INDUSTRY SOLUTION BRIEF

Transform the Chemicals Industry

Answer your network challenges with Open Systems

swiss safety center ISO 27001 certified system

Open Systems services are ISO 27001 certified.

What are some of the challenges of the global chemicals industry?

Manage a complex regulatory environment

Demonstrate compliance with IT security requirements from multiple regulatory agencies

Protect valuable intellectual property

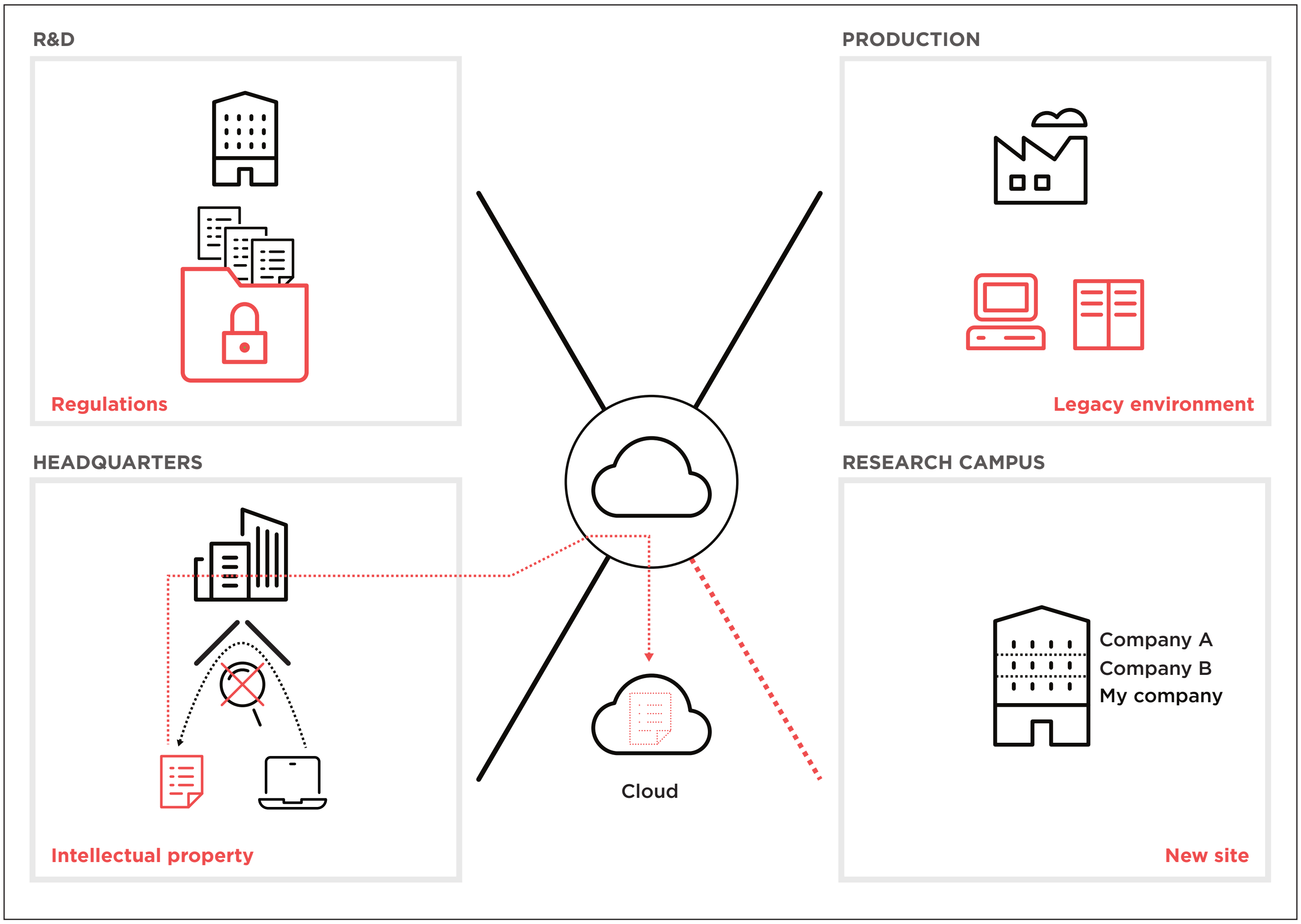
Safely control corporate intellectual property via flexible access protocols, and react quickly to any breach

Support legacy systems

Provide flexible security, continuous monitoring and manage vulnerabilities for older equipment

Integrate even difficult sites

Deliver resilient connectivity, robust network services and expertise regardless of location



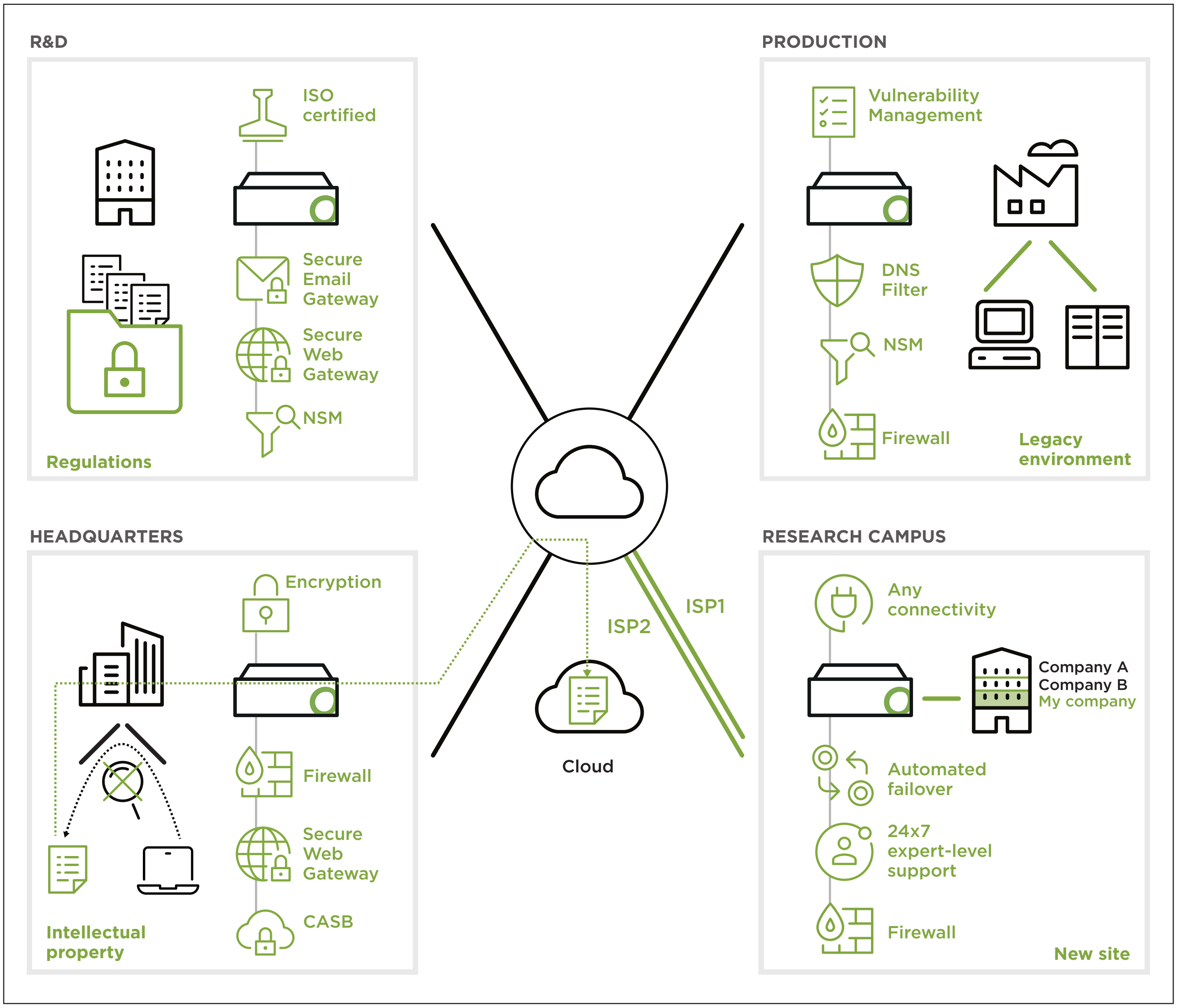
Common challenges in the global chemical industry

Chemicals enterprises require secure, resilient, and flexible networks

Large chemical manufacturers operate across the world in challenging locations and under demanding regulatory environments. They need networks that can meet requirements for connectivity as well as compliance — even as those networks also enable business innovation and acceleration. Security is always a priority, and never more so than with regard to the protection of an organization's intellectual property (IP). In addition, chemical industry networks typically support numerous legacy appliances that require special attention in the context of modern threat protection, detection and response.

Your SD-WAN is a key resource

A unified, secure network like the Open Systems Secure SD-WAN is critical to enabling chemical organizations to integrate difficult or remote sites, protect legacy systems, and deliver high levels of security not just for intellectual property, but for the organization as a whole. The built-in features and standardized deployments of our SD-WAN are also what makes possible simple and easily verifiable compliance with industry regulations.



Open Systems solutions support global chemical companies to overcome their challenges

R&D
ISO certified
Secure Email Gateway
Secure Web Gateway
NSM
Regulations

Let's address chemicals industry challenges one by one

Deliver advanced protection – and meet your regulatory obligations

With a global footprint, you need a fast, flexible, modern network to power your business. But network requirements don't end there. You need strong security protections at every level, and comprehensive solutions for threat detection and response. Moreover, you need to be able to demonstrate the security features and compliance of your network to multiple regulatory bodies.

The consistent architecture and advanced automation of the Open Systems Secure SD-WAN, combined with the 24x7 expert-level support that Open Systems provides, enables enterprises to easily meet IT regulatory requirements. Our SD-WAN protects you against external threats with built-in, best-of-breed security features, and delivers powerful threat detection and response via additional options. From a regulatory perspective, standardized setups enable global enforcement and deliver full visibility across your environment. Open Systems itself is certified and audited every year. Here are a few examples of how we deliver network protection:

Challenge

Open Systems solution

1

Like most chemical manufacturers, you must meet security requirements from CFATS and ITAR.

1

The Open Systems Secure SD-WAN features a **Next-Gen Firewall** with internal zoning so you can create a multi-tiered corporate security policy. Our **Secure Web Gateway and DNS Filter** provide protection from malicious content on the public internet, while our **Secure Email Gateway** keeps your email traffic confidential.

2

If – despite all protection mechanisms — a malware attack happens, you need a fast, comprehensive, and professional response.

2

The Open Systems **Network Security Monitoring, Endpoint Detection & Response, and Vulnerability Management** options provide network and endpoint surveillance and enable fast responses to suspicious activity.

3

As part of your compliance obligations, you must be able to show that regulations and standards are met across your organization.

3

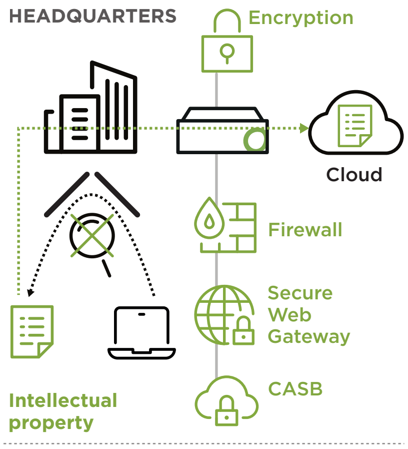
Open Systems Secure SD-WAN delivers a consistent architecture across all sites. Once the architecture is designed and agreed upon, it is enforced everywhere. Customers have full visibility and centralized control across global and local configurations.

4

Your external IT providers and partners must likewise be able to show relevant certifications.

4

Open Systems is **ISO27001 certified** and assessed annually by an independent auditor resulting in a **SOC 1 (ISAE3402/AT-C 320) report.**



Secure your critical intellectual property

Your organization's intellectual property is one of its most valuable assets. As a result, your enterprise IT needs to offer robust protections to keep that information private.

Open Systems directly addresses IP security concerns with a multi-layered, zero-trust approach, strong encryption for all traffic regardless of routing method, and a zoned, monitored environment in which you can easily control both, local access and interactions between end users and cloud-based applications and services. At the same time, in the event of a security breach, customers can rely on highly-experienced Open Systems NOC and SOC teams to provide a fast, holistic response.

Challenge

Open Systems solution

Challenge 1

You need to ensure internal communication remains private.

Solution 1

In addressing connectivity to all your sites, Open Systems adopts a zero trust strategy: all traffic, whether routed through ISP or MPLS lines, is **fully encrypted.**

Challenge 2

You have to provide strong protections for sites on shared campus facilities.

Solution 2

Our **Next-Gen Firewall** enables customers to segregate filter traffic between trusted and untrusted zones.

Challenge 3

Since cloud-based apps make up 95% of all apps, you also need protections and policies to control against data leakage on cloud applications.

Solution 3

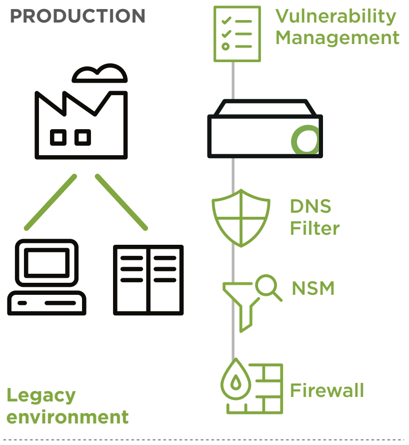
Open Systems offers a **Cloud Access Security Broker (CASB)** that can track cloud app usage and data transfers and enable customers to enforce access policies per application, per user, and per file type.

Challenge 4

In response to suspicious activity or a confirmed breach, you need a team with the experience and capabilities to respond immediately.

Solution 4

Open Systems takes a holistic approach to threat detection and response. In addition to **built-in security** on every layer of the SD-WAN and features that provide protection along the entire kill chain, our **NOC and SOC teams** are staffed by **expert-level engineers** who can coordinate and execute every stage of an intrusion response.



Provide specialized protection to your business-critical legacy environment

Older equipment and facilities that are still business-critical often require additional security measures in today's networked environment. Regardless of networking limitations, out-of-date software, or known vulnerabilities, your SD-WAN should fully support – and fully protect – your legacy sites.

Open Systems enables customers to segregate legacy facilities within the WAN via a zone-based firewall, and to protect legacy systems from external threats whether or not they support traditional protection measures. Our Vulnerability Management option secures machines running older software, while our Network Security Monitoring tracks the status of equipment for which Endpoint Detection & Response (EDR) is not always possible. Finally, our Global Threat Isolation feature can quickly disconnect legacy equipment in the event of a compromise.

Challenge

Open Systems solution

1

For added security, you should provide secure zones within the network for legacy equipment that remains business critical.

1

Our **Next-Gen Firewall** delivers internal network segmentation that enhances protection of vulnerable sites.

2

You need effective threat protection for legacy equipment that may or may not support traditional protection measures.

2

Open Systems delivers comprehensive threat protection via our **Secure Web Gateway** (for proxy-aware systems) and our **DNS Filter** (for non-proxy-aware systems).

3

With legacy equipment typically running older software, you need the ability to track and remediate vulnerabilities.

3

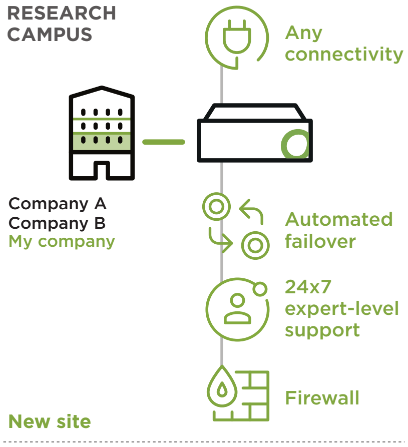
Open Systems **Vulnerability Management,** designed for hybrid IT environments, scans for and identifies vulnerabilities throughout your network — even tracking assets that can't be scanned with cloud agents.

4

Across your environment, you must continuously ensure that no legacy machine is compromised.

4

Our **Network Security Monitoring** provides real-time detection of compromised systems quickly — and enables fast and efficient analysis and response. In the event it's necessary, our **Global Threat Isolation feature** enables us to quickly disconnect a compromised machine, even with equipment that does not support EDR.



Enable connectivity at every site

Remote production sites in the chemicals industry are common; connecting them effectively is not. For new production sites or office labs on a shared campus, organizations need fast connectivity established. Likewise, for challenging locations, resilient connections are a must.

The Open Systems Secure SD-WAN is transport-agnostic, which enables us to establish site connectivity quickly. Fully automated hardware and line failovers protect uptime even in challenging locations, while automated monitoring and alerting in the event of an outage accelerates response time. Our expert-level support engineers respond to – and coordinate all actions – in the event of a security incident

Challenge

Open Systems solution

1

For new sites, you need connectivity as fast as possible, and you don't want to wait for an MPLS line to be installed.

1

Our SD-WAN runs on **any connectivity layer,** so we can establish communications quickly and easily. As better connectivity becomes available, for example once an MPLS line is installed, our **hybrid WAN** will incorporate that connection automatically.

2

You need to protect uptime, particularly at critical sites.

2

Leverage our SD-WAN to establish **fully automated hardware and line failovers** to ensure maximum protection for your communications.

3

In the event a site goes down, you must ensure an immediate, coordinated response.

3

Open Systems delivers automated **monitoring** of connectivity and services. Our **expert-level support is ready 24x7** to handle most responses. We fully coordinate analysis and remediation actions, and we **escalate to the customer** as needed.

Open Systems is a leading global provider of a secure SD-WAN that enables enterprises to grow without compromise. With assured security, AI-assisted automation and expert management that free valuable IT resources, Open Systems delivers the visibility, flexibility and control you really want with the performance, simplicity and security you absolutely need in your network.

To learn more, visit **open-systems.com** Follow us