



**INDUSTRY
SOLUTION BRIEF**

Leverage strong protections against attacks and downtime

Secure your network, your end users,
and your brand with Open Systems



Open Systems
services are
ISO 27001 certified.

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



Minimize the risk of phishing or spoofing attacks

Shield internal users, external clients, and the brand from all-too-common phishing attacks



Complement your SD-WAN with SOCaaS

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



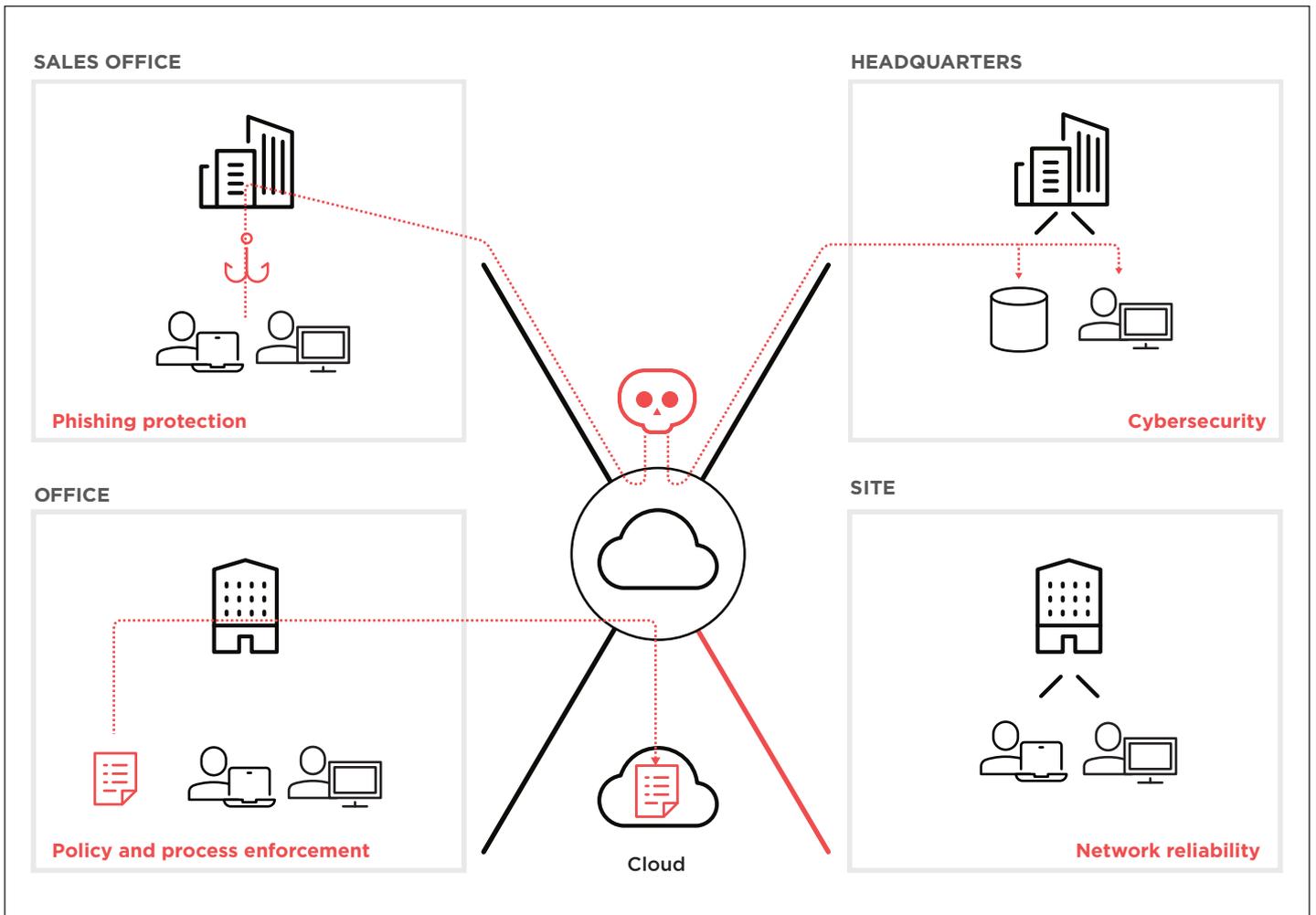
Enable global, policy-based compliance

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



Maintain an ultra-reliable network at all levels

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



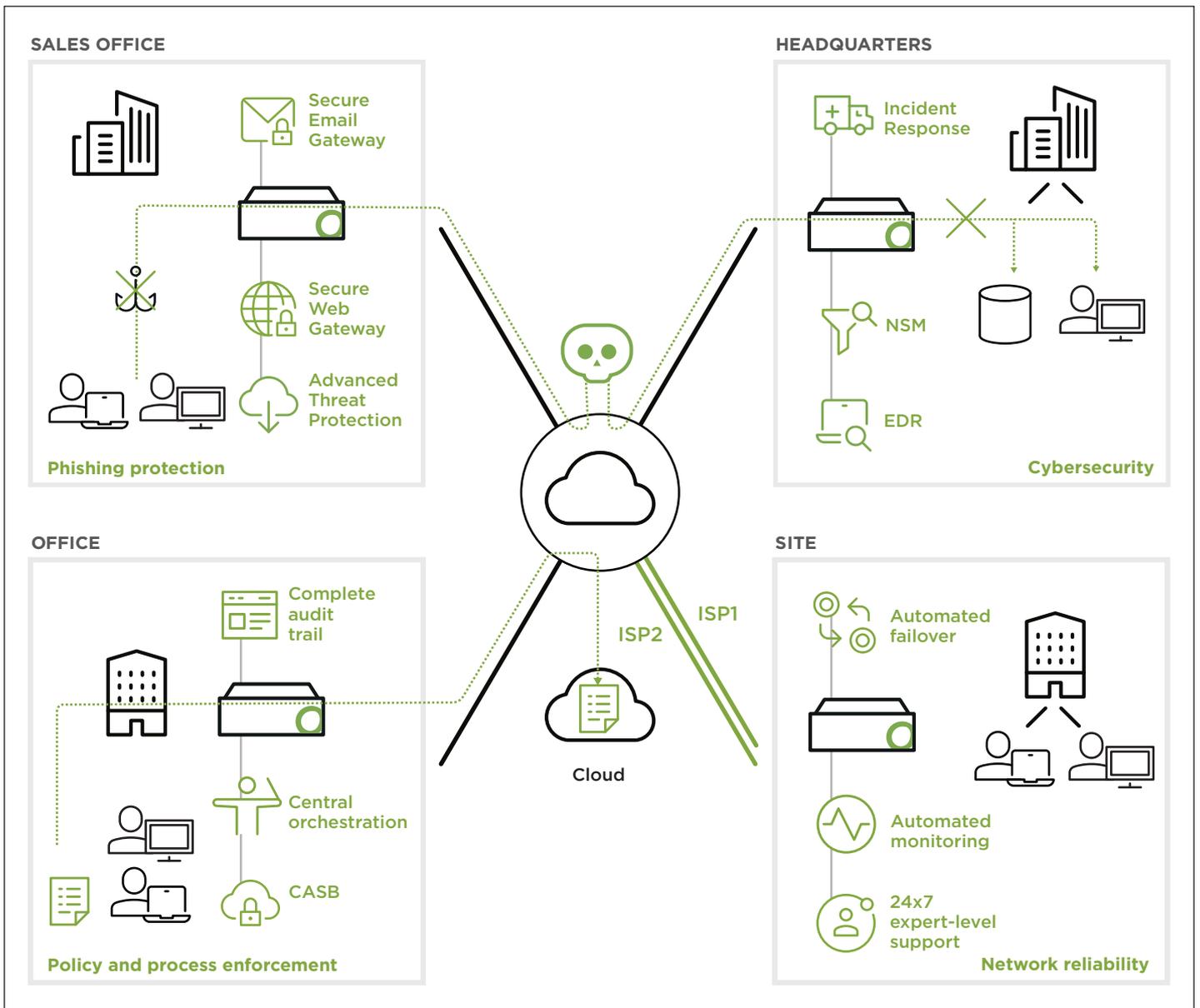
Most common pain points of financial services companies in their IT network and security environments

Financial services firms must focus on network defenses

Large financial services companies, with operations spread across regions or continents, present especially appealing targets for cyberattacks. Whether from phishing attacks on internal communications or domain spoofing on the internet, financial organizations must defend themselves with network capabilities that provide efficient access while protecting both end users – particularly in the context of today’s mobile workforce – and the brand itself. These enterprise networks must be able to maintain the highest levels of availability, offer 24x7 expert-level support, and deliver policy-based enforcement mechanisms that are transparent and global.

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 financial services organizations require. With a unified network, enterprises can seamlessly deliver intelligent network services, along with flexible connectivity that automatically adapts to available lines and increases efficiency, e.g. by enabling their robotic process automation (RPA). Critical operations can run securely and without interruption across a global environment. And Open Systems expert engineers provide comprehensive, 24x7 assistance every step of the way.



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

Let's address financial services challenges one by one



Protect users — and secure your brand reputation

In the business of continuously moving money, financial services organizations are popular — and lucrative — targets of phishing attacks. This represents a threat on two fronts: not just the potential for financial loss with an attack that diverts a delivery of funds, but the possibility of reputational damage to the brand from cyberattackers successfully masquerading as enterprise representatives. Organizations with a global footprint and a large number of connected users therefore need strong security protections at every level, and comprehensive solutions for threat detection and response.

The Open Systems SD-WAN protects against external threats from an integrated, 24x7 Operations Center that combines expert analysis with built-in, best-of-breed SD-WAN security features. These include unique phishing protection from the combined functionality of our Secure Email Gateway and our Secure Web Gateway, which can be enhanced with Advanced Threat Protection feeds, and the deep analytics and reporting of our built-in DKIM/DMARC features.

Here are a few examples of how we deliver protection to both users and brand.

Challenge

Open Systems solution

1

You must meet the dual challenges of phishing and spoofing attacks, particularly for your most valued customers.



The Open Systems Secure SD-WAN offers powerful threat protection from the dual filtering functions of our **Secure Email Gateway** and our **Secure Web Gateway**, which together deliver visibility, enforcement, and deep analysis across users' communications and browsing activity.

2

With attacks growing in sophistication, you need the additional security of real-time intelligence on current threats.



Significantly boost your protection with our **Advanced Threat Protection** option, which delivers zero-day and **phishing threat intelligence** to our Secure Email Gateway and our Secure Web Gateway defenses.

3

To protect the brand, you need strong protections against domain spoofing and brand hijacking.



Effective brand protection requires robust enforcement from **Domain-based Message Authentication Reporting and Conformance (DMARC)**. However, these solutions are often complex and difficult to implement. Open Systems makes it simple: our DMARC protection is built-in to our Secure Email Gateway, delivering extensive analytics and reporting to enhance brand protection.

HEADQUARTERS



Cybersecurity

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

Cybercrime happens where the money is. That's why the finance industry is one of the most frequent target of cyberattacks. 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.



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 robust and reliable threat protection as well as continuous and relevant detection.



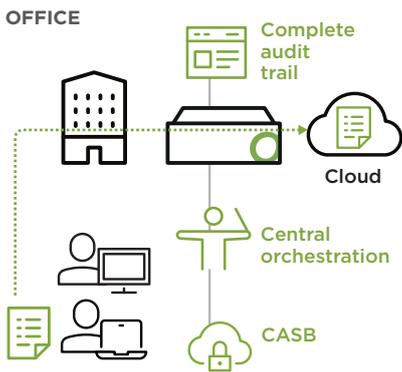
The Open Systems Secure SD-WAN with its **built-in security functions** allows consistent and effective threat protection. **Network Security Monitoring (NSM)** provides for security insights and threat detection for all devices connected to the WAN.

3

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



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.



Policy and process enforcement

Leverage policies and processes that seamlessly enhance your security

Every financial services 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.



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.



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.



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.

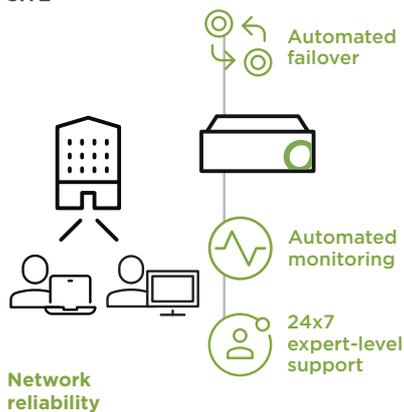
4

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



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.

SITE



Ensure network reliability throughout the enterprise

The most effective security measures or efficiency enhancements, like 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.



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.



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.



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.

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.