ANAPAYA

Webinar: SCION – Das sichere Internet der nächsten Generation jetzt in Liechtenstein: Was Unternehmen wissen müssen

Organisatorische Hinweise

- **Nutzung der Q&A-Funktion:**

  Nutzen Sie gerne die Q&A-Funktion, um während des Webinars Fragen zu stellen. Am Ende werden wir so viele Fragen wie möglich beantworten.

- **Aufzeichnung und Weitergabe:**

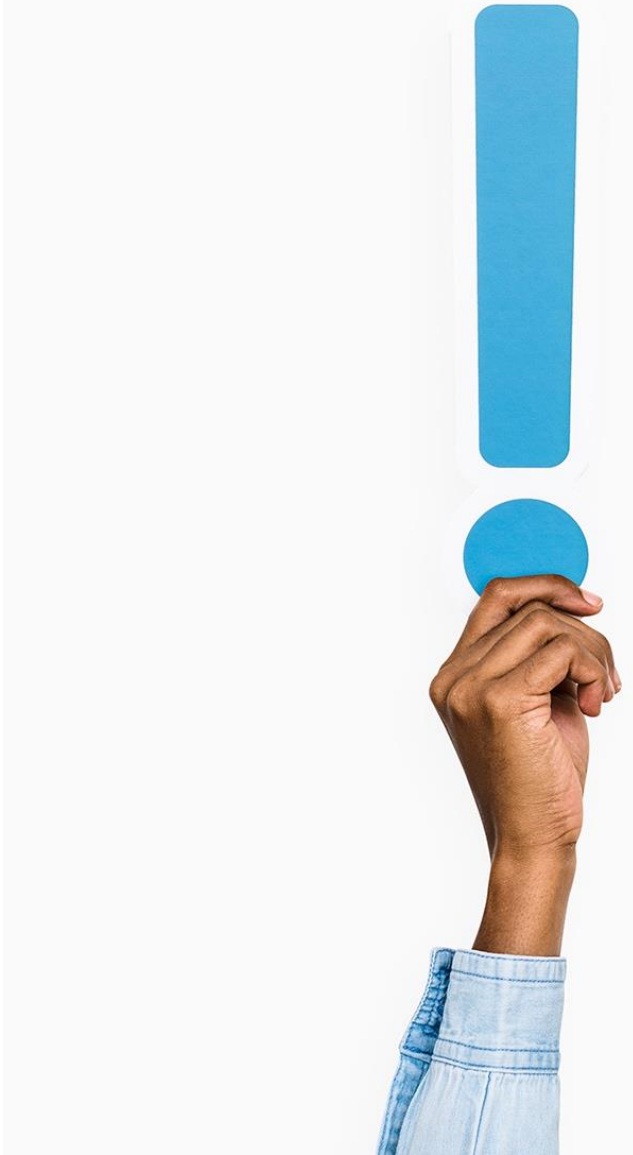
  Bitte beachten Sie, dass das Webinar zu Referenz- und Weitergabezwecken aufgezeichnet wird.

- **Folgeunterlagen:**

  Nach dem Webinar stellen wir Ihnen Folgeunterlagen zur Verfügung, darunter die Präsentationsfolien und die Aufzeichnung dieses Webinars zum Abruf.

- **Feedback:**

  Ihr Feedback ist uns wichtig! Nach dem Webinar erhalten Sie eine kurze Umfrage, in der Sie Ihre Meinung und Verbesserungsvorschläge mitteilen können. Wir freuen uns über Ihre Rückmeldung.



Ihre Moderatoren

ANAPAYA

Dario Colacicco

Chief Revenue Officer

The SCION Internet didn't happen over night

2012

SCION research started at ETH Zurich

2017

Anapaya Systems AG was incorporated

2018

1st commercially available SCION router introduced

2020

Successful pilot:
Secure Swiss Finance Network (SSFN)

Gartner "Cool Vendor", Wavestone "Swiss Cyber Security Radar"

2021

SSFN Go-live for 321 Swiss banks and financial market infrastructures

Government international projects Go-live

2022

HVR (HIN Vertrauensraum) Health Secure Network is ready

2023

GATE ANAPAYA

Anapaya GATE 100% reach in Switzerland to SCION

2024

Secure Swiss Finance Network (SSFN) will replace Finance IPNet by end of September

2025

Official launch of the Secure EFTPOS Network for payment networks and Secure Swiss Utility Network for the energy and utility sectors

"SCION is uniquely positioned as it solves the root causes of the Internet's security problems – in contrast to other solutions focused on solving symptoms."

Prof. Dr. Adrian Perrig

Department of Computer Science
Institute of Information Security, The Network Security Group

axpo · ETH zürich · LG U+ · SIX · Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Federal Department of Foreign Affairs FDFA · Schweizerische Nationalbank Banque nationale suisse Banca nazionale svizzera Banca naziunala svizra Swiss National Bank · Sunrise · swisscom · Switch

ANAPAYA

The Internet

Internet = is made of ASes (Autonomous Systems)

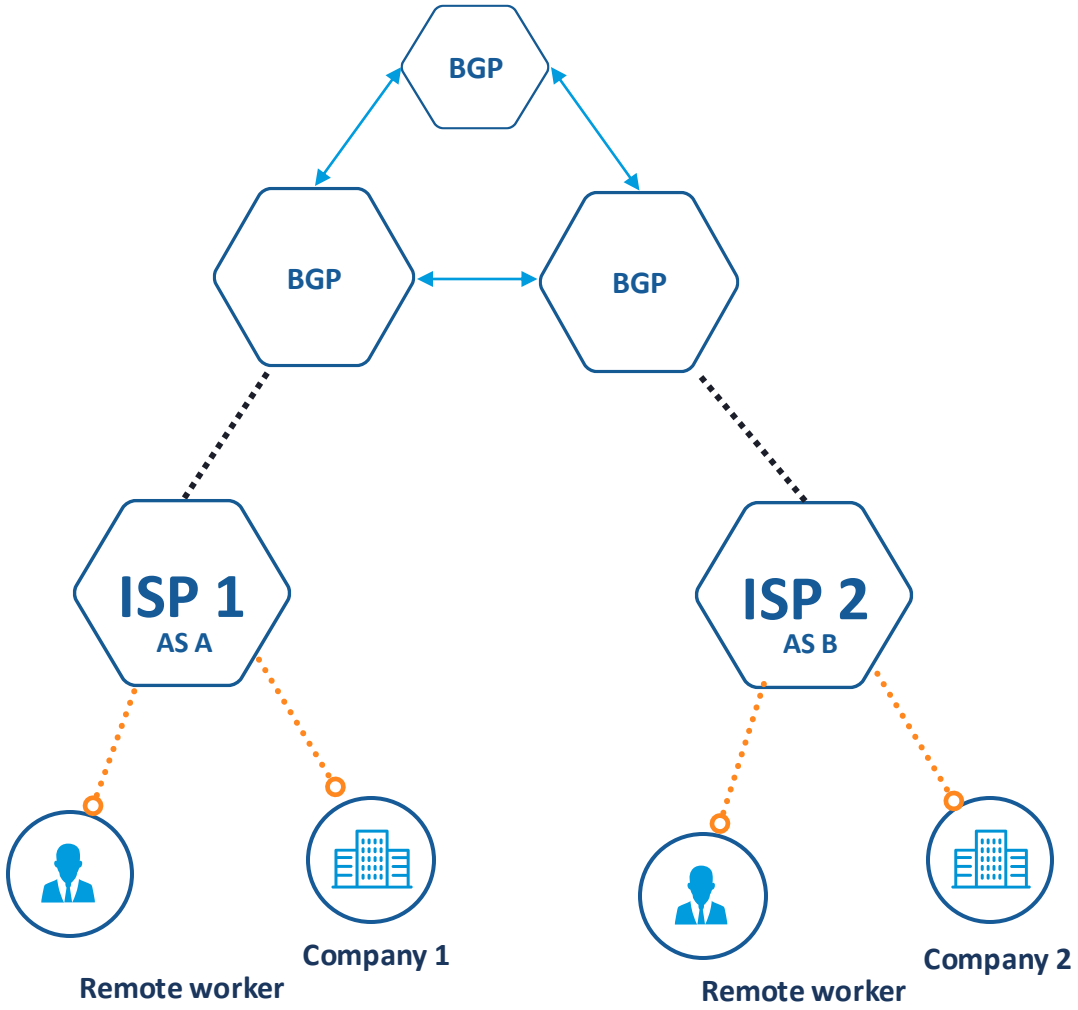
	The OSI model	The TCP/IP model
	Layer 7 - Application	Application layer
	Layer 6 - Presentation	
	Layer 5 - Session	
BGP	Layer 4 - Transport	Transport layer
	Layer 3 - Network	Internet layer
	Layer 2 - Data Link	Network Access layer
	Layer 1 - Physical	

BGP – Border Gateway Control

Typically, each AS is operated by a single large organization, an Internet Service Provider (ISP), or a large technology company.

The ASs are connected to each other and pass on the information via the BGP protocol.

BGP Route Exchange (AS A ↔ AS B)



BGP between two Autonomous Systems

- BGP (Border Gateway Protocol) connects networks of different ISPs.
- AS A and AS B establish a BGP session (TCP Port 179) between their border routers.
- BGP Announcements:
  - AS A says: “To reach 10.0.0.0/16, go through me.”
  - AS B says: “To reach 20.0.0.0/16, go through me.”
- Both store these routes in their routing tables → data can flow between A and B.
- The AS path shows the route across ASes and prevents routing loops.
- Each ISP applies policies to control which routes they accept or advertise.

The internet is outdated

The internet, as we know it today, is built on a **34-year-old protocol** that was not intended to scale to **1 billion hosts.**

The Internet is vulnerable to cyberattacks, including BGP hijacking and DDoS.

With SCION you can **minimize risk** by running data through authenticated paths only.

While you can adapt routing policies, users still have no control where their data is sent.

SCION offers path control which gives **unprecedented control** over your data.

Data is often sent on the cheapest but slowest route, impacting connectivity and performance.

SCION offers **better connections** by optimizing routes for best performance to keep your system running smoothly.

Solutions today, solve part of the problem

Today's solutions are **expensive**, offer **no control** over the path and **lack true flexibility and scalability.**

MPLS (Multiprotocol Label Switching)

MPLS is a protocol used for efficient packet forwarding in network. It is often used by enterprises to connect multiple locations securely.

Drawbacks:

MPLS can be expensive and may have limitations in terms of flexibility and scalability.

SD-WAN (Software-Defined Wide Area Network)

SD-WAN offers centralized control and the ability to use multiple connection types.

Drawbacks:

SD-WAN relies on the underlying networks for connectivity, and the effectiveness can depend on the quality of those connections.

VPN (Virtual Private Network)

VPNs provide a secure connection between two points over internet, allowing users to access a private network from remote location.

Drawbacks:

VPNs can sometimes suffer from latency and performance issues, and their effectiveness can be impacted by the quality of the underlying internet connection.

ANAPAYA

02 SCION

Anapaya, Revolutionizing the Internet

Secure, resilient, and control

Anapaya is revolutionizing the Internet for a future of **secure, resilient, and controlled** connectivity. Anapaya will empower business with a network infrastructure that **ensures availability** for a **seamless digital experience** through SCION technology.

Inherently secure

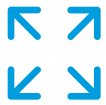
Built from the ground up with security in mind to effectively address today's internet from vulnerabilities.

Always available

Designed for resilience, ensuring uninterrupted operations even in the face of disruptions.

Unprecedented Control

Enjoy transparency and the flexibility to choose which providers have which access, choose what path your data takes and choose the performance of each connection.



Future-Ready Scalability

Offer scalable solutions that adapt to the evolving needs of your business.

What is SCION?

SCION is a **new Internet architecture** based on a decade of research at the Swiss Federal Institute of Technology in Zurich (ETH).

Path Control & Multipath

Sender decides **where** packets go and **how** they get there.

Multipath feature also allows senders to choose more than one path at the same time.

Isolation Domain

This self-contained unit connects internet service providers and users under a **unified trust environment.**

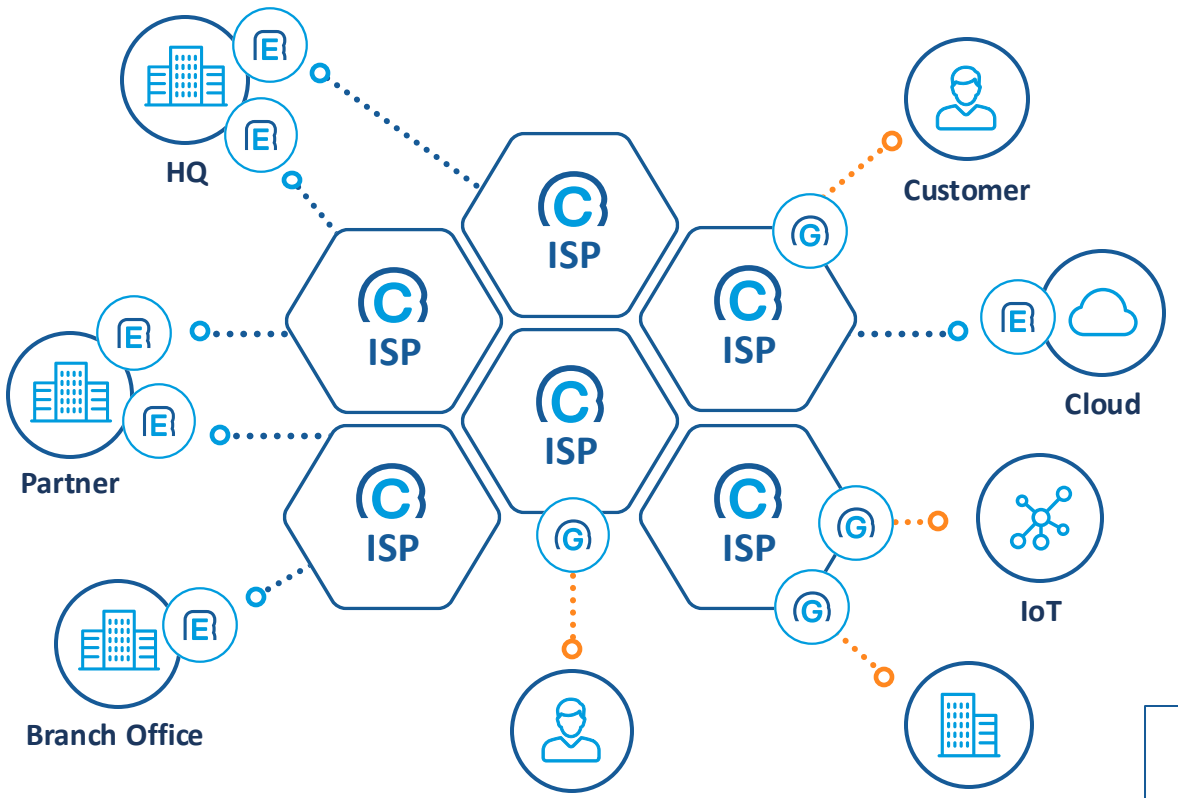
Explicit Trust

Visualize the various paths your data can traverse, paths that are **cryptographically authenticated.**

Critical infrastructure connectivity through Anapaya

- **Anapaya CORE**s operated by a community of network service providers **build the backbone** of the SCION Internet. CORE**s** are like **waypoints** on the path between the source and destination.
- **Anapaya GATEs and EDGEs** allow users to **securely access the SCION Internet**, without the need for any configuration or installation for end users
- **Using the EDGE and GATE guarantees business continuity** (DDoS prevention, fast failover), hijacking immunity, attack surface reduction, and geo-fencing
- **Improve system performance through simultaneous control** across several paths for increased capacity and lower latency AND choose a path based on latency, drop rate, jitter, or trust and geographical jurisdiction

[DEMO]



Prevent DDoS and intrusion attacks with Anapaya GATE

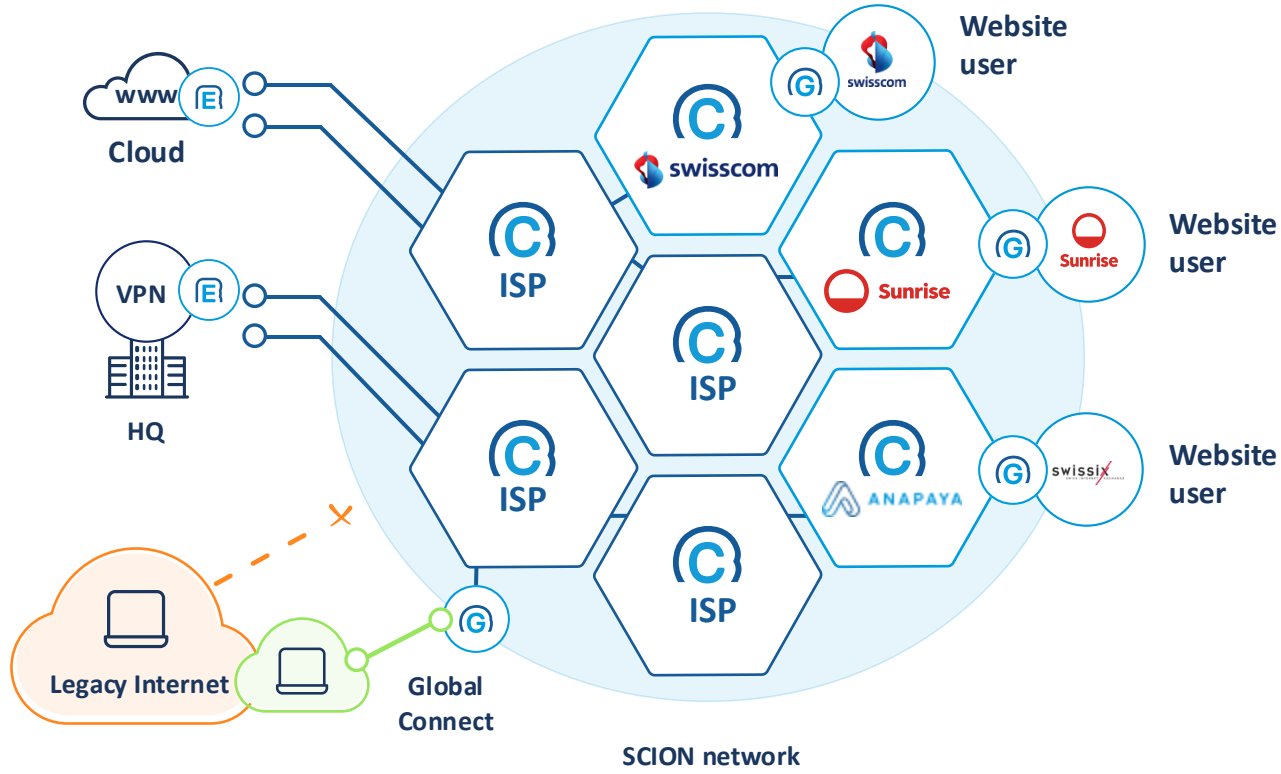
Secure your VPN, IoT or website

Choose which services to make public and which to restrict to specific ISPs and their users using **Anapaya GATE.**

Reduce your attack surface by up to **99.9%** - what cannot be seen, cannot be attacked.

Global reach in one click

With Global Connect, you can selectively and safely extend the reach of your web service to the broader public Internet without compromising security.



Your service

Always on

Uninterrupted operations with constant connectivity.

Always secure

Business continuity and data security with DDoS and intrusion attack prevention.

It's that simple

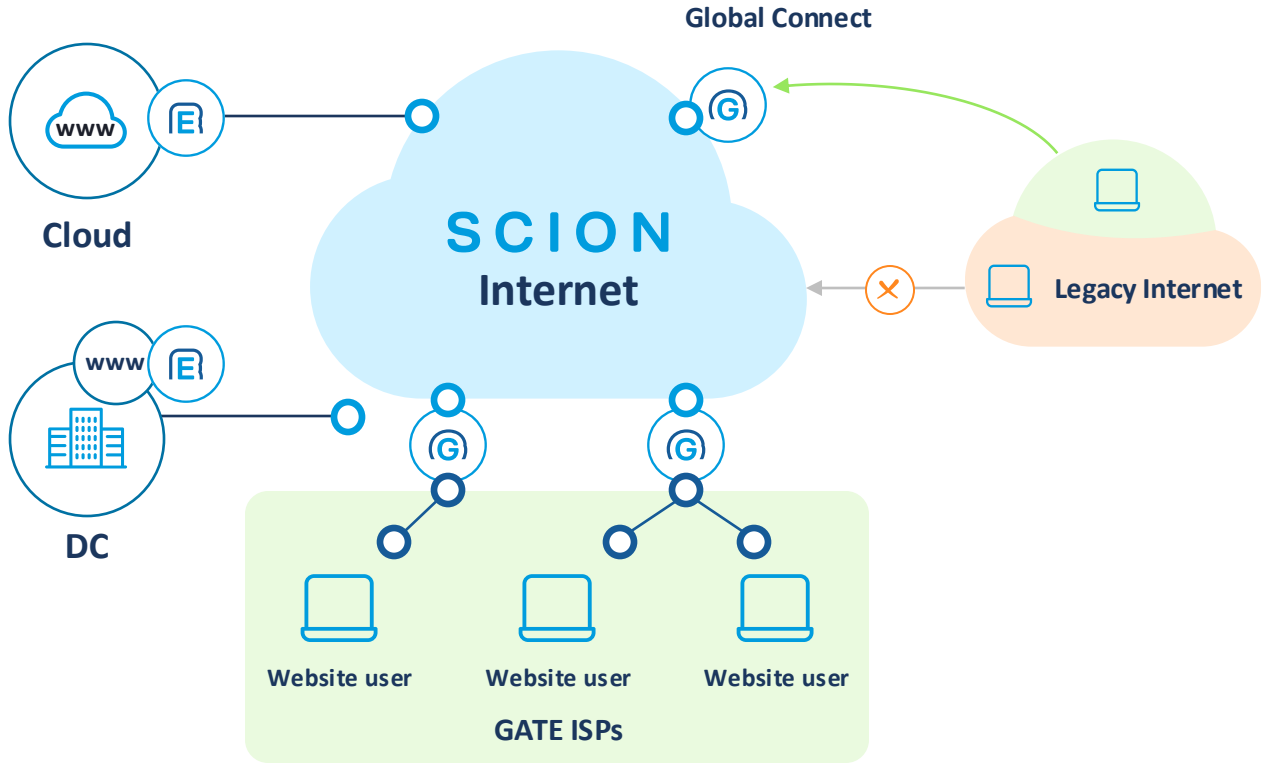
License-based model with no installation and 24/7 support.

Prevent DDoS and intrusion attacks with Anapaya GATE

Secure your VPN, IoT or website

Choose which services to make public and which to restrict to specific ISPs and their users using **Anapaya GATE.**

Reduce your attack surface by up to **99.9%** - what cannot be seen, cannot be attacked.



Global reach in one click

With Global Connect, you can selectively and safely extend the reach of your web service to the broader public Internet without compromising security.

Your service

Always on

Uninterrupted operations with constant connectivity.

Always secure

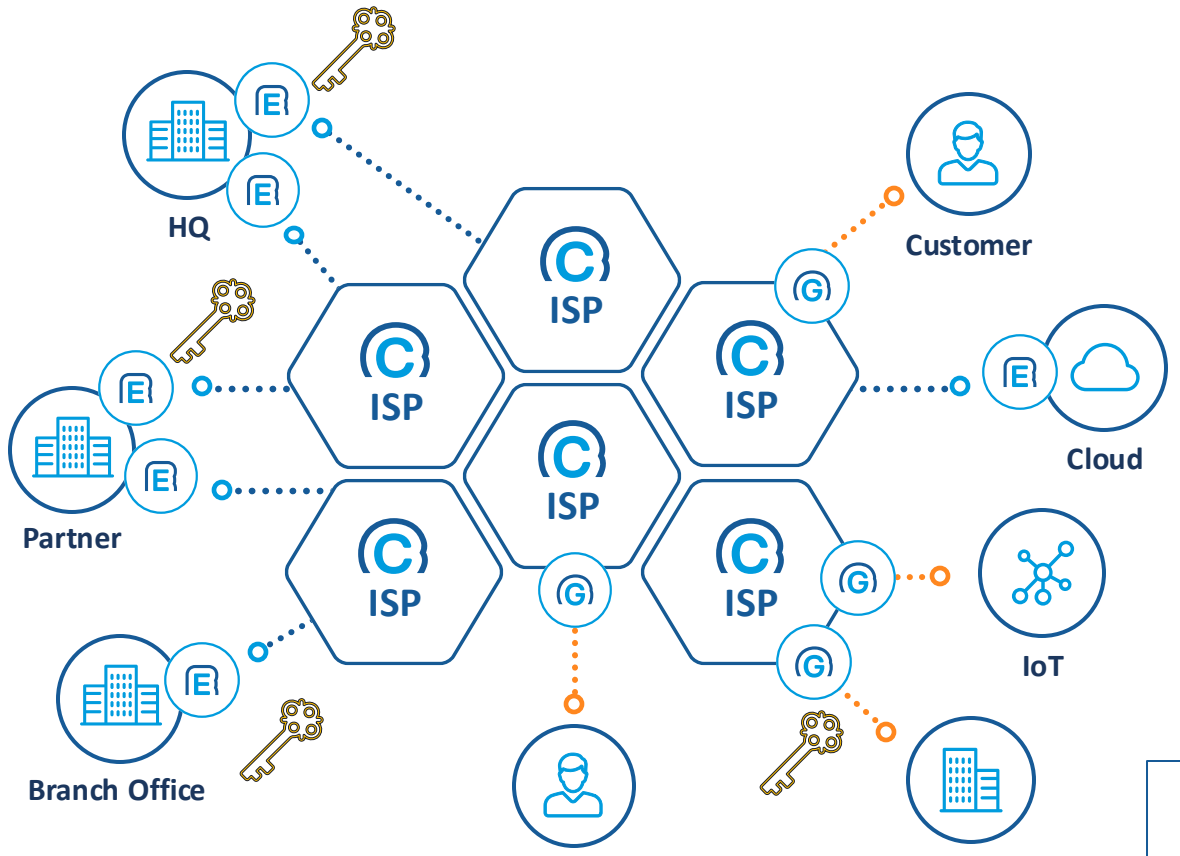
Business continuity and data security with DDoS and intrusion attack prevention.

It's that simple

License-based model with no installation and 24/7 support.

ISD: Independent Trust Zones in the SCION Architecture

- **Definition:** An ISD (Isolation Domain) is a self-contained trust and administrative zone within the SCION network. It represents the top layer of the SCION architecture and defines which organizations collaborate and under which trust policies they operate.
- **Trust Anchor**: Each ISD has its own Trust Root Configuration (TRC), which specifies the valid certification authorities, signatures, and security policies. This creates an independent and clearly defined trust base, separate from other ISDs.
- **Isolation and Security**: A key principle of SCION is isolation: failures, misconfigurations, or attacks inside one ISD remain contained within that domain and do not affect others. This provides strong stability, resilience, and security across the global network.
- **Inter-ISD Communication**
  Despite their isolation, ISDs can communicate securely with each other through defined gateways and policies. This preserves trust and governance within each ISD while still enabling controlled global connectivity.



Anapaya is trusted by Swiss industry leaders

SSFN: Secure Swiss Finance Network

The secure, reliable, community-based and sovereign network launched to interconnect **> 300 participants.**

SSHN: Secure Swiss Health Network

Improving the cyber-resilience of the health ecosystem in Switzerland by onboarding **~50k health professionals.**

SEPN: Secure EFTPOS Network

The Secure EFTPOS Network (SEPN) leverages SCION technology to deliver unmatched resilience, security, and flexibility in cashless payments.

SSUN: Secure Swiss Utility Network

The SSUN will improve the interconnectivity of the Swiss energy sector and provide secure and isolated communication between different companies in the ecosystem.

Government and Defense

Several initiatives with the Confederation are now active at different levels: from productive SCION connections between Asian locations and Switzerland.

Upgrade to SCION – here's how

Become SCIONabled through

Commercial provider of SCION

ANAPAYA

Our ecosystem partners

axpo, BT, CELESTE, cyberlink, eraneos, Extreme networks, EveryWare eCommunications, GÉANT, IBM, infoGuard, INFOSEC GLOBAL, Litecom, LG U+, proximus NXT, Sunrise, swisscom, Switch, TATA CONSULTANCY SERVICES, VARITY, GAS&COM, gmg, colt

What we offer

EDGE

Physical access to the SCION internet

Who's it for?

- Business
- Financial institutions
- Healthcare
- Government organizations

GATE

Render remote working data invisible to attackers

Who's it for?

- Remote workers
- Essential employees
- Traveling professionals
- Home users

CORE

SCION router at the border of ISP backbones

Who's it for?

ISPs

SCION: Full coverage in CH & expanding internationally

axpo · CELESTE · cyberlink · EveryWare

Litecom · Sunrise · swisscom · Switch

BT · colt · GÉANT · IBM · LG U+

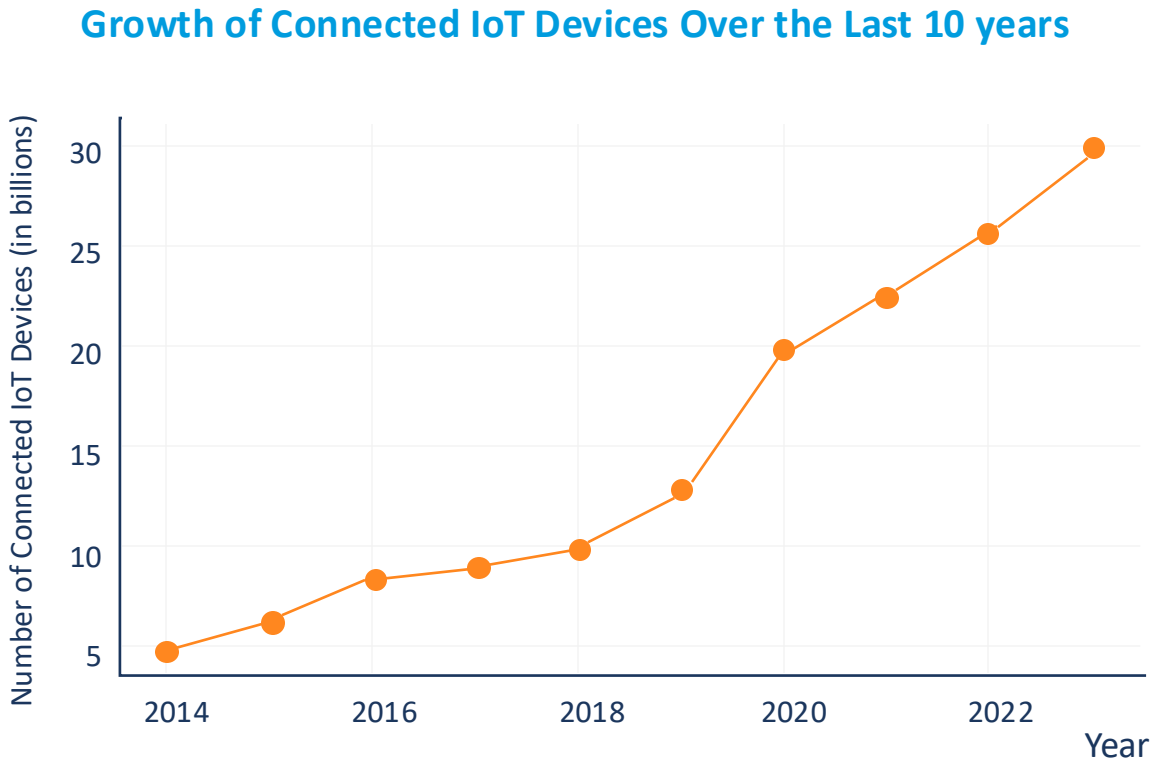
proximus NXT · gmg · TCS TATA CONSULTANCY SERVICES · VARITY WE THINK IN POSSIBILITIES

ANAPAYA

03 Use cases

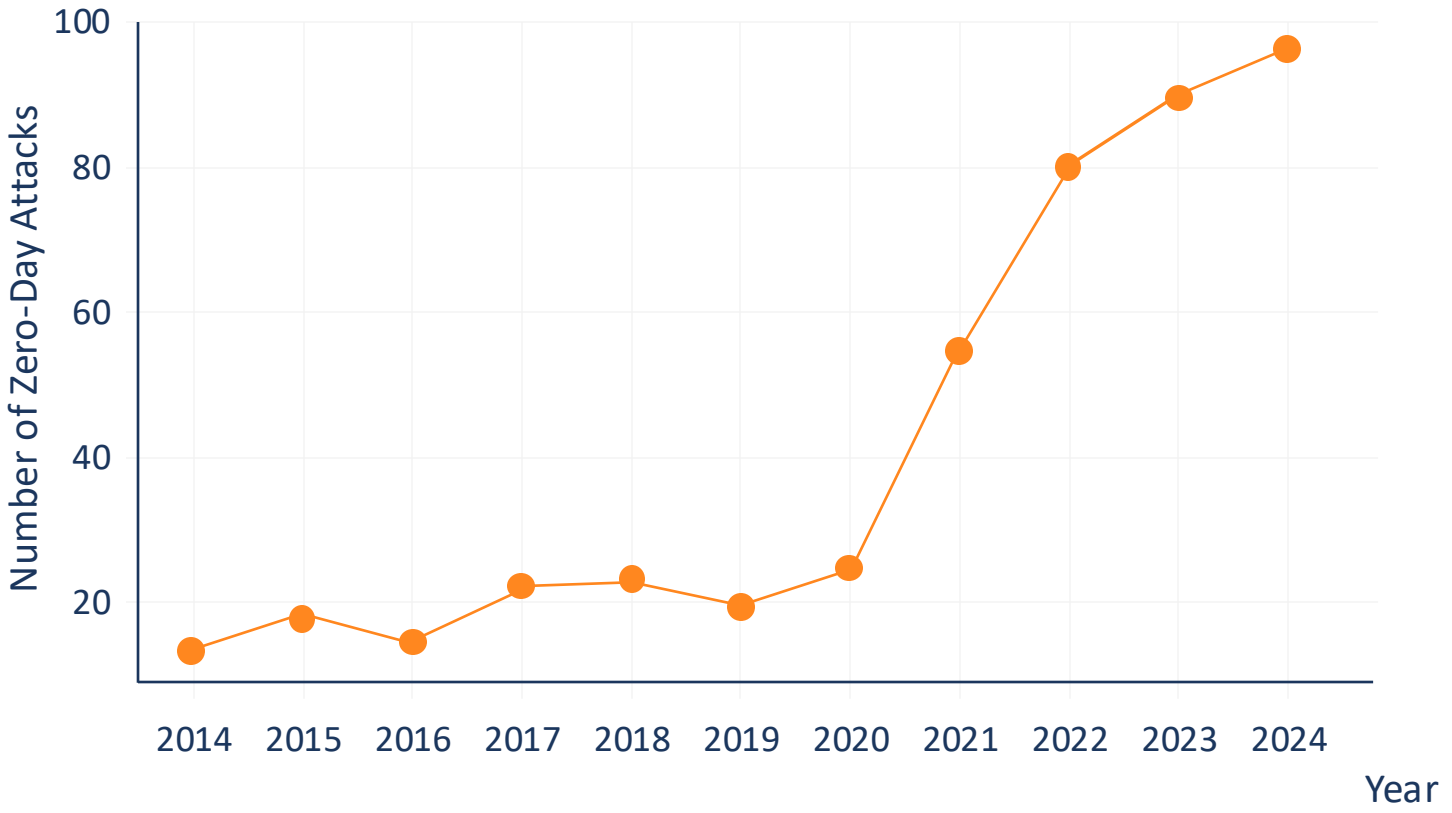
Internet of Things (IoT) dangerous growth factor

Charging stations, solar panels, wind turbines, heating units…

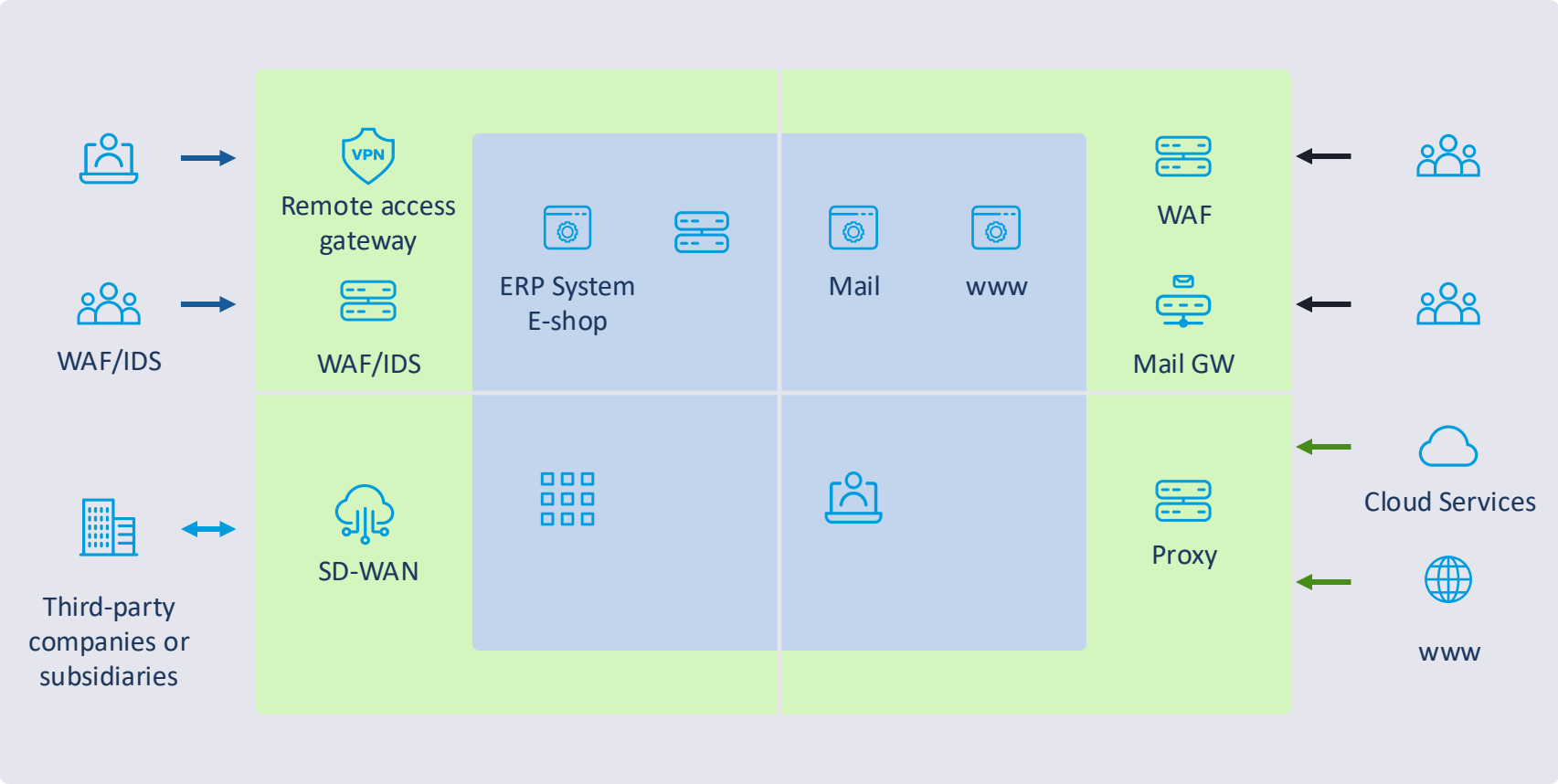


Zero-day attacks have been increasing in frequency
The Internet eats itself…

Reported Worldwide Zero-Day Attacks (2014-2024)



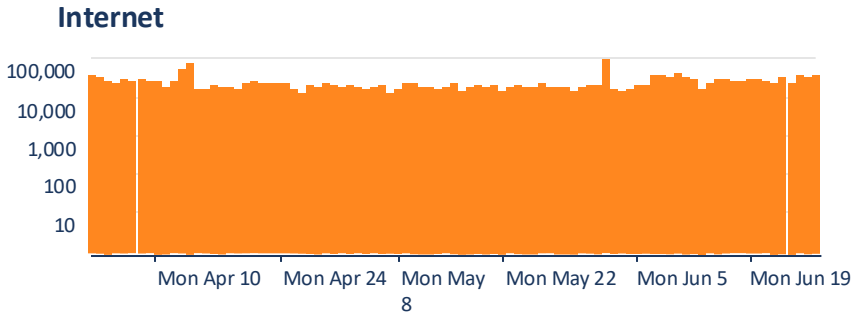
Internet, the number one operational business risk factor!



A corporate enterprise uses on average **40+ different security applications** to protect itself in the cyber space.

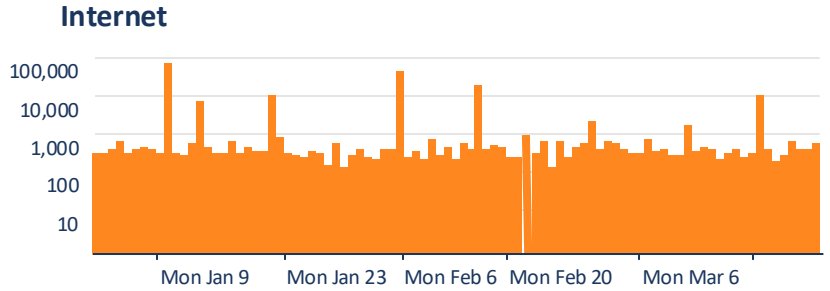
An Internet Service sees 30k scans & 1k attacks per day!

Attacks with unspecific intent



Total 8,837,232 2023

Attacks with malicious intent



Total 85,895 2023

Growing size of the Internet is resulting in more Zero-day's…

2024

Security issues and attacks affecting numerous organizations and users.

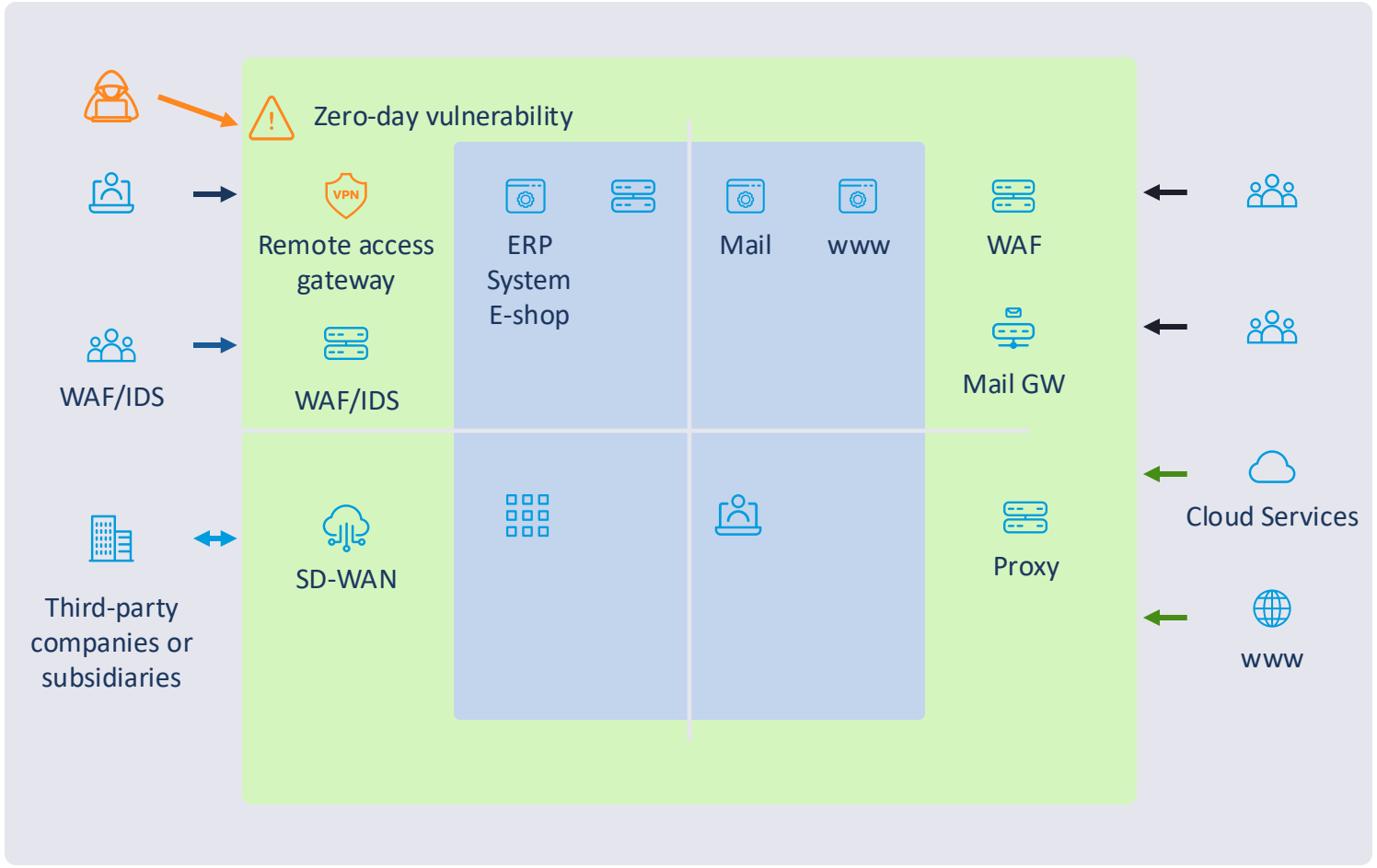
- **Palo Alto Networks:** PAN-OS (CVE-2024-3400): Command injection, actively exploited.
- **Cisco ASA:** and FTD (CVE-2024-20353, CVE-2024-20359): Control over affected systems through targeted attacks.
- **Ivanti** VPN (CVE-2024-21887): Exploited by nation-state attackers, exact user count not specified.
- **OpenVPN:** Zero-Day Vulnerabilities (CVE-2024-27903, CVE-2024-27459, CVE-2024-24974): Allowed remote code execution and privilege escalation, impacting thousands of companies worldwide

2025

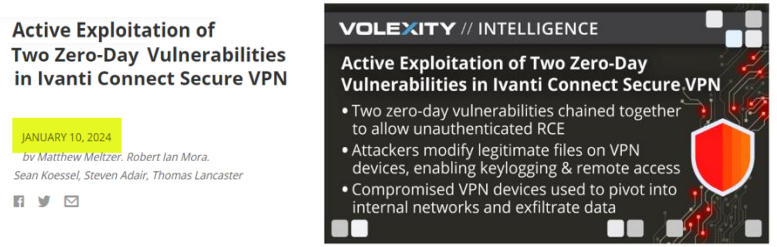
The attacks continue into 2025. These are just a few from Q1 of 2025.

- Palo Alto Networks PAN-OS (mgmt web UI) — **CVE-2025-0108:** Auth bypass on management interface; exploitation attempts observed; added to KEV in Feb. Disclosed **Feb 12**.
- Ivanti Connect Secure / Policy Secure / ZTA — **CVE-2025-22457:** Unauth stack buffer overflow → RCE. Disclosed **Apr 3**; campaigns observed from mid-March; KEV/industry confirm active exploitation.
- Citrix NetScaler ADC / NetScaler Gateway — **CVE-2025-7775:** Pre-auth memory overflow → **RCE/DoS** (specific IPv6/Gateway/AAA configs). Citrix confirmed **exploitation at disclosure** (**Aug 26**).

1 VPN Zero day = 1’700 compromised enterprises in 5 days



On **January 10th** 2024, a zero-day vulnerability on Ivanti remote access product is discovered…



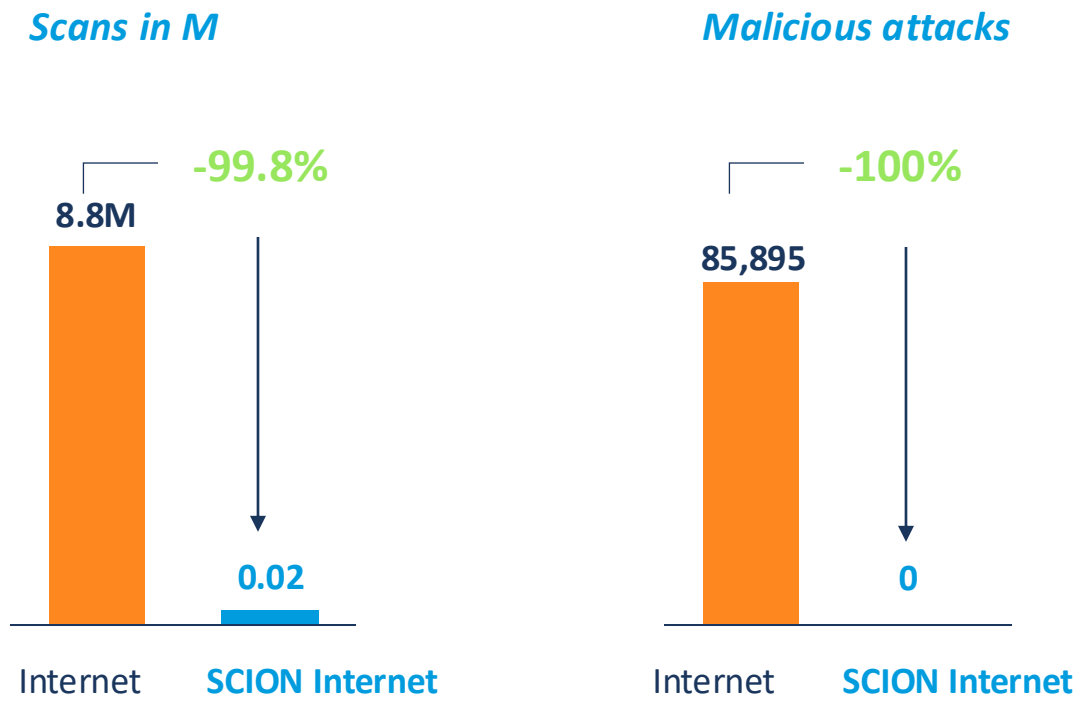
By **January 15th** at least **1,700 corporates** were reported to be compromised!

Internet Security Tech Corporation

Get control back with SCION

- Developed at ETH Zürich
- Inherently security by path-control
- Global standard governed by the independent SCION Association
- High resiliency & performance through multi-path architecture

Measured & Proven



ANAPAYA

04 Reference cases

Beyond the SSFN: The Frankfurter Bankgesellschaft leverages SCION connectivity to drive innovation, efficiency and security

The Frankfurter Bankgesellschaft moved to the SSFN as mandated to continue services with SIX but quickly added new use cases enabled only by their existing SCION infrastructure.

The challenges

- Rise in cyber threats pose a significant challenge.
- Clients expect seamless access to their services anytime, anywhere, and from any device.
- Remote access to critical internal systems requires a secure and resilient connectivity solution.

The solution

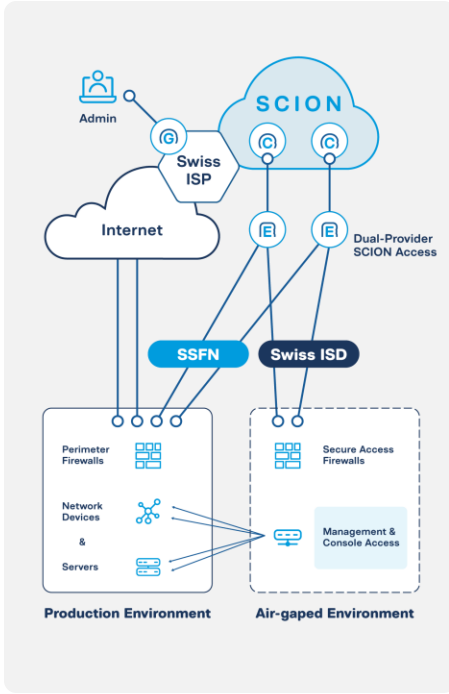
Leverage existing SCION network to establish resilient, secure remote access solution to its independent systems management infrastructure —a critical component for business continuity and disaster recovery.

The set up

The Anapaya EDGE routers installed support both SSFN and Swiss ISD on the same hardware ensuring segmented security:

- To their perimeter firewalls for SSFN services
- To a separate set of firewalls for secure access to out-of-band infrastructure

The Swiss ISD firewalls ensure remote access in case of network outage or cyber incident.



Peace of mind

Increased efficiency

Compliance

Cost optimization

Network resilience

The Frankfurter Bankgesellschaft leverages SCION connectivity to drive innovation, efficiency and security

Steve Erzberger

Head of IT

Frankfurter Bankgesellschaft
PRIVATBANK | Zürich | Frankfurt

"Building on our existing SCION infrastructure, we have enabled secure remote access to our out-of-band management network for IT administrators— ensuring controlled access to critical datacenter devices for maintenance work and disaster recovery. is air-gapped setup remains isolated from internal networks and the public internet while leveraging SCION's inherent security and resilience. By doing so, we have expanded our administrators' flexibility and reach without compromising security, compliance, or operational integrity."

Private Client Bank enhances cyber resilience with Anapaya GATE

Since its establishment in 1998, Private Client Bank has been owned by renowned entrepreneurial families from Switzerland and Germany, offering services for wealthy families and professional clients.

The challenge

To keep up with quickly evolving technologies — and the growing risk of cyber threats — PCB searched for a smart approach to enhance their cyber resilience by adding an extra layer of security.

As systems and data exposed to the Internet are prone to cybercrime, the focus was on the security of their remote worker access.

The solution

By deploying Anapaya GATE, PCB gained a new layer of security and sovereignty over its remote access infrastructure. Built on SCION, Anapaya GATE ensures that only authorized remote employee connections can access the bank's data, and these connections are exclusively routed through Swiss-controlled, trusted paths.

The set up

With an extensive network of GATE providers, access to any remote online service behind the Anapaya GATE is available across Switzerland through a Swiss isolation domain.

Swiss-based connectivity

Prevention of DDoS attacks

Seamless experience

Scans reduced by
99.8%

Private Client Bank enhances cyber resilience with Anapaya GATE

Barbara Hüber

COO Private Client Bank

PRIVATE CLIENT BANK

"As a bank built by families for families, trust is the foundation of the relationships with our clients; relationships that span generations. With the SCIONabled Anapaya GATE, we have taken an additional step toward ensuring that our remote access infrastructure meets the highest level of security—one that aligns with the standards of the Swiss National Bank."