INDUSTRY SOLUTION BRIEF

Securely accelerate your insurance services operations

Rely on comprehensive networking and security from 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 insurance industry?

Maintain an ultra-reliable network at all levels

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

Complement SD-WAN with SOCaaS

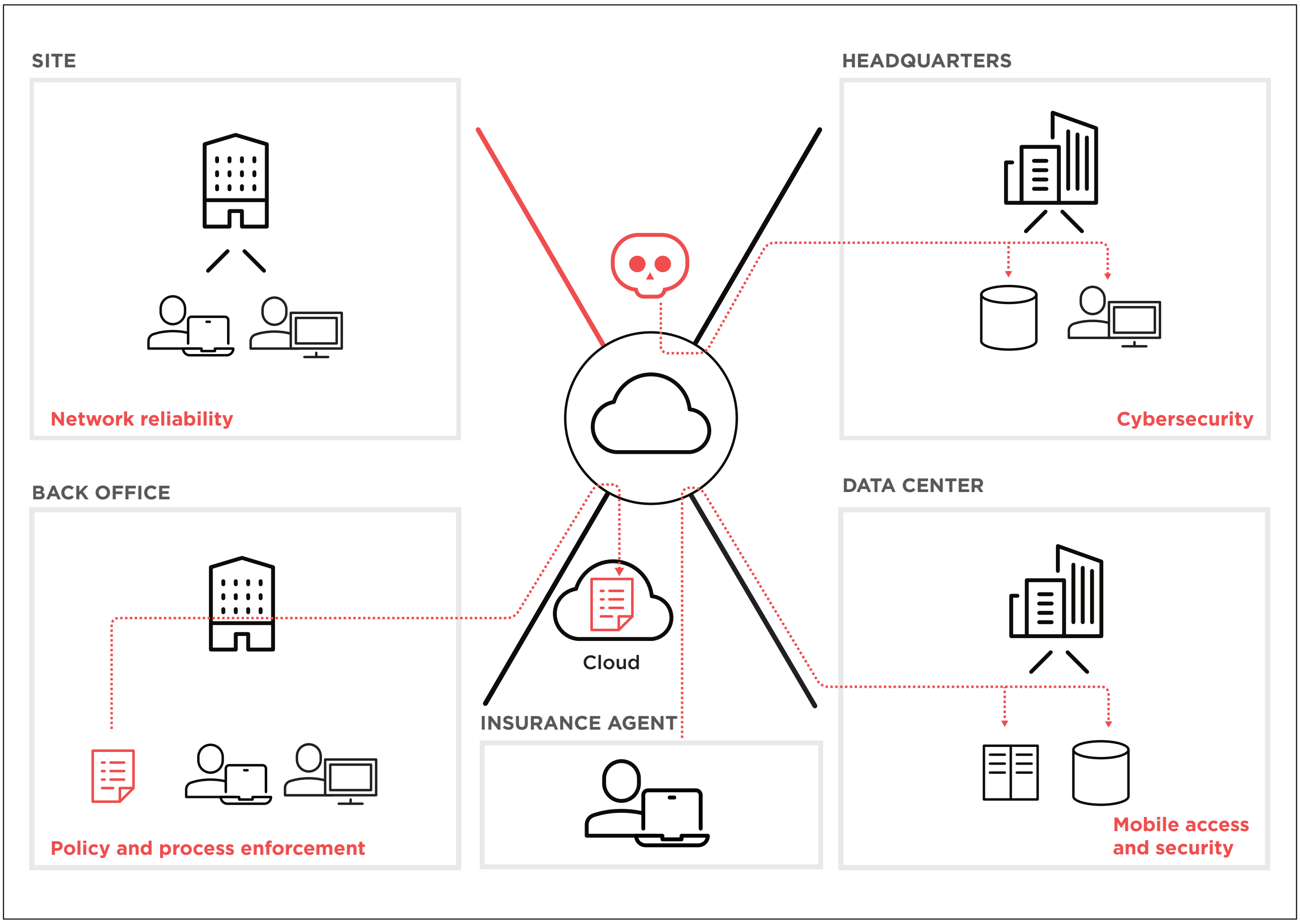
Mitigate your cybersecurity risk and protect your most valuable assets from malware, ransomware and viruses

Enable global, policy-based compliance

Deliver audit-ready enforcement processes covering browsing, application, and data usage

Extend protections to mobile users

Provide secure, seamless access for traveling or remote users and authorize access with different profiles



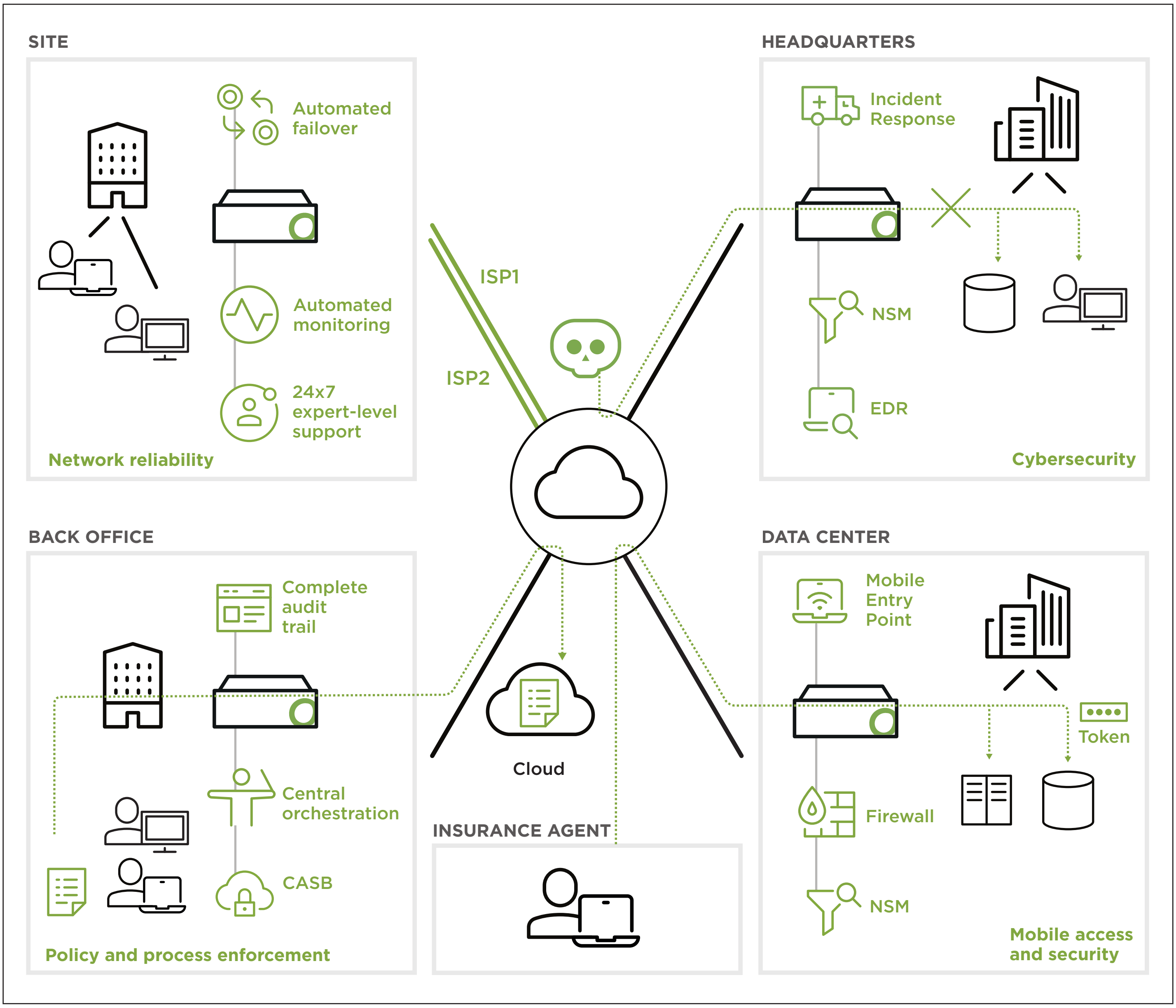
Most common pain points of insurance services companies in their IT network and security environments

Insurance firms require flexible networks with operational resilience

Large insurance companies, with operations spread across regions or continents, rely on worldwide IT networks for their operations. These enterprise networks must be able to maintain the highest levels of availability, offer 24x7 expert-level support, and deliver policy-based compliance mechanisms that are transparent and global. Moreover, insurance organizations rely on their networks to defend against the risks of phishing attacks on internal communications and domain spoofing on the internet. These requirements demand comprehensive networking and security capabilities that can deliver efficient access while protecting both end users – particularly in the context of today's mobile workforce – and the brand itself.

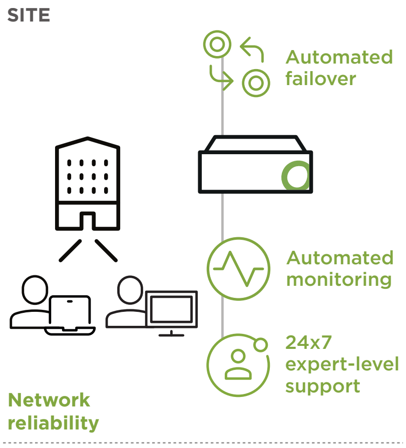
Your SD-WAN is a key resource

Given the demands on their IT, a unified, secure network like the Open Systems Secure SD-WAN can be critical to delivering the levels of protection, integration, and reliability that insurance organizations require. With a unified network, enterprises can seamlessly deliver intelligent network services to any user, along with flexible connectivity that automatically adapts to available lines. Critical operations can run securely and without interruption across a global environment, giving the back office as well as the traveling insurance agents uninterrupted and secure access to their tools. And Open Systems expert engineers provide comprehensive, 24x7 assistance every step of the way.



How Open Systems can support the insurance industry in reducing cybersecurity risks and maintaining a highly reliable network

Let’s address insurance industry challenges one by one



Ensure network reliability throughout the enterprise

All your efficiency enhancement initiatives – like robotic process automation (RPA) – don’t mean much without a highly available network on which to operate. Open Systems incorporates quality, flexibility, and reliability at every level — hardware, lines, and third-party connectivity providers — so that your uptime gets maximum protection. Better still, we deliver an expert-level, 24x7 Network Operations Center (NOC) to proactively monitor and remediate issues before they impact your business.

Challenge

Open Systems solution

1

Uptime is key. You need to deliver ironclad reliability for the enterprise.

1

Our Secure SD-WAN incorporates **high availability technologies** wherever possible and runs on any connectivity layer. For added uptime protection, Open Systems incorporates redundant flexibility to smoothly and automatically handle hardware and line failovers — and fallbacks.

2

To provide an optimal disaster response, you need resilient flexibility built into your network.

2

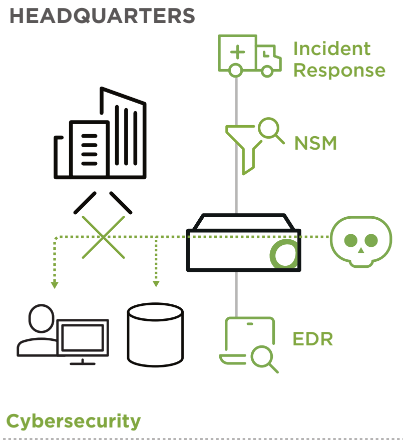
The Open Systems SD-WAN is **hybrid** by design: whether your connectivity is via internet, MPLS, or 4G doesn’t matter. Moreover, we leverage the differing connectivity offerings and technologies of numerous providers to deliver greater **flexibility** in responding to technical issues.

3

You should expect to get support whenever and wherever you need it.

3

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



Limit your cyberattack surface through built-in protection, global detection and robust processes

The insurance industry is an attractive target for cybercriminals. In case you are hit by a cyberattack, a fast, reliable and professional incident response process is inevitable to limit the damage and to follow-up properly to avoid such incidents in the future.

Enterprises today must contend for a limited attack surface by only implementing technology with built-in security. Such consistent protection in addition with a globally distributed, fine-grained threat detection network like our edge-deployed Network Security Monitoring, create a multi-layered, real-time defense of your environment.

This cyberdefense coverage can be expanded even to the end users who can be secured via our Endpoint Detection and Response (EDR).

Challenge

Open Systems solution

1

In case of a cyberattack, you must ensure fast and professional reaction to limit the damage to your enterprise.

1

Our **Incident Response** supports you with analyzing and coordinating events when hell breaks loose. Our OS-CERT team enables you to uncover the details of a breach quickly and take action. Working hand in hand with your own security organization, our globally networked experts can help you handle even large incidents.

2

You need to provide robust and reliable threat protection as well as continuous and relevant detection.

2

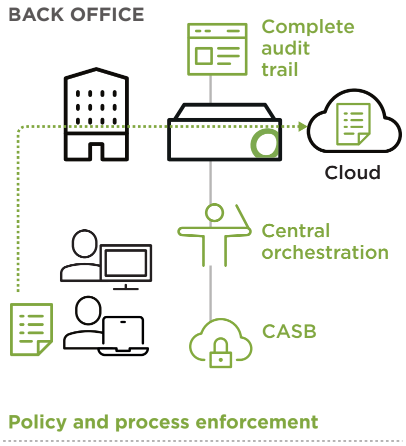
The Open Systems Secure SD-WAN with its **built-in security** functions allows consistent and effective threat protection. **Network Security Monitoring (NSM)** provides for security insights and threat detection for all devices connected to the WAN.

3

Across the whole network landscape, you must ensure consistent security and reliable detection.

3

Open Systems **Endpoint Detection and Response (EDR)** installed on all workstations and laptops enables permanent monitoring of all systems and allows detailed analysis in the case of detection.



Leverage policies and processes that seamlessly enhance your security

Every insurance enterprise has browsing, application, and data management compliance policies that are tailored to the organization's needs. Open Systems recognizes that an effective network security architecture must complement and extend existing enforcement processes while offering a transparent audit trail at every stage.

Open Systems provides effortless integration with your existing compliance architecture without creating new overhead. Our Secure SD-WAN uniquely enables organizations to apply their desired policies globally and granularly across the network — while at the same time our NOC engineers seamlessly adapt to customers' ticketing workflows. Tickets and audit trails are completely transparent and fully integrated into your existing structures.

Challenge

Open Systems solution

1

Your SD-WAN should not create additional complexity in your network and data management.

1

The Open Systems Secure SD-WAN **offers seamless integration** with an organization's existing ticketing templates and customer service desks. Deliver a streamlined workflow while avoiding reconfigurations and/or siloed management.

2

You need a reliable means of enforcing corporate communication, browsing, and application policies.

2

Leverage **simplified, centralized policy enforcement** across email (via our Secure Email Gateway), browsing (via our Secure Web Gateway), and application usage (via filtering on our Next-Gen Firewall).

3

In the cloud era, data leakage is a constant concern. To mitigate risk, you must define and enforce global application usage and data policies.

3

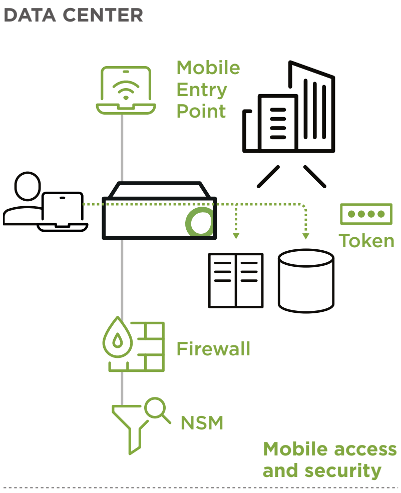
Open Systems delivers visibility across your cloud app landscape via a **Cloud Access Security Broker (CASB).** Discover and monitor cloud application usage within your network and get risk assessments of current activity. Leverage that information to enforce global policies over sanctioned and unsanctioned apps, and scan the data on API-connected cloud apps to ensure against data security violations and to protect against various strains of malware.

4

For all your security operations and management, you need full visibility and audit reporting of all actions.

4

Every blacklist/whitelist entry and every new enforcement rule in the Open Systems Secure SD-WAN is accompanied by a corresponding ticket in the web portal, and a **complete audit trail** is available.



Meet security requirements even for your mobile workforce

Insurance companies must contend for network access and security for their mobile — or fully remote — insurance agents. Mobile end users require the same seamless experience that they would have on premises, and your organization needs to maintain a consistent security posture no matter where the users are.

Open Systems delivers fast and reliable network access regardless of user location. Our Mobile Entry Point (MEP) technology provides a secure connection for every user — tailored to the user's particular access profile: firewall, web, and email protections are automatically applied for all clients according to their credentials. Likewise, end-user laptops can be secured via our Endpoint Detection and Response (EDR).

Challenge

Open Systems solution

1

On a daily basis, you must assure secure and reliable access to the enterprise WAN for traveling, remote, and mobile users.

1

Our **Mobile Entry Point** functionality delivers a secure, encrypted connection to the WAN from any location, effortlessly.

2

You must verify and secure user access across the enterprise without negatively affecting the end-user experience.

2

Open Systems Secure SD-WAN provides for **universal access profiles** that correspond to specific security measures applied via the Firewall (for instance, additional subnets available only to users who've used two-factor authentication) and via the **Secure Web Gateway** (which, as an example, may limit browsing access or cloud application availability).

3

Across every corporate device, you must ensure consistent security and reliable service.

3

Open Systems **EDR** installed on all workstations and laptops enables permanent monitoring of the system. For all mobile devices, **Network Security Monitoring (NSM)** provides security insights when devices are connected to the WAN via MEP.

Contact your Open Systems representative to find out how our Secure SD-WAN can power your global operations.

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

Open Systems proprietary 2019