SCION ASSOCIATION

SIX

eraneos

ANAPAYA The SCION Company

WHITE PAPER

COST SAVINGS AND BUSINESS BENEFITS OF SCION

Based on a use-case-centric analysis, this white paper shows how SCION delivers high ROI and is more cost-effective compared to other enterprise connectivity solutions such as MPLS and SD-WANs while offering strategic and business advantages.

ABOUT THIS PAPER

This content has been produced by a coalition of organizations deploying SCION in different capacities, bringing together a 360° perspective grounded in factual, data-driven insights. The coalition is led by the SCION Association, a non-profit organization responsible for maintaining and promoting the SCION technology, together with SIX, an initiator of the first industrial-grade SCION application (SSFN); Eraneos, a consulting firm with expertise in SCION; and Anapaya, a commercial provider of SCION technology.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

SCION Internet architecture combines the security of private networks with the flexibility of the Internet. What this paper demonstrates is that across Enterprise WAN and secure remote access use cases, SCION can, in the scenarios assessed in this paper, offer a more cost-efficient connectivity model than traditional network architectures, while delivering improvements in cyber resilience, provider diversity, and regulatory alignment.

FINANCIAL BENEFITS

USE CASE	COST REDUCTION [%]	ROI [%]	PAYBACK TIME
SCION vs leased lines	91	2389	<1 month
SCION vs MPLS	81	1110	<1 month
SCION vs SD-WAN	32.6	228	<4 months
SCION GATE by Anapaya for remote access	N/A	71.6	9 months

STRATEGIC BENEFITS

- Compliance & regulation: Where NIS2 and DORA impose compliance obligations, SCION can strengthen the technical control environment by improving path transparency, governance, and resilience-related network controls.
- Optionality and sovereignty: Multi-provider architecture reduces concentration risk and increases control at the network layer.
- Third-party risk management: Visibility and control over the entire value chain at the routing level.

OPERATIONAL BENEFITS

- Cybersecurity: Reduced attack surface lowers exposure to cyberattacks.
- Cyber-resilience: Multi-provider architecture that eliminates concentration risk and improves availability.
- Infrastructure sovereignty: Path control enables visibility and choice at the network layer.
- Network governance: Strict control at the network layer for improved visibility across third parties.

INTRODUCTION

Topics once considered purely IT such as AI, cyberattacks, cloud hyperscalers, supply-chain dependencies, compliance, quantum computing, and others have become regular items on boardroom agendas across organizations - a trend that peaked in 2025 but one that had been escalating for years.

In this context, business leaders are required to rethink their approach to IT, not as a purely functional domain, but as a strategic capability that directly impacts resilience, risk exposure, and long-term competitiveness.

The Internet sits at the center of this turning point, enabling connectivity across global ecosystems spanning finance, healthcare, energy, defense, and government. Yet many of today's Internet-based connectivity solutions struggle to meet the growing requirements for security, reliability, sovereignty, and provider optionality.

SCION introduces a fundamentally different approach to connectivity, one designed to address core challenges faced by business leaders, from regulatory compliance and cyber resilience to concentration risk and digital sovereignty.

At the same time, innovation, even when validated through real-world deployments, must be substantiated not only by clear technical and business advantages over alternative solutions, but also by a credible and transparent cost rationale. The economic value of innovation emerges only in comparison: against the cost of achieving similar outcomes through traditional solutions, or against the financial and systemic consequences of leaving cyber threats unaddressed. The relevant benchmark is therefore not today's spending level, but the cost and risk profile of the available alternatives.

This white paper examines SCION through a use-case-driven analysis of cost, return on investment, and strategic characteristics, providing decision-makers with a structured framework to assess its economic and operational impact.

For an explanation of the terminology used in this white paper, please refer to the Glossary in the Appendix.

ABOUT SCION TECHNOLOGY

As an increasing share of our economic and societal systems now operates in the digital space and relies on Internet connectivity, the need for solutions that can better protect against cyberattacks with potentially severe financial and reputational consequences has become critical.

This need is further amplified by the growing weaponization of dependencies and vulnerabilities in IT infrastructures within international tensions. Never before has this challenge been more pressing, as business systems increasingly intersect with services essential to society.

The biggest issue with today's Internet lies in the fact that its attack surface is massive: every user, application, and connected device can become an entry point into a system. Reducing that surface must be a priority for critical infrastructure operators and business leaders alike as they increasingly become targets of national security-level attacks, all the while ensuring a diverse IT supply chain. In fact, we see an IT solution landscape dominated by just a few providers that is creating concentration risk and sovereignty concerns for businesses and critical infrastructure operators.

KEY LIMITATIONS OF TRADITIONAL CYBERSECURITY SOLUTIONS

Typically, businesses rely on private lines like MPLS to minimize cyber threat exposure and control network paths, but private circuits are costly and inflexible when large ecosystems or many third parties must be connected.

Many businesses therefore turn to the public Internet combined with an encryption overlay (e.g. SASE/ SD-WAN). Yet even with these solutions, Internet-based communication remains exposed to cyberattacks, especially as AI accelerates the exploitation of zero-day vulnerabilities from months to days, with increasing impact on perimeter devices, such as firewalls and VPN hubs. In addition, the lack of control over data paths results in traffic potentially routing through congested paths, untrusted jurisdictions, or single points of failure, challenging the overall resilience of the business.

Ultimately, both MPLS lines and SD-WAN solutions are typically provided by a single operator or vendor, creating a supply chain risk and potentially a single point of failure. This impacts the cyber resilience of the business.

For remote access to business applications or websites, organizations leverage commercial solutions whose endpoints are exposed on the Internet. However, several of such endpoints are affected by zero-day vulnerabilities, now accelerated by AI, threatening perimeter security and impacting organizations' business continuity.

In terms of business continuity, across all of these solutions, businesses lack redundancy in their IT supply chains because they have no real choice when selecting IT suppliers. This creates single points of failure, jeopardizing cyber resilience. Optionality entails having a more diverse IT supply chain to naturally help address the concentration risk that stems from relying on a handful of large IT providers.

SCION provides a combination of properties that is difficult to achieve simultaneously in conventional enterprise connectivity models: it brings the security and control of private lines together with the openness and flexibility of the Internet - all the while providing optionality at the network layer.

SCION @ A GLANCE

A SCION network, technically defined as an Isolation Domain (ISD), is built by a federation of telcos, within a trust environment, to guarantee resilience and security.

SCION networks not only operate under defined routing rules that allow operators control over the paths their data travels over. They also constitute a contractual and technical boundary, substantiated by strict governance with defined criteria on who is admitted to the network and who can exchange data with whom.

The responsibility to assign these rules lies with the creator of the ISD. This architectural conceptualization translates into an IT infrastructure that is private, with strict control – ultimately, the IT infrastructure is not on the "open Internet."

Each SCION network is multi-provider, which means it is made of various ISPs. ISPs can be part of multiple ISDs by leveraging the same hardware and software infrastructure, and thus offset the initial investment.

For a more technical overview of SCION, you can explore the resources listed in the Appendix of this paper.

USE CASES FOR SCION WITH COST AND BENEFIT ANALYSIS

SCION-based networks are well suited to replace traditional network designs, particularly in ecosystem environments that connect multiple stakeholders, or to complement existing solutions when it comes to publicly accessible critical services, such as remote access. In this section, we examine two common deployment scenarios and their associated network architectures, with a focus on cost implications and operational considerations.

The cost and benefit analysis of these use cases, while based on real-life examples (which have been standardized and anonymized), should not be interpreted as a fixed model. Prices are estimations based on current prices of Swiss providers. Pricing and data may vary depending on the specific provider, geographic region, network design, and enterprise setup.

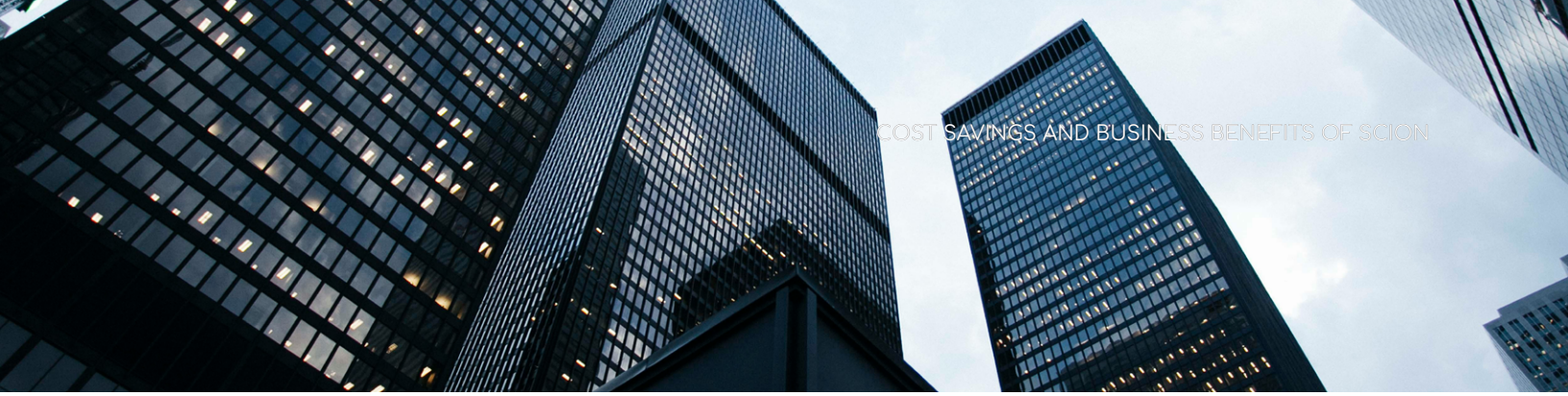
THE USE CASES WE WILL EXPLORE:

1. Enterprise WAN connectivity

- High availability WAN: Streamlined connectivity across a limited number of locations, such as data centers, administrative sites, or production environments, including multi-party ecosystems.
- Networking of the branch network: Centralized connectivity for large and more complex ecosystems, such as a headquarters or a primary data center.

2. Secure applications and services for remote access

- Protected services for home offices, field operations, IoT devices, and public websites.



1. USE CASE: ENTERPRISE WAN CONNECTIVITY

1.1 SCENARIO: HIGH AVAILABILITY WAN

In this use case, different office locations must be maximally available and securely connected to each other. These can be, for example, locations of blue light organizations, production sites with high interconnection or several office buildings of a service company.

Traditionally, redundant leased lines are used for this purpose: dedicated point-to-point connection via a provider's fiber-optic network. Alternatively, for minimally lower requirements, MPLS networks or SD-WAN can be used.

In this use case, we compare this traditional setup with a comparable SCION setup that offers similar availability and security properties.

SCENARIO DEFINITION

The enterprise network we will analyze consists of a headquarters and six remote locations. For all solutions under evaluation, the prices are based on recent price indications from Swiss providers. Numbers have been rounded for clarity.

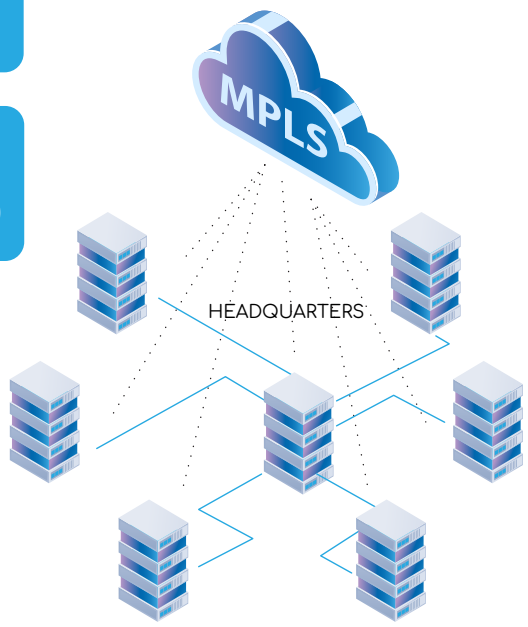
SOLUTION 1: TRADITIONAL SETUP WITH POINT-TO-POINT LEASED LINES (P2P) AND BACKUP MPLS

SETUP OVERVIEW AND ASSUMPTIONS

- Primary connections: 6 dedicated P2P leased lines with 1 Gbps / 1Gbps bandwidth and 99.99% with 24/7 support SLA
- Secondary (redundancy) connections: 7 MPLS connections with 1 Gbps / 1Gbps bandwidth and 99.99% with 24/7 support SLA

MONTHLY COST
CHF 123,700

ANNUAL COST
CHF 1,484,000



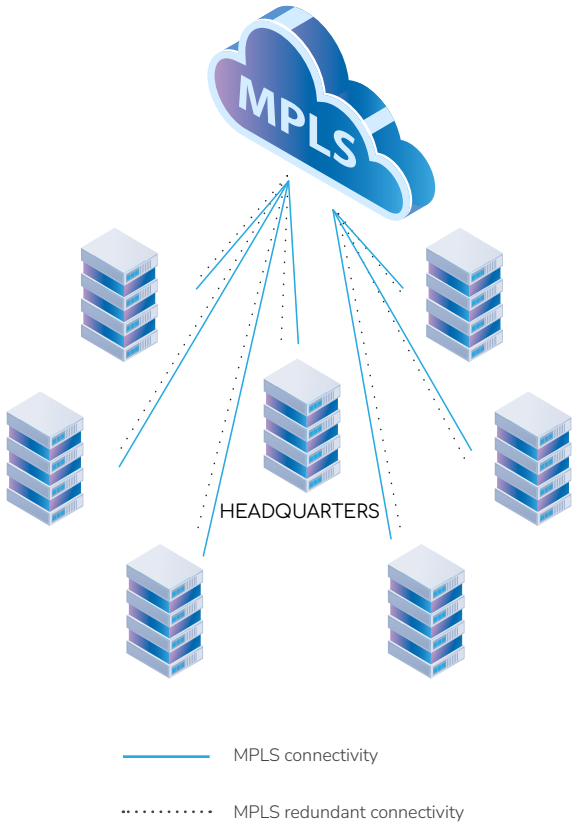
COST ANALYSIS

LEASED LINE ITEMS	QUANTITY	UNIT PRICE PER MONTH [k CHF]	TOTAL PER MONTH [k CHF]	TOTAL PER YEAR [k CHF]
Dedicated point-to-point leased lines	6	14.9	89.4	1.072
Second redundant connection (MPLS)	7	4.9	34.3	411.6
TOTAL			123.7	1.484

SOLUTION 2: TRADITIONAL SETUP WITH REDUNDANT MPLS

SETUP OVERVIEW AND ASSUMPTIONS

- Primary connections: 7 MPLS connections with 1 Gbps / 1 Gbps bandwidth and 99.99% with 24/7 support SLA
- Secondary (redundancy) connections: 7 MPLS connections with 1 Gbps / 1 Gbps bandwidth and 99.99% with 24/7 support SLA



MONTHLY COST
CHF 61,600

ANNUAL COST
CHF 739,200

COST ANALYSIS

MPLS	QUANTITY	UNIT PRICE PER MONTH [k CHF]	TOTAL PER MONTH [k CHF]	TOTAL PER YEAR [k CHF]
WAN	14 (2 redundant lines per site)	4.4*	61.6	739.2
TOTAL			61.6	739.2

*Compared to the MPLS line in solution 1, the monthly cost in this case is lower as often a line in a package of two redundant lines is priced lower than a single MPLS line.

SOLUTION 3: NEW SETUP WITH REDUNDANT SCION

SETUP OVERVIEW AND ASSUMPTIONS

- Primary connections: 7 SCION connections with 1 Gbps / 1 Gbps bandwidth and 99.99% with 24/7 support SLA , including managed EDGE device.
- Secondary (redundancy) connections: 7 SCION connections with 1 Gbps / 1 Gbps bandwidth and 99.99% with 24/7 support SLA, including managed EDGE device.
- No specific isolation domain (ISD) is created but the endpoints are connected on the public Swiss isolation domain.
- To ensure privacy among the participants, an overlay encryption is implemented.

MONTHLY COST	ANNUAL COST	INITIAL COST
CHF 11,600	CHF 139,500	CHF 54,000

COST ANALYSIS

SCION	QUANTITY	UNIT PRICE PER MONTH [k CHF]	TOTAL PER MONTH [k CHF]	TOTAL PER YEAR [k CHF]
SCION connection (with redundant lines)	14	0.235	3.3	39.5
SCION managed EDGE	14 (2 redundant lines per site)	0.500	7	84
Shared ISD / Core Fee	7	0.190	1.33	16
TOTAL			11.63	139.5

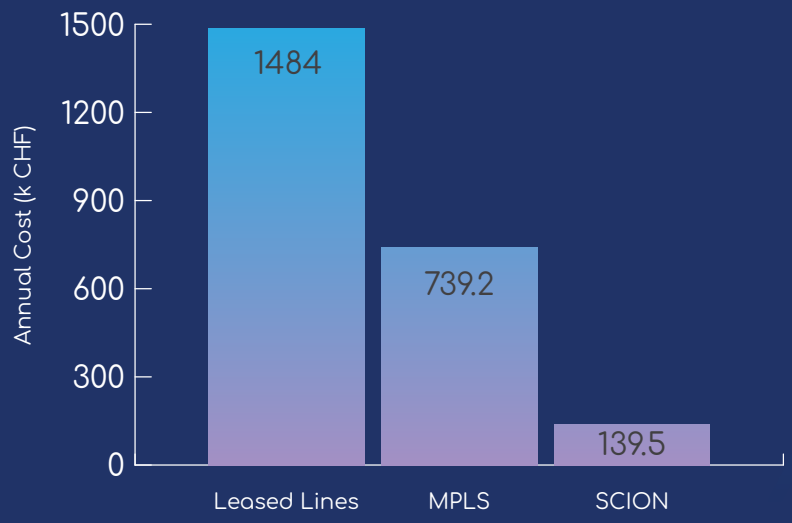
INITIAL INVESTMENT COST

In addition to the above cost analysis, setting up a SCION-based network involves one-time project costs for installing the infrastructure, changing network configurations, testing, and migration. This includes costs for both the central IT department and on-site installation. Switching to SCION may also involve project management efforts or the execution of procurement processes. As traditional setups also require regular contract renewals or technology upgrades, those efforts are not considered in the following analysis.

SCION	QUANTITY	PRICE PER SITE [k CHF]	PROJECT COSTS [k CHF]
Configuration / Testing / Migration			40
On-Site Installation	7	2	14
TOTAL ONE-TIME			54

KEY FINDINGS: HIGH AVAILABILITY WAN

ANNUAL COST COMPARISON



SCION VS LEASED LINES

- 91% reduction of annual costs
- CHF 112k monthly cost savings
- CHF 1.34M annual cost savings
- 2389 % ROI
- Payback < 1 month

Replacing leased lines with SCION can reduce connectivity costs by 91%, saving approximately CHF 1.3M per year.

SCION VS MPLS

- 81% reduction of annual costs
- CHF 50k monthly cost savings
- CHF 600k annual cost savings
- 1110% ROI
- Payback < 1 month

By replacing MPLS with SCION, organizations can cut connectivity costs by over 80% while saving roughly CHF 600k annually.

Calculation details for ROI and payback time are available in the Appendix.

1.2 SCENARIO: NETWORKING OF THE BRANCH NETWORK

This use case addresses organizations operating large, complex enterprise environments – such as banks with multiple branches, retailers, or manufacturing facilities – with global headquarters, primary data centers, and interconnected business units, often spanning multiple regions and administrative domains.

While this specific scenario only considers locations within Switzerland, a similar deployment could also be realized across a global footprint.

SCENARIO DEFINITION

In addition to its headquarters, a nationwide company operates a service center, a data center, and sites of various sizes. All sites are connected to the data center. Availability requirements depend on the size of the site.

Traditionally, the central sites are connected via highly available networks. Sites are connected through classic Internet connections (e.g. FTTH) with additional SLAs.

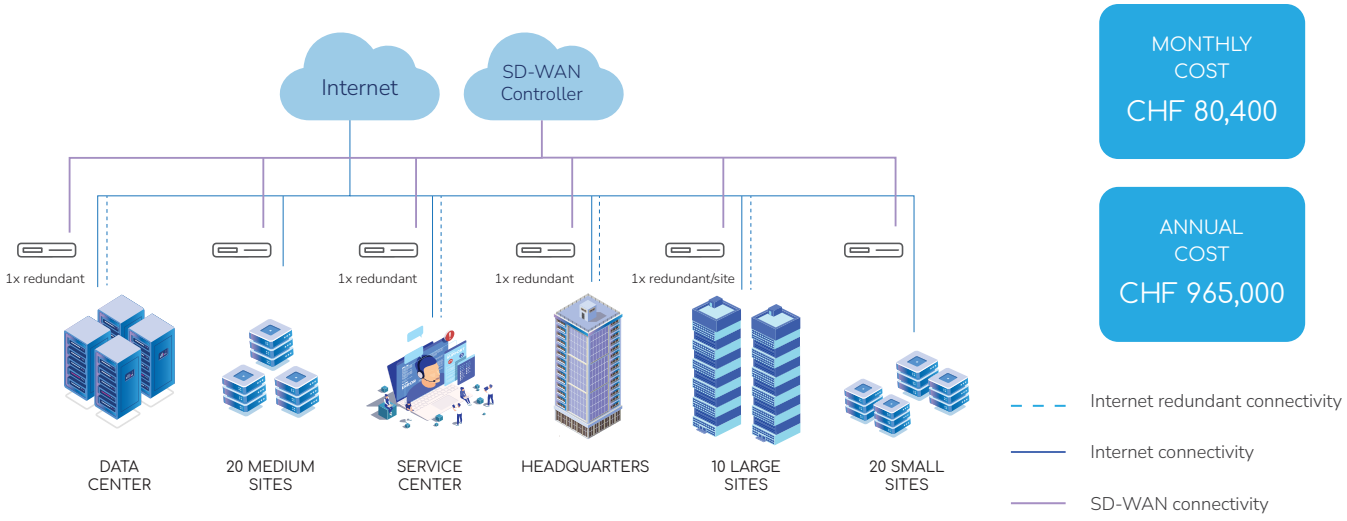
In this scenario, the enterprise network consists of 1 central site (headquarters) and 1 central service center, 1 central data center, 10 large sites (20-50 employees), 20 medium sites (10-20 employees), and 20 small external sites (3-10 employees).

For all examples, the prices are based on recent price indications from Swiss providers. Numbers have been rounded for clarity.

SOLUTION 1: TRADITIONAL SETUP WITH SD-WAN

SETUP OVERVIEW AND ASSUMPTIONS

- 1 central site (headquarters) and 1 central service centre
  4 connections including redundancy with 1 Gbps/ 1Gbps bandwidth and 99.99% with 24/7 support SLA
- 1 central data center
  2 connections including redundancy with 1 Gbps/ 1Gbps bandwidth and 99.99% with 24/7 support SLA
- 10 large sites (20-50 employees)
  20 connections including redundancy with 1 Gbps/ 1Gbps bandwidth and 99.99% with 24/7 support SLA
- 20 medium sites (10-20 employees)
  20 connections with 200/100 Mbps bandwidth and 98.9% with 10/6 support SLA
- 20 small external sites (3-10 employees)
  20 connections with 200/100 Mbps bandwidth and 98.9% with 10/5 support SLA



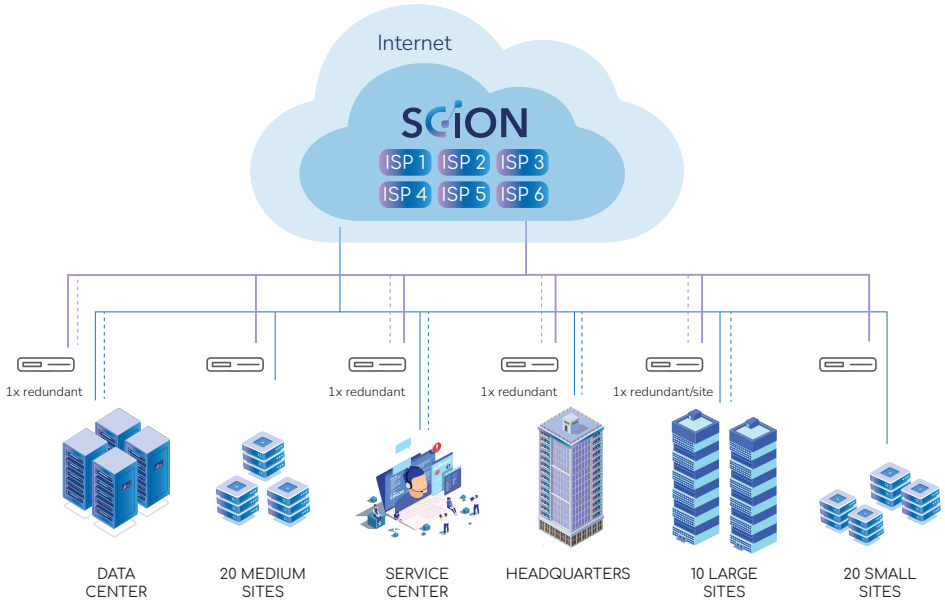
COST ANALYSIS

SD-WAN ON THE INTERNET	QUANTITY	UNIT PRICE PER MONTH [k CHF]	TOTAL PER MONTH [k CHF]	TOTAL PER YEAR [k CHF]
Headquarters / Service Center	4 (redundancy 2 lines per site)	4.2	17	204
Data Center Dedicated business Internet	2 (redundancy 2 lines per site)	4.2	8.5	102
Large sites	20 (redundancy 2 lines per site)	2.1	42	504
Medium sites	20	0.175	3.5	42
Smaller sites	20	0.125	2.5	30
SD-WAN Appliances including encryption	66	0.105	6.9	83.1
TOTAL			80.4	965

SOLUTION 2: NEW SETUP WITH SCION

SETUP OVERVIEW AND ASSUMPTIONS

- 1 central site (headquarters) and 1 central service centre
  4 SCION connections including redundancy with 1 Gbps / 1 Gbps bandwidth and 99.99% with 24/7 support SLA, including managed EDGE devices.
- 1 central data center
  2 SCION connections including redundancy with 1 Gbps / 1 Gbps bandwidth and 99.99% with 24/7 support SLA, including managed EDGE devices.
- 10 large sites (20-50 employees)
  20 SCION connections including redundancy with 1 Gbps/ 1Gbps bandwidth and 99.99% with 24/7 support SLA
- 20 medium sites (10-20 employees)
  20 SCION connections with 200/100 Mbps bandwidth and 98.9% with 10/6 support SLA
- 20 small external sites (3-10 employees)
  20 SCION connections with 200/100 Mbps bandwidth and 98.9% with 10/5 support SLA
- All sites include managed EDGE devices.
- No specific isolation domain (ISD) is created but the endpoints are connected on the public Swiss isolation domain.
- To ensure privacy among the participants, an overlay encryption is implemented.



MONTHLY COST	ANNUAL COST	INITIAL COST
CHF 54,100	CHF 650,000	CHF 96,000

COST ANALYSIS

SCION	QUANTITY	UNIT PRICE PER MONTH [k CHF]	TOTAL PER MONTH [k CHF]	TOTAL PER YEAR [k CHF]
SCION connection (with redundant lines)	26	0.235	6.11	73
SCION connection	40	0.125	5	60
SCION EDGE (with redundant lines)	66	0.500	33	396
Shared ISD / Core Fee	53	0.190	10.07	121
TOTAL			54.18	650

INITIAL INVESTMENT COST

In addition to the above cost analysis, setting up a SCION based network involves some project costs for installing the infrastructure, changing network configurations, testing and migration. This involves both costs for the central IT department as well as on-site installation. Switching to SCION might involve project management efforts or execution of procurement processes. As traditional setups also require regular contract renewals or technology upgrades, those efforts are not considered in the following analysis.

SCION	QUANTITY	PRICE PER SITE [k CHF]	PROJECT COSTS [k CHF]
Configuration / Testing / Migration			40
On-Site Installation Simple	50	1	50
On-Site Installation Complex	3	2	6
TOTAL ONE-TIME			96

KEY FINDINGS: NETWORKING OF THE BRANCH NETWORK

ANNUAL COST COMPARISON

SCION VS SD-WAN

32.6%	CHF 26.3k	CHF 315k	228%	< 4 months
reduction of annual costs	monthly savings	annual cost savings	ROI	payback time

Replacing SD-WAN with SCION reduces connectivity costs by CHF 315k annually, delivering a 32.6% reduction in annual costs, and a payback period of approximately 4 months.

Calculation details for ROI and payback time are available in the Appendix.

SCION IN ACTION: THE SECURE SWISS FINANCE NETWORK

The Secure Swiss Finance Network (SSFN) is a SCION-based communication infrastructure for the Swiss financial sector. Launched by the Swiss National Bank and SIX, it replaced the end-of-life Finance IPNet.

The SSFN is a closed network (known as an Isolation Domain) where participants are granted access only after obtaining the appropriate SCION certificate based on established governance rules.

LEGACY NETWORK CHALLENGES

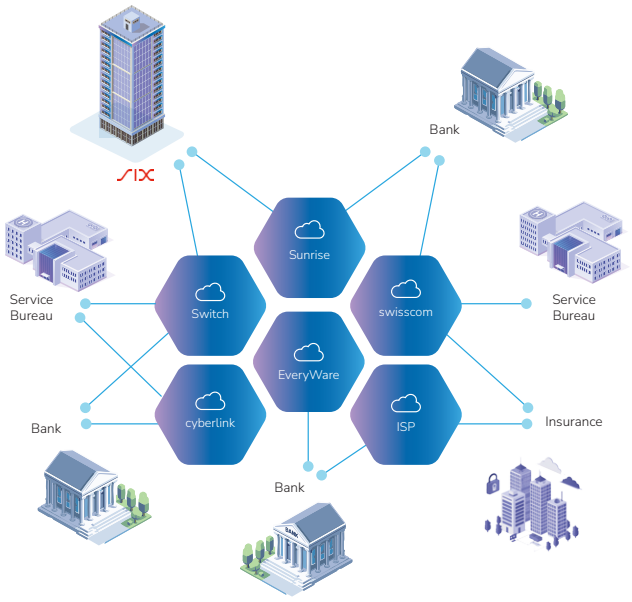
- The legacy network, based on leased and MPLS lines, was inflexible, offering limited connectivity to SIX instead of the desired any-to-any communication among connected organizations.
- The new network solution needed to be multi-provider and serve multiple customers, avoiding single points of failure with clear governance.

SIX customers and the Swiss financial community asked more and more for Internet-based service delivery. To fulfill this need, a thorough analysis and comparison of different technologies were conducted to replace Finance IPNet, including the consideration of modernizing the existing MPLS. SD-WAN was discussed but deemed unsuitable for a multi-provider, multi-customer market. SCION met the necessary requirements and was chosen due to its flexibility and adaptability to multi-party networks, making it suitable for the SSFN initiative.

KEY BENEFITS OF THE SSFN INCLUDE:

- Increased resilience with multi-provider setup
- Fast-failover feature for time-critical services
- Strong governance with clear rules
- Data sovereignty with path control
- Any-to-Any connectivity for all parties connected

Since its inception, SSFN has proven to be a robust and reliable network. Operating without glitches, it continues to support the evolving needs of the Swiss financial industry. Looking ahead, SSFN will keep adapting to emerging trends.



Read more about the Secure Swiss Finance Network here.

"With SCION, we have achieved the desired resilience against cyberattacks."
William Boye, Head of Network Services, Swiss National Bank

2. USE CASE: SECURE APPLICATIONS AND SERVICES FOR REMOTE ACCESS

This use case focuses on organizations that provide publicly accessible, business-critical services to users, devices, or systems outside their network perimeter such as eBanking platforms, insurance applications, e-Commerce, and more. These services often include employee remote access, field operations, IoT deployments, customer-facing applications, and public websites.

Due to the massive attack surface of the Internet on which these systems operate, the risk of cyberattacks is correspondingly high. With AI-accelerated attacks now exploiting zero-day vulnerabilities in days rather than months, securing these applications has become critical. In addition, reliance on single providers for security solutions introduces further vulnerability, particularly in terms of outages and network downtime. Equally important, cybercriminals are increasingly launching targeted DDoS attacks on critical services and applications.

SCENARIO DEFINITION AND ASSUMPTIONS

In this scenario, we are considering a banking institution with 800 employees operating in the Swiss financial sector. The cost analysis evaluates the financial impact of adding SCION GATE by Anapaya to the existing cybersecurity stack in terms of potential savings resulting from an attack surface reduction of up to 99%.

Figures are illustrative and scenario-specific; actual results may vary depending on organizational structure, risk profile, and deployment scope. Only direct costs are accounted for in the calculation. We do not include indirect costs like reputation damage, PR measures, or legal assistance after a security incident. For all examples, the prices are based on recent price indications from Swiss providers. Numbers have been rounded for clarity.

COST ANALYSIS

ANNUAL CYBERSECURITY COSTS

Based on industry interviews, the cost per employee per year in the Swiss banking sector ranges from CHF 800 to CHF 1,040 depending on the institution; therefore, an average figure of 920 CHF was adopted for our calculations for this specific bank that has 800 employees. The total annual cybersecurity costs of the bank amount to CHF 736k.

In this scenario, we assume that 30% of the cybersecurity costs are attributable to perimeter-based attacks – aligned with FINMA's 2025 report. This represents the portion of addressable cybersecurity costs that SCION GATE by Anapaya can impact, driven by the up to 99% reduction in attack surface it delivers. The remaining 70% relates to other attack vectors and is therefore not taken into account in this calculation.

This means that the bank faces CHF 220.8k in annual cybersecurity costs related to perimeter-based attacks that can be reduced with SCION GATE.

	[k CHF]
Total cybersecurity costs per year	736
Addressable costs (30% of tot) - related to perimeter-based attacks, reduced by SCION GATE by Anapaya	220.8

Based on industry interviews, the allocation of the cybersecurity costs by the bank is as follows:

- 55% for personnel and external services
- 25% for hardware
- 20% for licenses and software (not considered in this analysis)

Based on the baseline of addressable cybersecurity costs, three-year cost projections can be derived by accounting for expected increases over time.

THREE-YEAR ADDRESSABLE CYBERSECURITY COSTS

In the finance sector, the volume of cyberattacks is growing by approximately 30% annually (FINMA Risk Monitor 2024). In parallel, cybersecurity investments are increasing by around 20% per year, reflecting the rising threat landscape (Switzerland Cybersecurity in Financial Services Market). Based on this market data, we estimate that cybersecurity solution costs for banks will increase by 20% annually. We apply this 20% increase to the addressable costs associated with perimeter-based attacks (CHF 220.8k).

	YEAR 1 [k CHF]	YEAR 2 [k CHF]	YEAR 3 [k CHF]	TOTAL [k CHF]
Addressable cybersecurity costs	265	318	381	964
Annual increase of addressable costs	44	53	64	160

HARDWARE COST SAVINGS

In this scenario, we estimate that reducing the attack surface on the SCION Internet by up to 99% significantly lowers system load. This enables an extension of the hardware lifecycle from 3 to 4 years, bringing down hardware amortization from 33.3% to 25% of the hardware value per year, resulting in savings of approximately 8.3%. These savings are calculated only on future hardware investments, not on hardware already deployed.

	YEAR 1 [k CHF]	YEAR 2 [k CHF]	YEAR 3 [k CHF]	TOTAL [k CHF]
Hardware costs (25% of total addressable cybersecurity cost increases)*	11	13	16	40
Of which HW amortization over 3Y (33.3% of HW costs per year)	3.6	4.4	5.3	14
Of which HW amortization over 3Y (25% of HW costs per year)	2.7	3.3	4	10
Hardware savings	0.9	1.1	1.3	3.3

*Based on industry interviews, hardware costs account for 25% of cybersecurity costs.

PERSONNEL AND EXTERNAL SERVICES COST SAVINGS

We assume that, due to the attack surface reduction provided by SCION GATE by Anapaya, the operational burden on the security team decreases significantly. In particular, the need for resources in incident response is reduced, as complex analyses and escalation processes are required less frequently. We estimate that an 80% reduction in personnel and external services costs can be achieved following the deployment of SCION GATE by Anapaya.

	YEAR 1 [k CHF]	YEAR 2 [k CHF]	YEAR 3 [k CHF]	TOTAL [k CHF]
Personnel and external services costs (55% of total addressable cybersecurity costs)*	145	175	210	530
Personnel and external services savings (80%)	116	140	168	424

* Based on industry interviews, personnel and external services costs account for 55% of cybersecurity costs.

TOTAL COST SAVINGS

Based on the calculations above, we can now evaluate the total savings from implementing SCION GATE by Anapaya alongside existing cybersecurity solutions.

	YEAR 1 [k CHF]	YEAR 2 [k CHF]	YEAR 3 [k CHF]	TOTAL [k CHF]
Licensing fees, Connectivity, Initial implementation & configuration costs of SCION GATE by Anapaya	88.4 *inc. setup costs	80.4	80.4	249.2
Personnel and external services savings	-116	-140	-168	-424
Hardware savings	-0.9	-1.1	-1.3	-3.3
Total savings	-117	-141	-169	-427
Net savings	28.6	60.6	88.6	177.8

KEY FINDINGS: SECURE APPLICATIONS AND SERVICES FOR REMOTE ACCESS

SCION GATE BY ANAPAYA + CURRENT SOLUTION

CHF 142k

average annual savings across three years

71.6%

ROI (using a 3-year amortized cost basis)

9 months

payback period

Calculation details for ROI and payback time are available in the Appendix.

- Costs for SCION GATE by Anapaya average CHF 83,067 annually over a three-year period. Despite the initial investment required by deploying this solution, the bank saves money already in the first year, reaching more than CHF 177K over three years.
- By reducing future investment requirements, particularly in personnel and hardware, this solution enables a positive ROI within the first year of deployment.

SCION IN ACTION: SECURING THE FUTURE OF ENERGY

EKT AG is a leading Swiss energy and data services provider delivering reliable electricity and digital infrastructure to local energy providers, business, and public sector clients across and beyond the canton of Thurgau.

With increasing demands such as remote work, secure supplier access, and traditional VPNs, traditional standard Internet routes posed risks in latency, scalability and especially data security. EKT AG needed to ensure a secure, seamless connection to their remote access platform.

EKT AG deployed SCION GATE by Anapaya, a SCION-based solution, to establish reliable and verifiable connections between remote users and their remote access platform. Using the Swiss Isolation Domain, EKT AG ensures that only domestic users are able to connect to the access infrastructure, whereas it is completely hidden to regular Internet users.

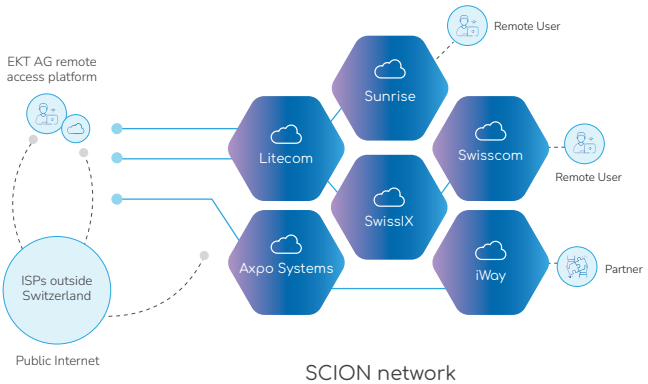
To enable secure and controlled access for remote employees and field engineers, the following architecture was deployed:

- SCION EDGE acts as a network access point, connecting EKT AG's internal systems to the SCION network.
- Via SCION GATE by Anapaya, only remote employees located in Switzerland can connect to the remote access platform – tremendously reducing the attack surface.

See more about this use case study here.

KEY BENEFITS:

- Higher security: Remote workers now access critical infrastructure over a trusted, identity-bound SCION path, eliminating reliance on insecure Internet routing.
- **Improved performance:** Noticeable latency reduction and improved system responsiveness for remote operators.
- **Reduced risk:** Attack surface minimized by avoiding exposure to untrusted networks.
- **Scalability:** Flexible onboarding for new partners and regions without compromising governance.



SCION network

"With Anapaya GATE, we now have a trusted, secure way to connect our remote teams and suppliers to our central remote access platform — no compromises on performance or security. It's a fundamental part of our digital operations." Andreas Plüer CISO of EKT AG

CONCLUSION

The white paper demonstrates that SCION is a more cost-effective solution than other products and solutions available in the market today across various use cases. In addition, SCION brings significant benefits in terms of availability, supply chain diversity and redundancy.

FINANCIAL BENEFITS

USE CASE	SOLUTION DEPLOYMENT	COST REDUCTION [%]	ANNUAL COST SAVINGS [CHF]	ROI [%]	PAYBACK TIME
SCION vs leased lines	Replacement	91	1.34m	2389	<1 month
SCION vs MPLS	Replacement	81	600k	1110	<1 month
SCION vs SD-WAN	Replacement	32.6	315k	228	<4 months
SCION GATE by Anapaya for remote access	Complement	N/A	142k (average across three years)	71.6	9 months

BUSINESS BENEFITS

- Business continuity: SCION can reduce the likelihood and operational impact of service outages, which may in turn reduce associated revenue loss and service-delivery risk.
- Financial and reputation resilience: SCION can help limit financial and reputational exposure by reducing attack surface and improving network-level control for critical services, and can help avoid crisis communication and escalation costs.

OPERATIONAL BENEFITS

- Cybersecurity: Reduced attack surface lowers exposure to cyberattacks.
- Cyber-resilience: Multi-provider architecture that eliminates concentration risk and improves availability.
- Infrastructure sovereignty: Path control enables visibility and choice at the network layer.
- Network governance: Strict control at the network layer for improved visibility across third parties.

STRATEGIC BENEFITS

- Compliance & regulation: Where NIS2 and DORA impose compliance obligations, SCION can strengthen the technical control environment by improving path transparency, governance, and resilience-related network controls.
- Optionality and sovereignty: Multi-provider architecture reduces concentration risk and increases control at the network layer.
- Third-party risk management: Visibility and control over the entire value chain at the routing level.

INDIRECT COSTS

- Learning curve & organizational change: SCION introduces an innovative Internet architecture model and network and security and IT teams must understand new routing concepts. Although the learning curve is typically fast for experienced network engineers, time and internal capacity must be allocated.
- Initial setup & migration effort: SCION deployment is technically straightforward, but it requires endpoint installation (SCION EDGE or GATE), and migration planning from legacy MPLS / SD-WAN / VPN / solutions.
- Ecosystem & provider availability: SCION is deployed across critical infrastructure and growing in enterprise environments, but it is not yet as universally available as traditional Internet services. Consideration should be given to the availability of SCION-enabled ISPs in specific geographies, as well as the need to align suppliers or partners to connect via SCION.
- Foundational security not all-in-one: SCION reduces the attack surface and improves resilience, but it does not eliminate human-factor risks (phishing, misconfiguration). Organizations must view SCION as foundational infrastructure strengthening, not a complete cybersecurity replacement.

SCION: THE FOUNDATION FOR CRITICAL INFRASTRUCTURE CONNECTIVITY

In our examples, SCION particularly excels with enterprise WANs and critical infrastructures such as in the finance, healthcare, defence, control grids (e.g. energy) and government industries that have a need for enhanced levels of network trust and control over the participants in their network and where their data is travelling. This is something that is currently only possible with leased lines and MPLS, but these solutions are inflexible, vendor-specific, expensive, and often lack the resilience required today.

SCION offers a differentiated combination of path awareness, multi-provider connectivity, and governance capabilities that is uncommon in conventional enterprise network models. It is inherently designed to support multi-provider and interoperates with commodity Internet connections from multiple ISPs, whilst providing assurances and control over the networks over which data is sent. It therefore not only provides substantial ROI when replacing traditional solutions, but also offers superior capabilities that go a long way towards meeting present day cyber resilience, data protection, and regulatory compliance requirements.

As IT increasingly becomes a matter of cyber resilience and business sustainability, SCION technology becomes both a financially sound and strategic choice for business leaders.

APPENDIX

GLOSSARY

SCION: SCION (Scalability, Control, and Isolation On Next-Generation Networks) is an Internet path-aware technology that supports trusted inter-domain multipath routing through cryptographically validated end-to-end paths selectable by endpoints. Paths are authenticated at discovery and verified when traffic is forwarded, providing higher assurances that packets will follow particular paths, preventing routing security problems, and ensuring geofencing. Source: www.scion.org

ISD: SCION Isolation Domains (or trust domains) represent a logical grouping of networks (SCION autonomous systems or ASes) based on trust. An ISD is administered by a smaller subset of the ASes that govern its policies. Each ISD relies on its own roots of trust, called a trust root configuration (TRC). Source: www.scion.org

Leased lines: A leased line is a private telecommunications circuit between two or more locations provided according to a commercial contract. It is sometimes also known as a private circuit, private connect, and as a data line. Source: Wikipedia

P2P: point-to-point connectivity between two sites or nodes. Source: Wikipedia

MPLS: Multiprotocol Label Switching (MPLS) is a private, high-performance networking technology for enterprises, used to connect branch offices, and it is widely used for critical applications as it is separate from the public Internet. A MPLS network is typically provided and administered by a single telecom provider. Source: Wikipedia

SD-WAN: A Software-Defined Wide Area Network (SD-WAN) is a wide area network technology that uses centrally orchestrated VPN tunnels over the Internet to connect enterprise branches. Source: Wikipedia

VPN: A virtual private network (VPN) is a technology that encrypts and tunnels data so that it can transit across a public network, such as the Internet. Source: Wikipedia

TECHNICAL RESOURCES

- About SCION website: https://www.scion.org/about-scion/
- SCION IETF Specifications: https://datatracker.ietf.org/doc/draft-dekater-scion-controlplane/
- https://datatracker.ietf.org/doc/draft-dekater-scion-dataplane/
- https://datatracker.ietf.org/doc/draft-dekater-scion-pki/
- The Complete Guide to SCION (2022). https://link.springer.com/book/10.1007/978-3-031-05288-0
- SCION: A secure Internet Architecture (2017) https://scionproto-contrib.github.io/publications/pdfs/2017/SCION-book.pdf

ROI AND PAYBACK TIME CALCULATION

ROI = (SAVINGS – INVESTMENT) / INVESTMENT × 100

PAYBACK TIME = INVESTMENT ÷ SAVINGS

PUBLICATION DETAILS

Published by

SCION Association
www.scion.org

In collaboration with

SIX
www.six-group.com

Eraneos
www.eraneos.com

Anapaya - The SCION Company
www.anapaya.net