ANAPAYA

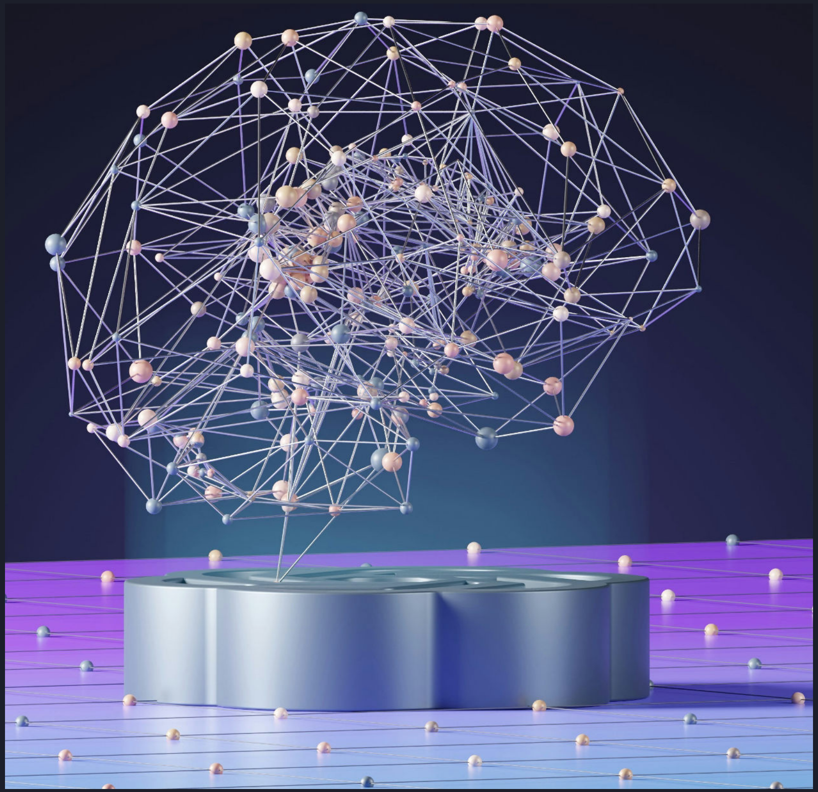
SCION and AI

Trustworthy AI depends on a secure network

Martin Bosshardt,

CEO, Anapaya Systems
Member, stars Scientific Board,
Zurich, Switzerland

A secure internet infrastructure is critical for AI

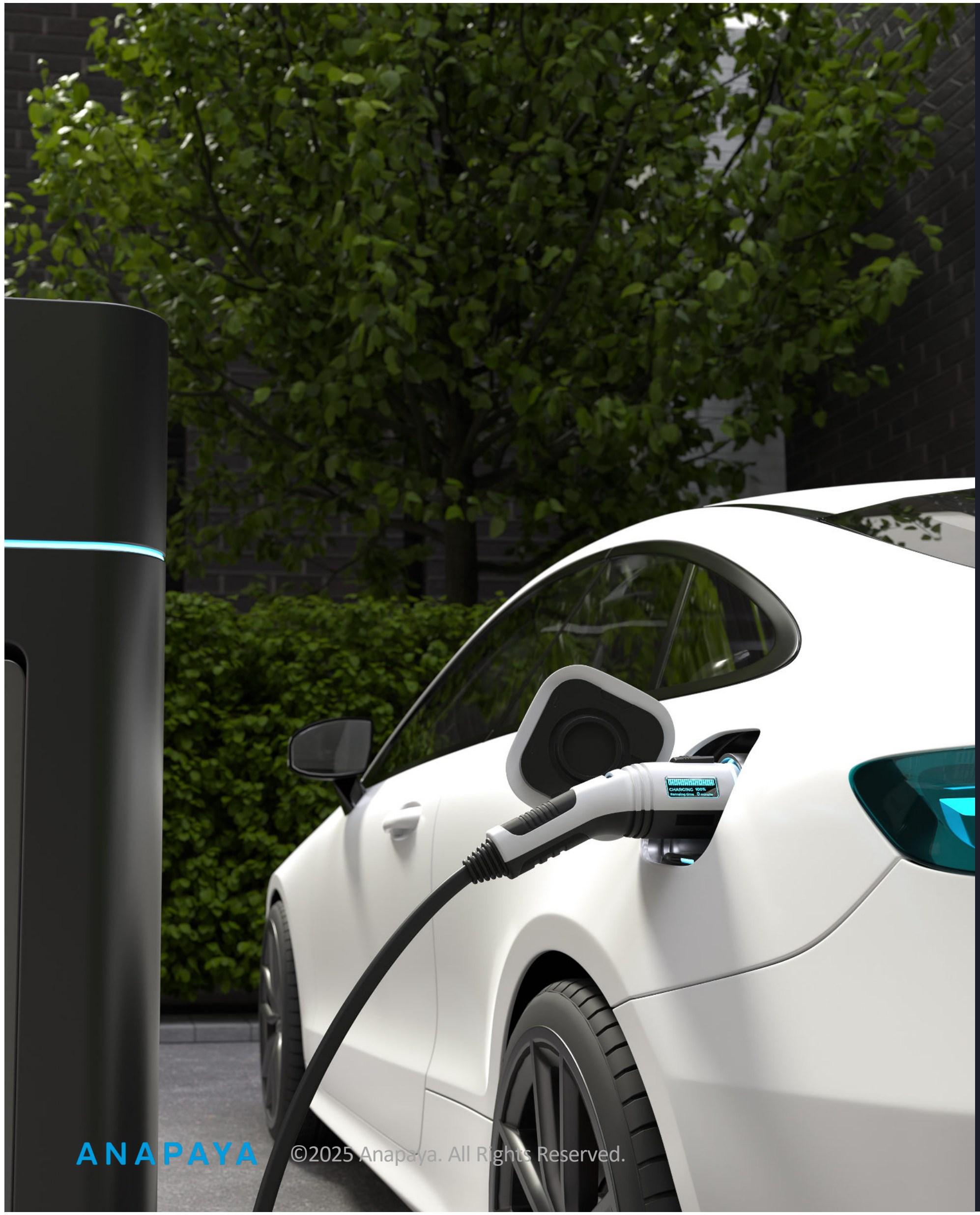


Real-time data access

Cloud-based AI delivery

Inter-connected ecosystems

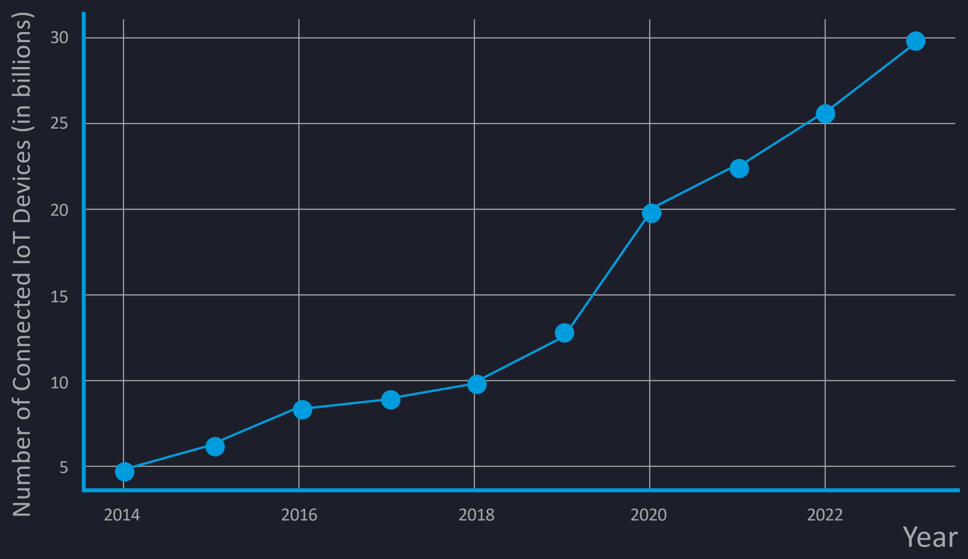
Compliance and data security



Internet of Things (IoT) dangerous growth factor

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

Growth of Connected IoT Devices Over the Last 10 years



Source: IoT Analytics, Statista

DDoS attacks have been increasing in frequency
The Internet eats itself…

Midway through 2025, Cloudflare has already detected

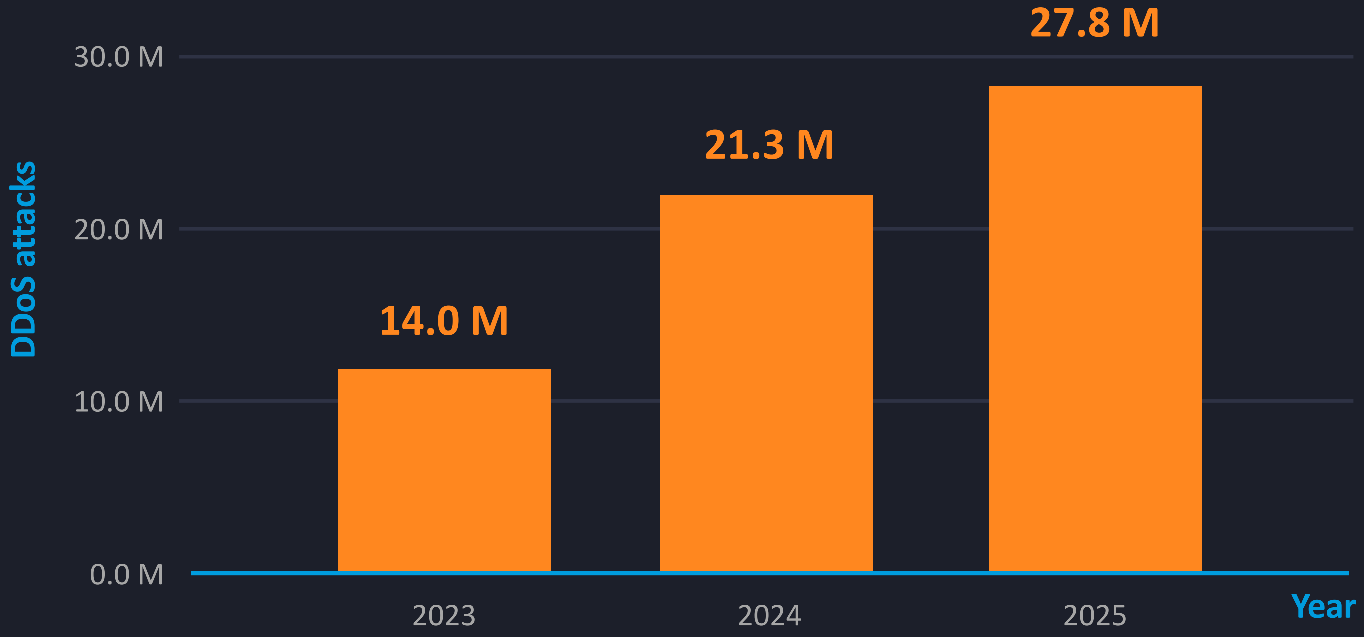
27.8 million DDoS attacks

equivalent to

130%

of DDoS attacks in 2024

DDoS attacks by year

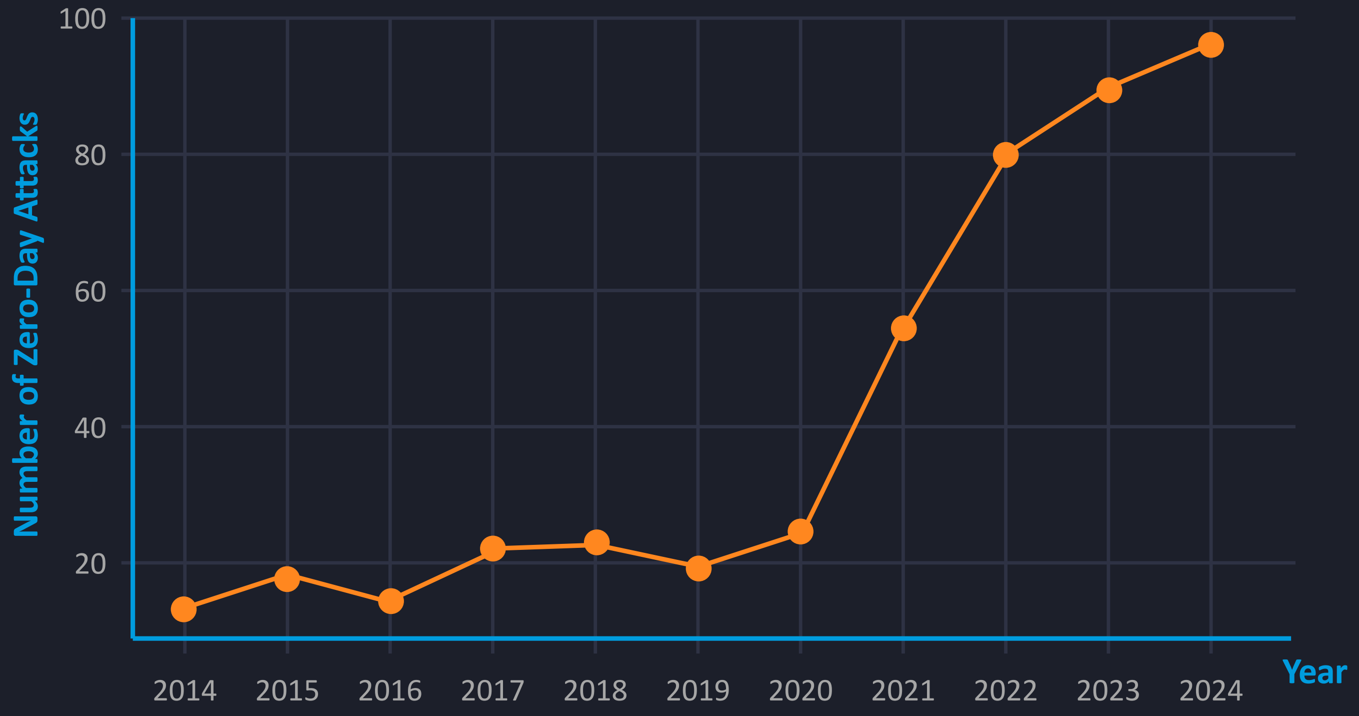


Sources: Cloudflare’s 2025 Q2 DDoS threat report

ANAPAYA

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

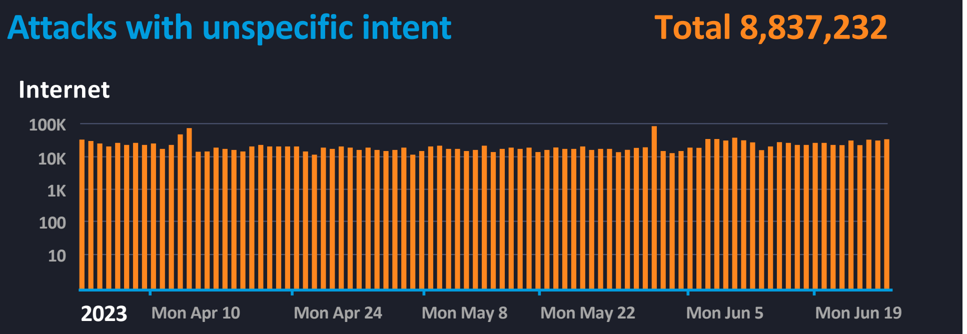
Reported
Worldwide
Zero-Day Attacks
(2014-2024)

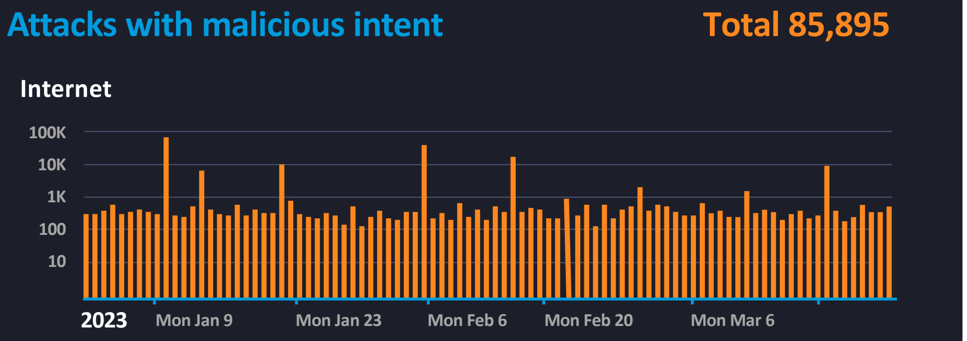


Sources: Google Project Zero, Mandiant, Symantec

ANAPAYA

An Internet service sees 30k scans / 1k attacks x day!





ANAPAYA

Fingerprinting Attacks resulting in highly efficient and effective attacks on disclosed Zero-day vulnerabilities

2024:

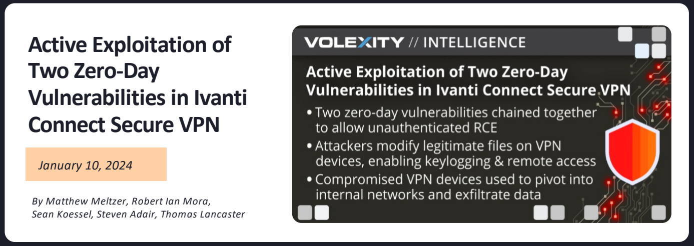
Continued security issues and attacks affecting numerous organizations and users.

- **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.

1 VPN Zero day -> 1’700 compromised enterprises in 5 days

January 10 2024

A zero-day vulnerability on Ivanti remote access product is discovered…



Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

January 10, 2024

By Matthew Meltzer, Robert Ian Mora, Sean Koessel, Steven Adair, Thomas Lancaster

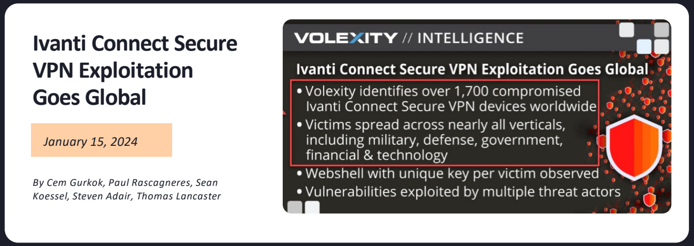
VOLEXITY // INTELLIGENCE

Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

- Two zero-day vulnerabilities chained together to allow unauthenticated RCE
- Attackers modify legitimate files on VPN devices, enabling keylogging & remote access
- Compromised VPN devices used to pivot into internal networks and exfiltrate data

January 15 2024

In 5 days, at least **1,700 corporates** were reported to be compromised!



Ivanti Connect Secure VPN Exploitation Goes Global

January 15, 2024

By Cem Gurkok, Paul Rascagneres, Sean Koessel, Steven Adair, Thomas Lancaster

VOLEXITY // INTELLIGENCE

Ivanti Connect Secure VPN Exploitation Goes Global

- Volexity identifies over 1,700 compromised Ivanti Connect Secure VPN devices worldwide
- Victims spread across nearly all verticals, including military, defense, government, financial & technology
- Webshell with unique key per victim observed
- Vulnerabilities exploited by multiple threat actors

ANAPAYA

Growing size of the Internet and AI based attacks are resulting in more Zero-day’s…

2024:

Continued 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: Q1 2025 (Jan–Mar)

- **Ivanti Connect Secure / Policy Secure / ZTA — CVE-2025-0282**
  Unauth stack buffer overflow → RCE. Zero-day exploitation observed mid-Dec 2024; disclosed **Jan 8**. Google Cloud+2Ivanti Community+2
- **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**. security.paloaltonetworks.com+2GreyNoise+2
- **Fortinet FortiOS / FortiProxy — CVE-2025-24472** *(edge case but widely reported as exploited)*
  CSF proxy auth bypass → super-admin under specific conditions; multiple advisories flagged **active exploitation** in **Feb**. NVD+2fortiguard.com+2

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

2024:

Continued 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: Q2 2025 (Apr–Jun)

- **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. TechRadar+4Rapid7+4Ivanti Community+4
- **Citrix NetScaler ADC / NetScaler Gateway — CVE-2025-6543**
  Pre-auth memory overflow (Gateway/AAA) → control-flow/DoS; **added to KEV Jun 30** for active exploitation. CISA+2NVD+2

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

2024:

Continued 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: Q3 2025 (Jul–Sep)

- **Citrix NetScaler ADC / NetScaler Gateway ("CitrixBleed 2") — CVE-2025-5777**
  Pre-auth memory disclosure (Gateway/AAA) → session/credential leakage; active exploitation reported **early July**. watchTowr Labs+2Akamai+2
- **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**). Tenable®+3Citrix Support+3Rapid7+3

ANAPAYA

SCION – the next Generation Internet - solving the root causes

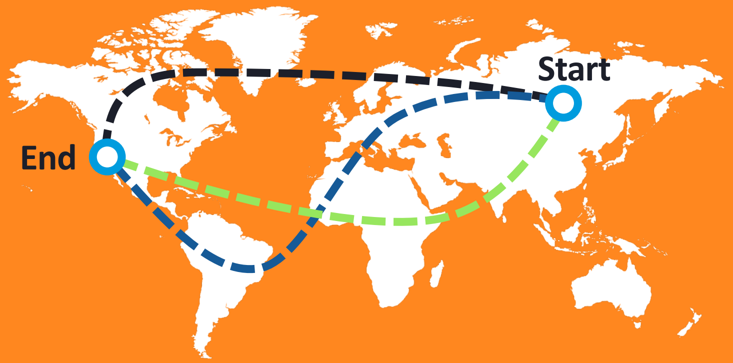
Governance: Control the exact route your data will travel

Security: Be in control who gets the routing information to your service

Resilience: Use several paths at the same time for one session

The Internet

Traveling with a compass.



VS

The SCION Internet

Traveling with a GPS.

ANAPAYA

SCION didn’t happen over lunch

2012

SCION research started at ETH Zurich

2017

Founding of Anapaya Systems AG to deliver SCION to the market

2019

The Swiss National Bank (SNB) and SIX embark on building the Secure Swiss Finance Network (SSFN)

2020

Successful pilot of the SSFN with ZKB, UBS, SIX, Raiffeisen

2021

- SSFN go-live for >300 Swiss financial institutions;
- Government projects go-live

2022

HIN Trust Circle is ready

2023

Anapaya GATE achieves 100% SCION coverage in Switzerland

2024

Finance IPNet to be decommissioned by end of September and replaced by SSFN

Our co-founder

"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 of ETH Zurich
Department of Computer Science, Institute of Information Security, The Network Security Group

SCION Ecosystem

axpo, BT, BICS, colt, cyberlink, eraneos, EveryWare

Extreme networks, GÉANT, InfoGuard SWISS CYBER SECURITY, INFOSEC GLOBAL, LG U+

proximus NXT, Sunrise BUSINESS, swisscom, Switch, VARITY WE THINK IN POSSIBILITIES

SCION: Full coverage in CH & expanding internationally

axpo

cyberlink

Sunrise BUSINESS

swisscom

SWITCH

vtx

BT

bics

colt

GÉANT

InterCloud

LG U+

Megaport

odido

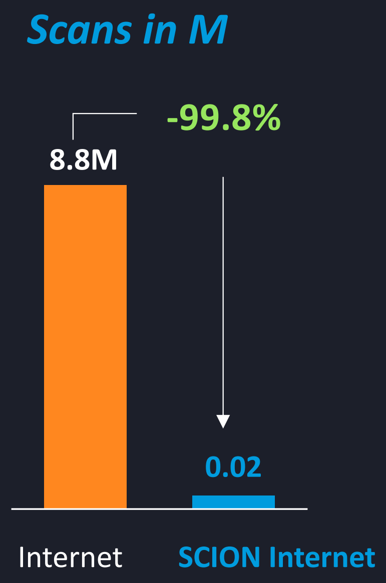
proximus NXT

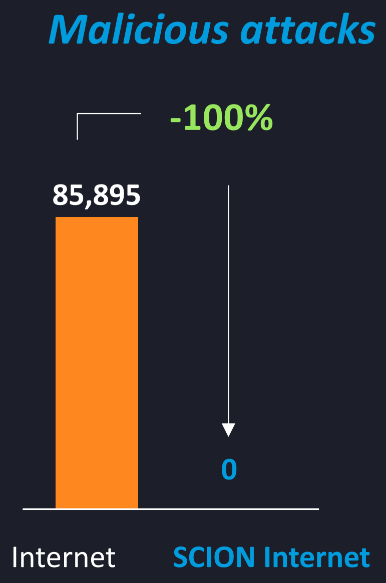
ANAPAYA

Get control back with SCION

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

Measured & Proven


Scans in M


Malicious attacks

Hear it from the industry leaders themselves

Financial services

“With SCION, we have achieved the desired resilience against cyberattacks.”

William Boye | *Head of Network Services*

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

UBS

HSBC

SIX

RAIFFEISEN

Zürcher
Kantonalbank

Government / Defense

“SCION offers more control and security. The innovation ecosystem around SCION is unique.”

Dr. Vincent Lenders| *Head of Cyber-Defense Campus*

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee
Armée suisse
Esercito svizzero
Swiss Armed Forces

RUAG

armasuisse

Healthcare

“SCION renders our connections invisible, away from malicious actors.”

Urs Fischer| *Head of Innovation*

HIN

Kantonsspital
Graubünden

Anapaya’s channel and technology partners

axpo

aws

BT

colt

Extreme
networks

eraneos

InterCloud

GÉANT

proximus NXT

tcs TATA CONSULTANCY SERVICES

vtx

swisscom

Sunrise

ANAPAYA

SCION: the Internet for critical infrastructure

SSFN: Secure Swiss Finance Network

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

> 2.5 Mio transaction/day

> 500B EUR volume / day

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.

Source: The Swiss Interbank Clearing (SIC) payment system Report on the SIC System and Disclosure Report 2022

ANAPAYA

www.anapaya.net

ANAPAYA

Martin Bosshardt

CEO, Anapaya Systems AG

Experience:

ABB BERGHUUS Radons EQT eevolve opensystems westhive Y&R GROUP SWITZERLAND

Education:

ETH zürich

Coolest personal accomplishment?

Building a scanning tunnel microscope to see atoms

Superpower?

Building an exciting and fun corporate culture