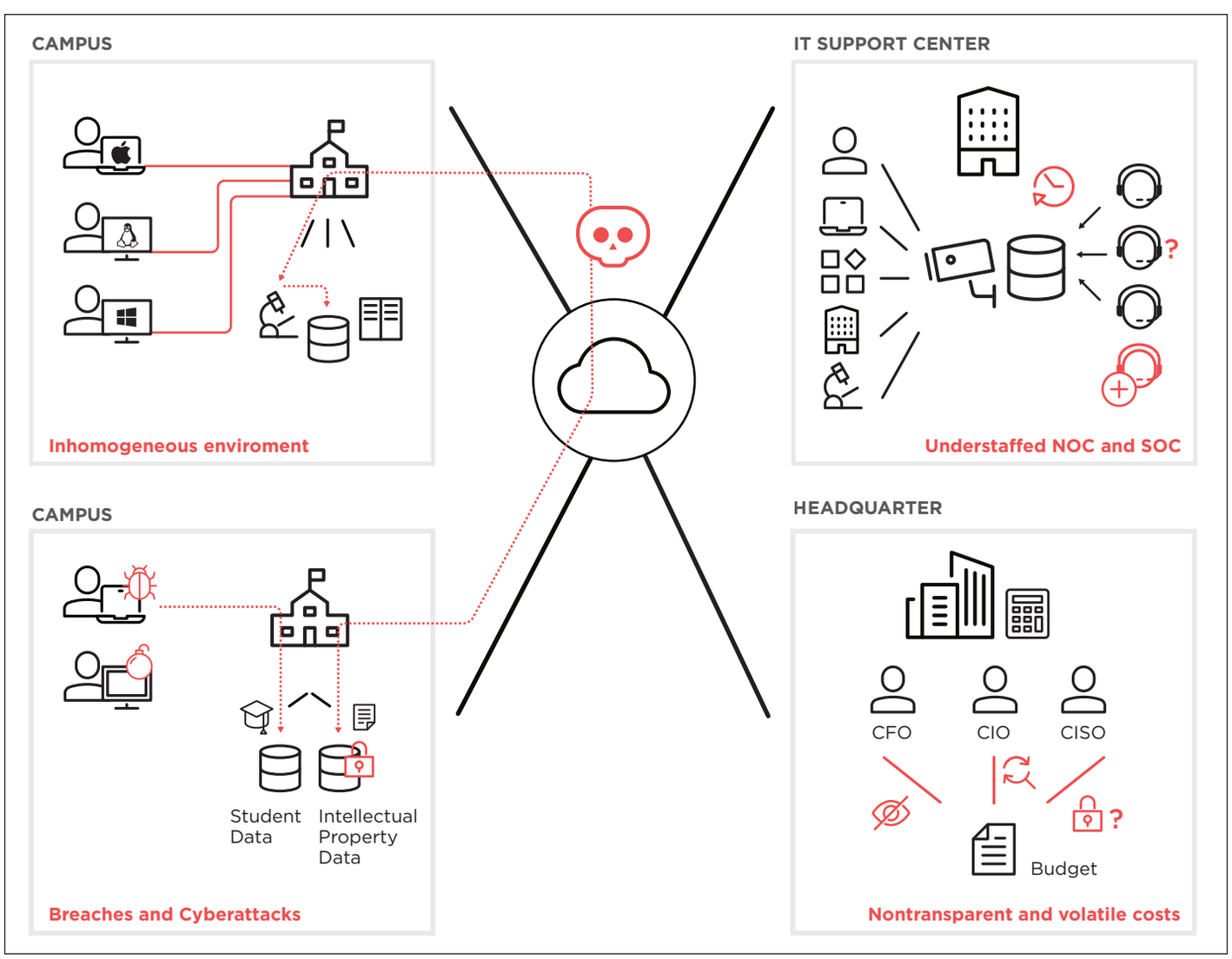
Focus on supporting your end users in day-to-day operations while offloading 24x7 security maintenance, monitoring and troubleshooting to a SOC.

Breaches and cyberattacks

Develop a customized risk-based strategy to manage a large attack surface and protect sensitive data. Cover the whole kill chain and stay tuned to real alerts.

Cost is of the essence

Budget up front for an all-inclusive SOC without hidden charges, which will also give you more flexibility to phase products in or out in a multi-point life cycle.



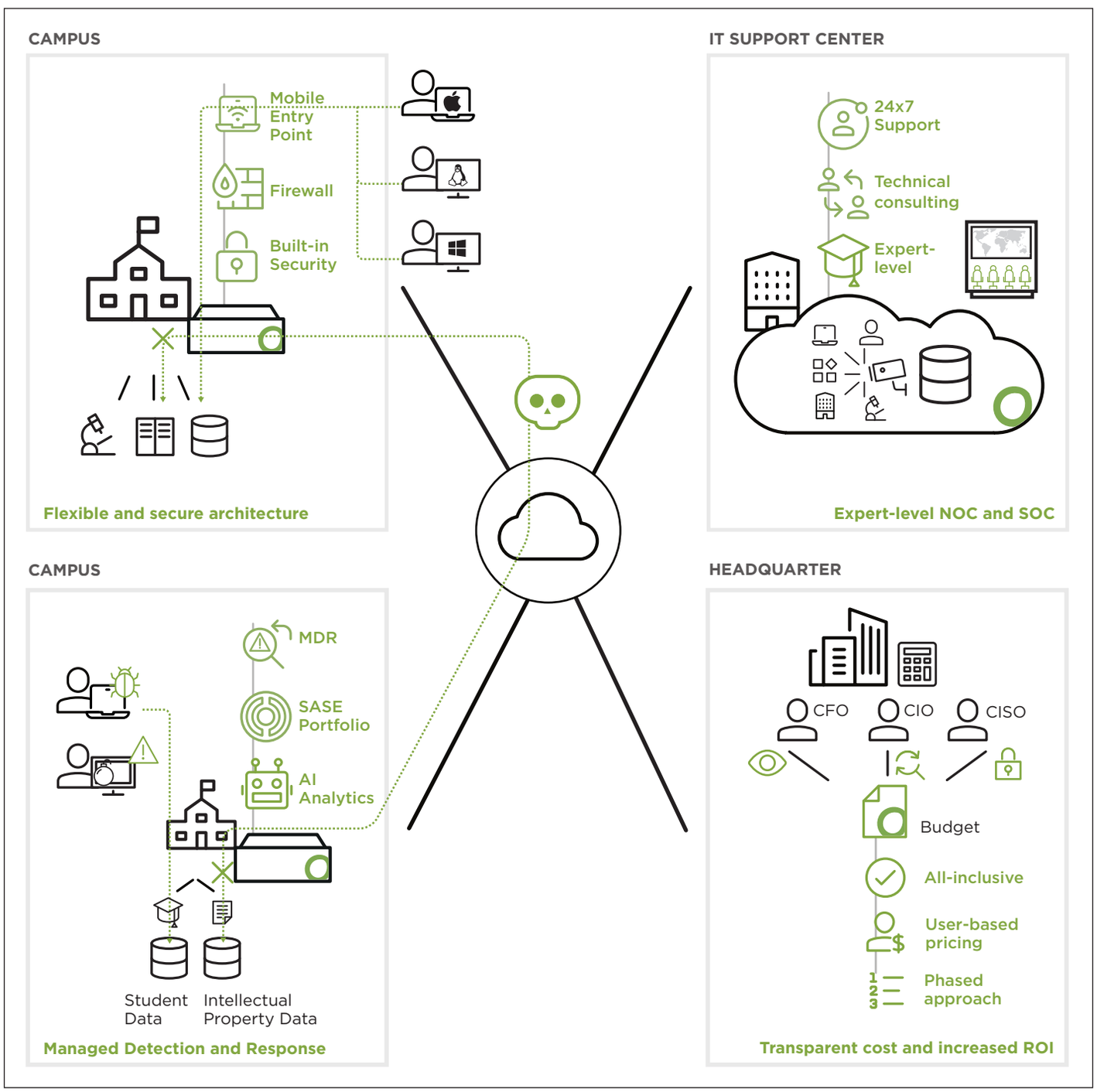
Most common pain points of higher education institutions in their IT network and security environments

Your primary focus are students and faculty, not IT

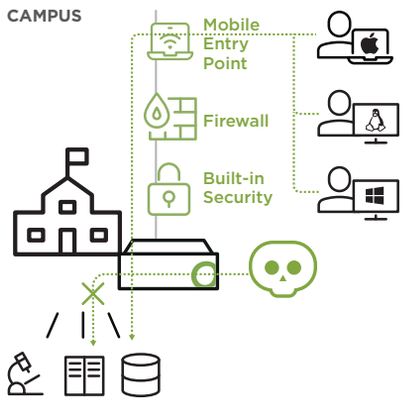
Operations means keeping things going and interconnecting the devices of students, faculty and project collaborators on and off-campus. It means dealing with a variety of applications, gadgets and instruments in lecture rooms and labs, as well as various online tools. At the same time, sensitive research and student data needs to be protected in an infrastructure that is anything but simple. In the background, there are procurement policies budget constraints to balance against the potential risks of breaches and attacks, and the damage associated with them.

IT security strategy that matches expectations and meets your needs

We enable your IT employees to collaborate with our experts to develop and maintain a strategy that covers an inhomogeneous environment, so that you can do what you know best and concentrate on the needs of students and faculty. We deliver the broad experience and services that are necessary for different devices and network participants, as well as specific expertise on how to respond to breaches and attacks. In this way, you can plan ahead to modernize ageing infrastructure and phase out existing contracts for solutions that are no longer helpful, while at the same time watching your costs.



Open Systems can support higher education by protecting sensitive research and student data and simplifying complex infrastructure



Flexible and secure architecture

Let's address higher education challenges one by one

Manage an inhomogeneous environment securely

In the dynamic environment of higher education where users are constantly evolving and changes are frequent, there is a need for clear security zones and policies, as well as defined governance. In addition to laboratory sensors, gadgets and server infrastructure with legacy applications, there are a myriad of end-user devices to deal with as part of a standard BYOD strategy. Work from home is more the norm than the exception, hence requiring adequate security concepts.

Open Systems configures and takes care of a flexible network architecture that makes frequent dynamic changes easy. Remote work is easy to configure and manage with the Mobile Entry Point (MEP) service. Our Firewall uses a zoning concept to keep important assets separate and less likely to be attacked. By using flexible policies, you can be on top of governance even for ageing parts of the infrastructure.

Challenge

Open Systems solution

1

You're in charge of connecting and managing a zoo of devices in a dynamic and distributed environment, including remote work.

1

An Open Systems **MEP client** (anyconnect) runs on all endpoints, whose monitoring and troubleshooting is done by experienced DevOps engineers. Any legacy machines or laboratory equipment that have an IP address can be included in the **MEP solution** accompanied by the Open Systems **DNS Filter.** The ZTNA concept is employed wherever possible.

2

You're responsible for ensuring that changes are made quickly so students and faculty can work and have the right type of access.

2

Open Systems engineers configure a **flexible architecture** that allows for changes and **dynamic adaptation,** e.g. network changes or automatic remote access for students via AD sync.

3

Many different security zones exist in your environment bringing about a need to separate various levels of security and trust.

3

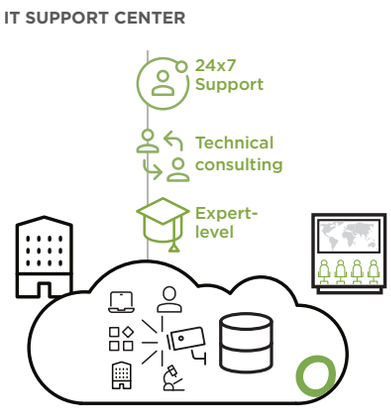
The Open Systems **Firewall** comes with a zoning concept where assets from different security zones can only communicate via certain protocols, as defined in individual firewall rules, and security zones can be shielded from each other by restricting or blocking their zone transitions. For interoperability and a manageable zone transition policy, many different network segments can be grouped into one zone of a certain security level.

4

Due to an inhomogeneous environment, different security policies have grown over the years and governance is often missing, which puts you into a constant firefighting mode.

4

Policy orchestration and **central management** for homogenous, global security policies.



Expert-level NOC and SOC

Balance available IT staff and skillsets for daily operations as well as 24x7 security

Legacy devices, such as laboratory machines, may not support web proxies – rendering them vulnerable – and their control software may also be at risk due to age. These assets need to be handled specially in the midst of an already complex networking and security picture, and, if a vulnerable device is compromised, the network must have controls to prevent the internal spread of infections.

Open Systems solutions address these challenges with a variety of integrated technologies – like a global, zone-based firewall, a DNS Filter, a Secure Web Gateway, and MDR – that means you can stay focused on your strategic objectives. All solutions come with a premium service: 24x7 expert-level support, continous technical consulting and complete lifecycle management.

Challenge

Open Systems solution

1

You are required to focus on everyday operations and end-user support, which leaves little time or resources for routine updates and trend evaluations.

1

You won't need to spend time on installing the hardware, configuring the system or organizing **regular patching** – that's all done by Open Systems engineers. **Installation** and **configuration** are designed to be clear and easy to follow.

2

Your organization does not have enough staff to legally cover 24x7 operations.

2

Open Systems Mission Control is your go-to **Network Operations Center (NOC)** and **Security Operations Center (SOC),** 24x7 worldwide.

3

Your staff needs to concentrate on operations and cannnot build up enough expertise for tasks related to security and networks, to troubleshoot both across and in-depth.

30

3

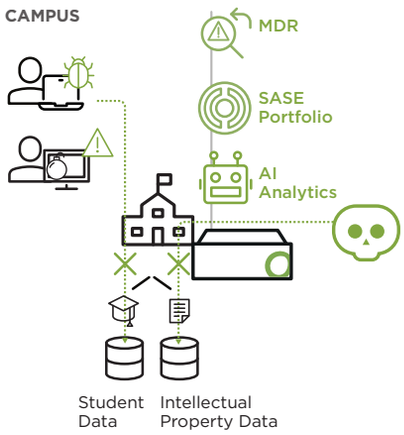
Mission Control at Open Systems has accumulated **expertise** and more than **30 years of experience** in the field, as well as dedicated Technical Account Managers and Security Analysts working with you. And being there when you need them, so that you can be there when your students and faculty need you.

4

It is difficult to hire and retain IT operations and cybersecurity staff after spending considerable effort on training them.

4

Open Systems **attracts, trains and certifies** level-3 engineers for our **Devops** NOC and SOC as well as making sure that the infrastructure to support you is kept up to date.



Managed Detection and Response

Deal with breaches and cyberattacks proactively and effectively

It's clear these days that cyberattacks are a matter of when, not if. Open Systems' MDR platform provides a best practice framework for detecting threats and it will continually evolve to keep pace with the changing nature of modern cyberattacks.

Whereas our SD-WAN protects you against external threats with built-in, best-of-breed security features, MDR covers the whole kill-chain. Our expert-level support (NOC) engineers respond to – and coordinate all actions – in the event of a security incident.

Challenge

Open Systems solution

1

Your're taking care of sensitive data with a large attack surface in spite of limited means for cybersecurity.

1

SASE (Secure Access Service Edge) protects the weakest parts of the network, while **MDR** covers the whole kill-chain to detect threats early and to shield users from ransomware and malware.

2

Standard security solutions don't work for inhomogeneous environments.

2

The holistic service portfolio of Open Systems has **built-in security** and provides a **360° view** through the cloud-native SIEM in MDR. All security solutions can be adapted and per customer alligned Scurity Analytics **tune MDR to your needs.**

3

Your already busy staff are prone to alert fatigue as there is too much digital noise in the false negatives, making it difficult to separate true risks from potential ones.

3

With standard protection, experience in setup and AI, our security services can reduce the noise and amplify the signal. Open Systems delivers **automated, proactive monitoring** that identifies most issues before they become problems. Our expert-level support is ready 24x7 to handle most responses. We fully coordinate analysis and remediation actions, and we **escalate to customers** as needed, so that you're sure of high fidelity alerts.

Transparent cost and increased ROI

Flexibly manage IT products in a multi-point life cycle while being cost aware

You have ongoing contracts for multiple IT products that expire at varying times, which makes budgeting trickier on top of the approval processes for extra security in IT.

The service packages of Open Systems are flexible so that you can align the phase-out of your older products with the phase-in of newer services and architecture, at a cost that is budgetable in advance. Benefit from a transparent, user-based pricing without hidden costs. Leverage your existing Microsoft investments with Open Systems services perfectly complementing or integrating with them.

Challenge

Open Systems solution

1

Dynamic environments keep you on your toes when it comes to budgeting correctly.

1

Open Systems offers **packages** based on which services need to be installed as well as the **number users** that need them, which can be fixed for specific periods.

2

Hidden costs, such as professional services for setup or incident case handling, result in higher expenses.

2

Open Systems Mission Control is **all inclusive:** the setup, deployment, professional services, all changes and incident tickets are part of the support fee.

3

You're struggling to manage complex life cycles of various multi-point IT solutions.

3

By using a **phased approach** in MDR, it is possible to plan more specifically and account for existing contract phase-outs as they happen.

4

It's difficult to show the value for money spent on security solutions especially, when continously new ones have to be added

4

A solution that provides peace of mind including **reports** to show what happened, where, when and what was done about it.

opensystems

Open Systems is a secure access service edge (SASE) pioneer supporting enterprises in their digital transformation journey. Our cloud-delivered Secure SD-WAN and Managed Detection and Response (MDR) services unify security and comprehensive networking capabilities, enabling organizations to connect their clouds, branches, applications and users anywhere in the world, in a secure and agile way. Open Systems' service delivery platform combines AIOps and automation with 24x7 experts to deliver immediate peace of mind and future-proof business-critical infrastructure.

Learn more at **open-systems.com** |