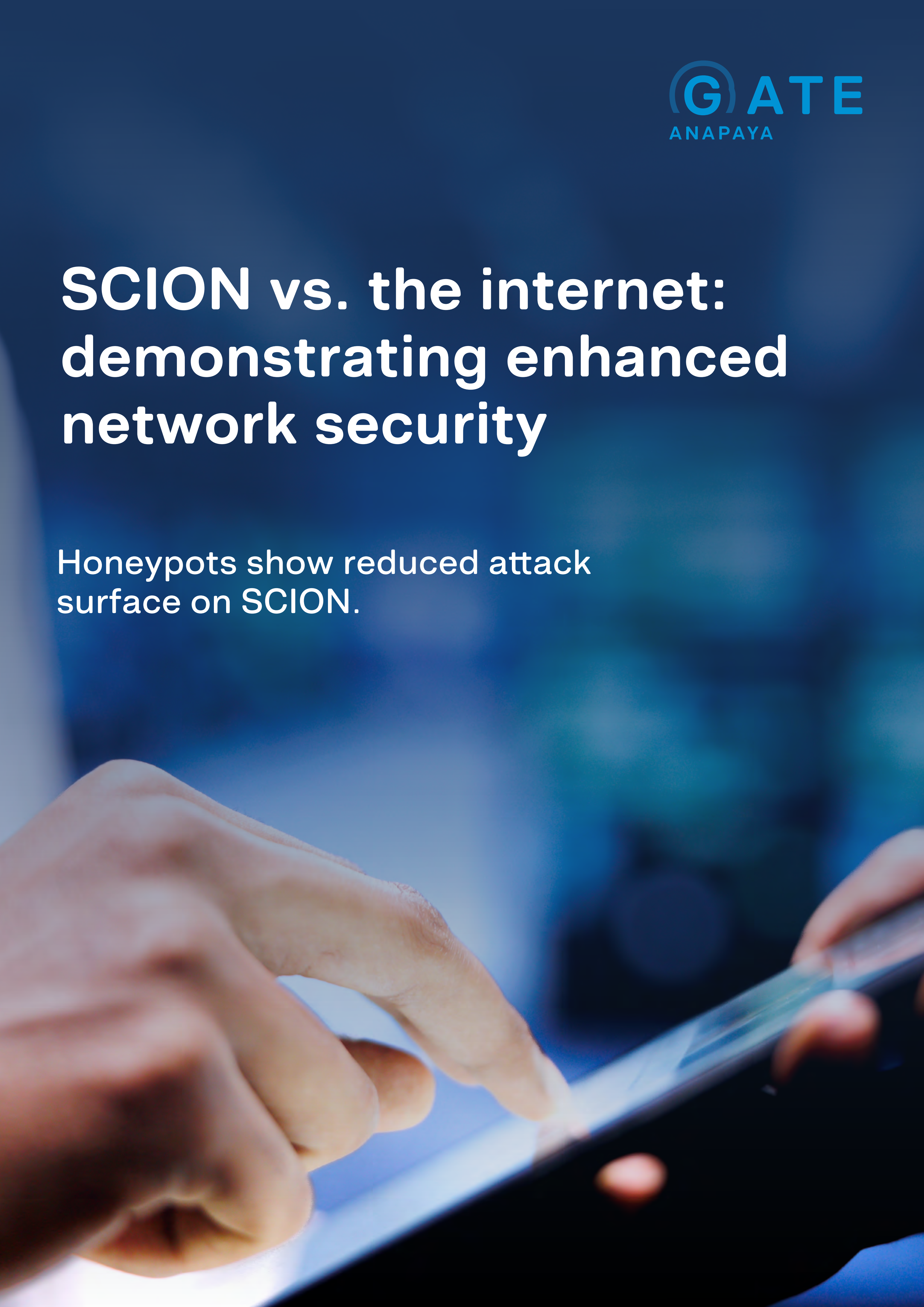
GATE
ANAPAYA

SCION vs. the internet: demonstrating enhanced network security

Honeypots show reduced attack surface on SCION.



Summary

This case study delves into the critical issue of cybercrime risk and the efficacy of network security, with a focus on the innovative SCION architecture. We explore real-time insights derived from honeypots, shedding light on the stark differences between the internet and SCION in attack surface risk. The findings show that on the SCION internet (hereafter SCION), the attack surface is smaller than on the internet.

This shows that deploying your service on SCION through Anapaya EDGE and permitting access exclusively to chosen ISPs and their users via Anapaya GATE can effectively prevent DDoS and intrusion attacks on your critical service.

The internet as the epicenter of cybercrime

In today's interconnected and highly digital society, we rely on the internet to advance our economy as well as our social lives. The influence of the internet touches on all aspects of modern business – ecommerce, smart infrastructure, supply chain management and hybrid workforces to name a few. As with any opportunity this vast, it exhibits the flip side of risk. In the case of the internet, which was developed four decades ago, the risk has grown along with the size of the network and is now massive. This brings us to an alarming number and variety of cyber security threats.

The Internet Society says so itself: *"systemic security issues about how traffic is routed on the Internet make it a relatively easy target for criminals. Criminals manipulate the ways in which traffic is routed on the Internet to launch attacks that bring down networks and services. Some attacks result in denial-of-service (DoS) that can damage both the reputation of affected organizations and their ability to conduct business operations."*

Business case backdrop:

"Cybercrime has the potential to affect half the world's population, as half the world has access to the internet. The internet is the backbone of cybercrime."

Ernesto Hartmann
Chief Cyber Defence Officer,
InfoGuard AG

Let us zoom in on Switzerland, where InfoGuard - a Swiss cybersecurity firm - has seen a surge in cybercrime incidents since 2020 and noticed a pattern over the last 3 years; a startling increase in incidents resulting from network vulnerabilities.

Every device or user connected to the internet is a potential entry point into networks for malicious actors.

Today's targets:

Business services

IoT services

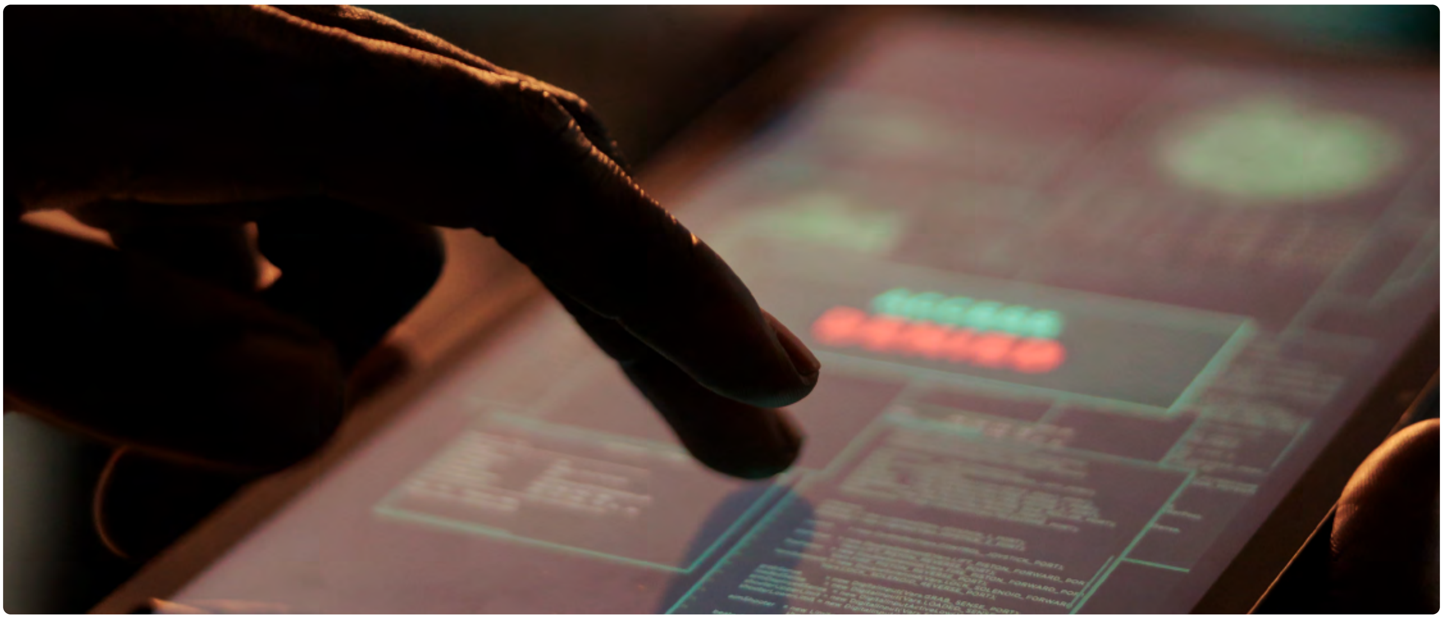
Web services and apps

With the increasing significance of home office or hybrid work culture, we have more and more remote workers and remote services such as VPN or Citrix. All these services are interconnected via the internet. Same for smart infrastructure that, via billions of IoT devices, captures and transmits sensitive data over the internet and whose disruption can cascade across other interconnected systems. Other familiar scenarios include online shopping, e-payments and many other day-to-day activities happening on the web. These websites and apps become a target precisely because they live on the internet.

The attack surface of services connected to the internet is massive.

Attack surface explained

IBM defines it this way: "An organization's attack surface is the sum of vulnerabilities, pathways or methods – sometimes called attack vectors – that hackers can use to gain unauthorized access to the network or sensitive data, or to carry out a cyberattack."



In 2022, Gartner highlighted the expanding attack surfaces of enterprises, driven by risks associated with cyber-physical systems, IoT, open-source code, cloud applications, digital supply chains, and social media. IBM further validates this, noting that as organizations embrace cloud services and hybrid work models, their networks and associated attack surfaces are growing in size and complexity.

In Switzerland as well, InfoGuard reports that out of all the incidents they processed in 2022, 40% of them resulted from exploited vulnerabilities in systems connected to the internet.

“Most criminal actors are opportunists, vultures. And the internet today is full of opportunities. What we have to look at now is that the risk of attack is getting bigger, and we are running out of time.”

Mathias Fuchs
InfoGuard VP Intelligence
and Investigation

The reduction of the attack surface is an effective way to limit the opportunities an attacker finds to target your service or network. Fortinet concluded that the smaller the attack surface, the easier it is to protect.

Companies need to be strategic with their service exposure and ensure their attack surface is as small and selected as possible.

Beware of DDoS and intrusion attacks

Cybercriminals leverage large attack surfaces of systems or services on the internet to launch intrusion and DDoS attacks – to compromise or steal data and to disrupt operations, respectively.

Statista reported that in 2022, companies in the United States faced network intrusion as the most prevalent form of cybercrime, constituting 45% of incidents. Similarly, in Switzerland during 2023, a Swiss bank encountered over 8 million scans and 35,000 malicious attacks within a quarter as recorded by Anapaya.

Distributed denial-of-service (DDoS) attacks disrupt the operations of a server, service, or network by flooding it with unwanted internet traffic. These attacks can shut down a website or entire networks for extended periods of time.

Globally, cybercriminals launched approximately 7.9 million DDoS attacks in the first half of 2023, representing a 31% year-over-year increase as announced by NetScout.

45%
network intrusion attacks
USA in 2022

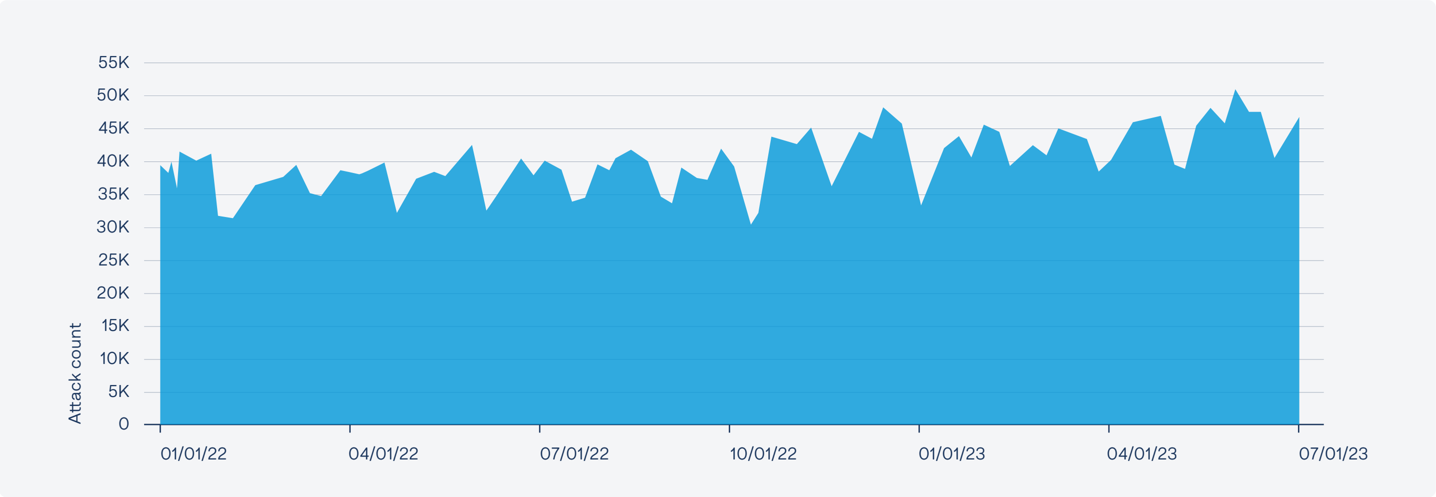
8M+
scans
Swiss bank stats in 2Q 2023

7.9M
DDoS attacks
1H of 2023 globally

150
Daily attacks
Switzerland in 2023

DDoS and intrusion attacks both benefit from a large attack surface.

Global daily attack count (2022-2023)



Source: NetScout Global Highlight 2023

Using honeypots to assess attack surface reduction

It is difficult to pinpoint a business's precise attack surface because you need a real-time awareness of available attack vectors, including vulnerability exploits – and even then, there may be unknown cracks in your network. But basically, the larger your attack surface the greater your risk.

Since reducing attack surface can exponentially reduce the risk of being attacked, InfoGuard decided to run a honeypot project to visualize the variation in attack surface risk between the internet and SCION.

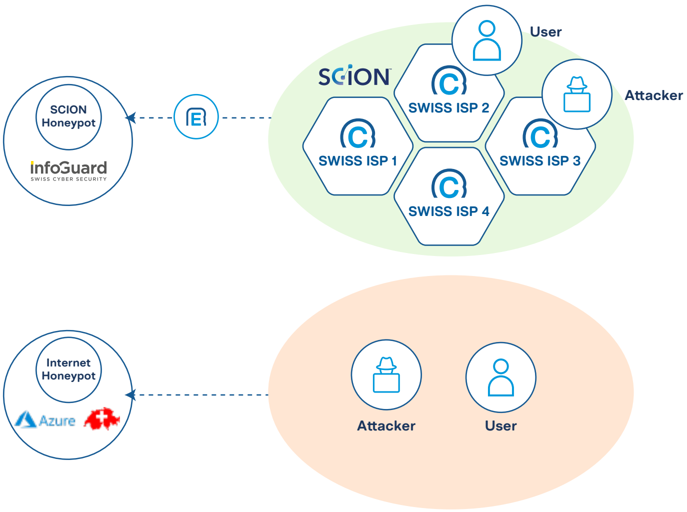
Question:
How much does the attack surface available to malicious actors change with respect to the network you are connecting to?

Time frame:
November – December 2023

Setup:
One honeypot on the internet and one on SCION with Anapaya EDGE and reachable only thorugh Anapaya GATE

About SCION

SCION is a new internet architecture developed at ETH Zurich that offers security, reliability and higher performance by giving data senders control over the path their data takes.



Network profiles:

- Public internet (cloud and Swiss network) – BGP protocol
- SCION on a Swiss ISD made of Swiss SCION-enabled internet service providers (ISPs) – SCION protocol

Honeypot results

The honeypots reflect the kind of crime that is happening on the internet right now and demonstrate that the service on SCION is more secure than on the internet.

Intrusion attempts on networks

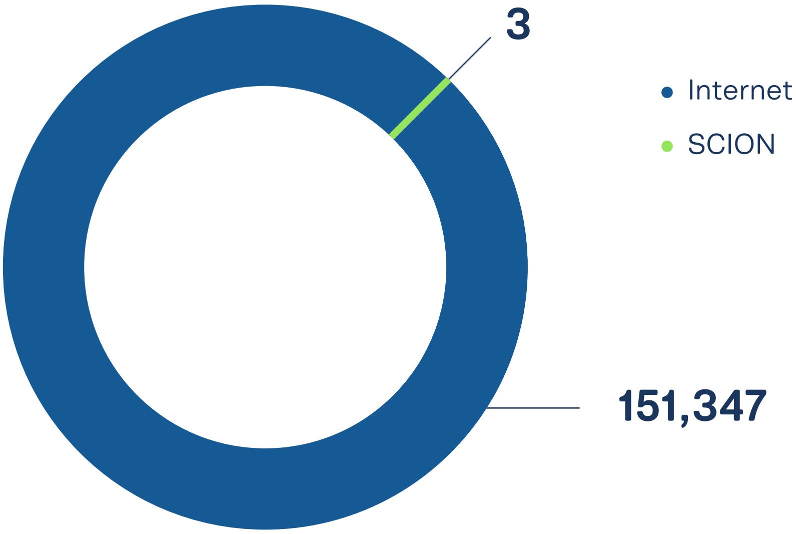
The attack surface on SCION is up to 99.9% smaller compared to the internet in the time frame measured.

3

intrusion attempts on the SCION honeypot

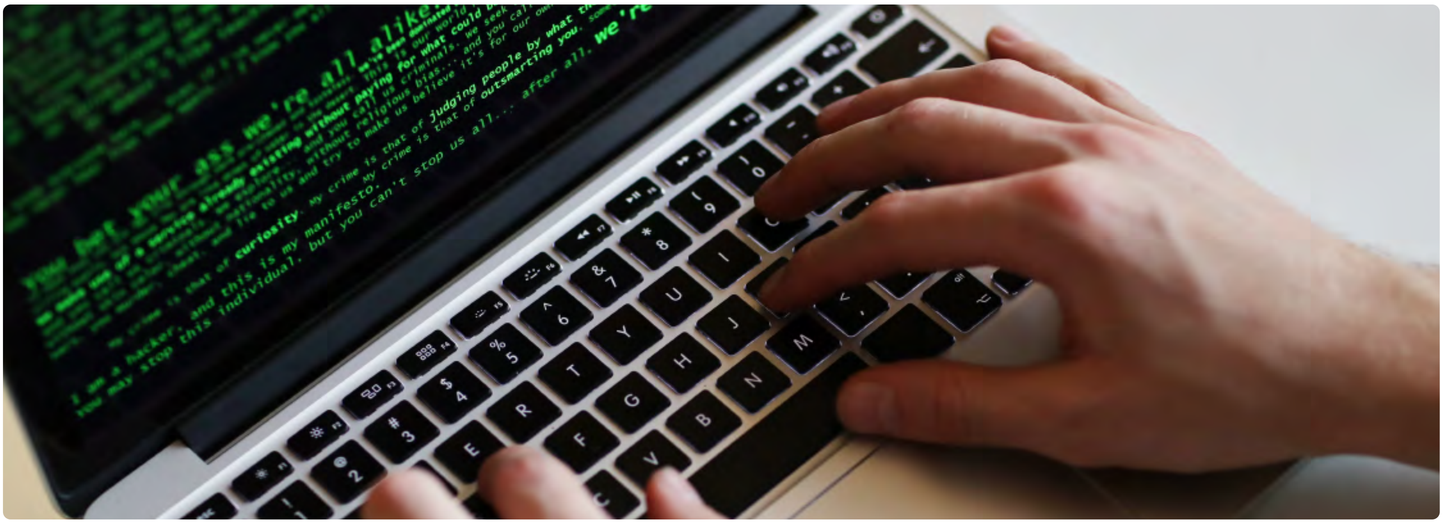
ca. 151,000

intrusion attempts on the internet honeypot



The SCION network faced intrusion attacks by actors most likely operating from within Switzerland.

Intrusion attempts on the honeypots Nov-Dec 2023

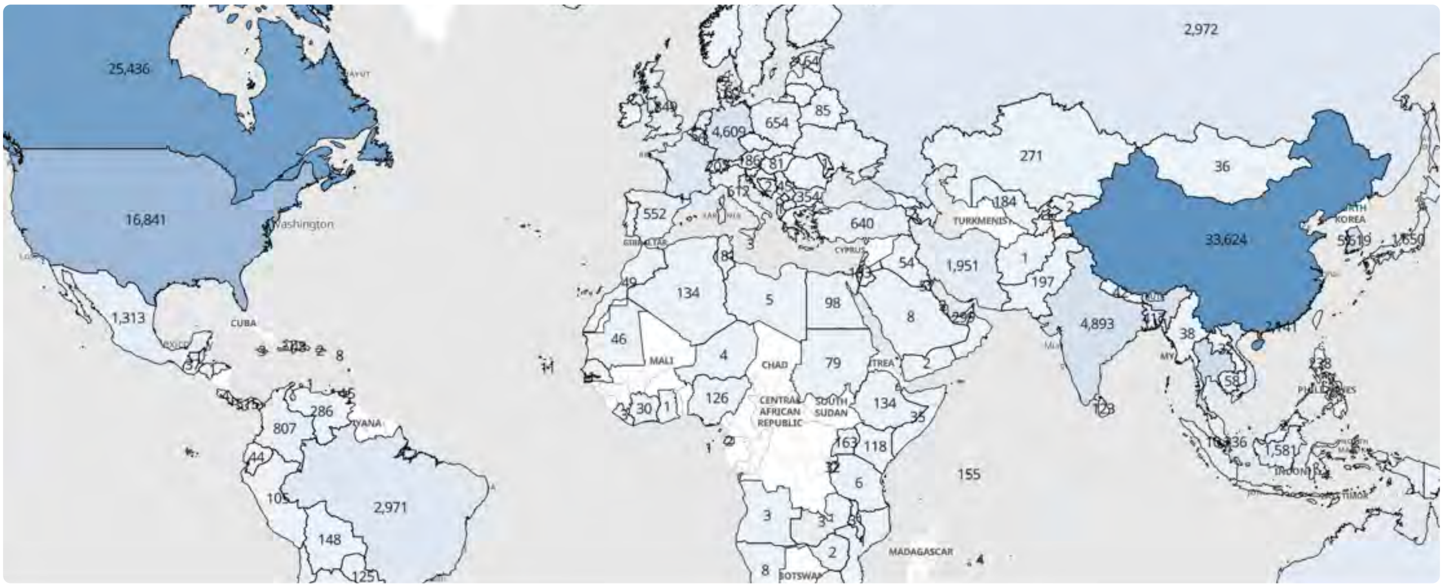


Intrusion attempts per country

Most of malicious activities' IP addresses originate from China, Canada, United States and Singapore.

207 IP
addresses originated in Switzerland

151,000+ IP
addresses came from elsewhere



Origin countries of the intrusion attempts (November - December 2023)

Key findings from the honeypots

On SCION:

The attack surface is up to
99.9%
smaller

Your critical service is
invisible
to the global internet

You can more
easily
identify, stop and prosecute bad actors

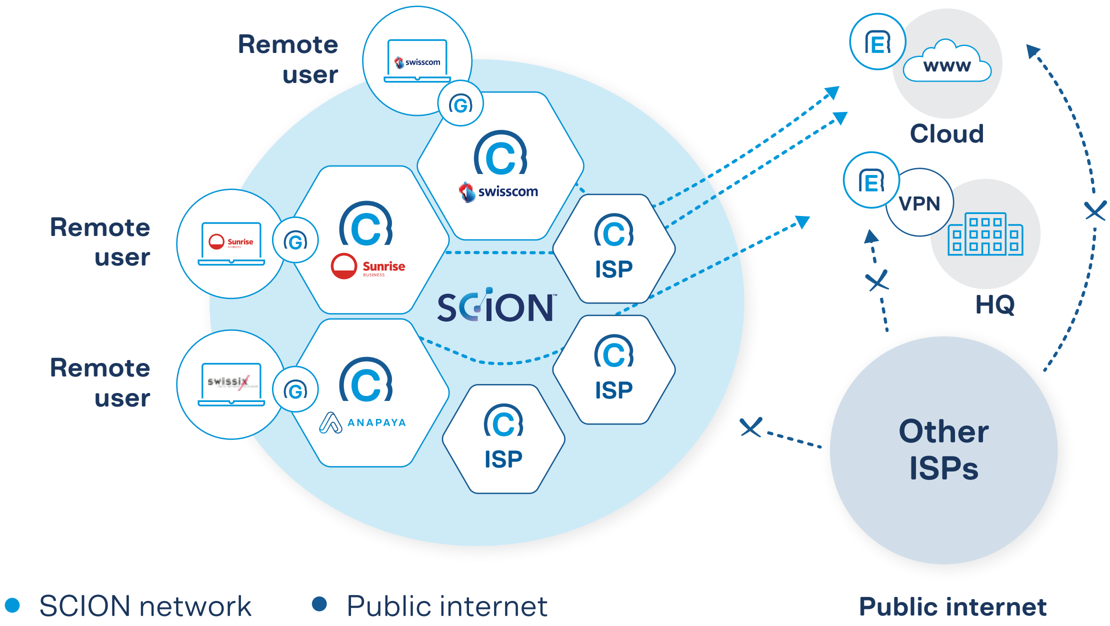
How to strengthen your network security

Strengthening your network security starts with minimizing the attack surface. You can secure your critical services within the SCION network – on a server or on the cloud - using Anapaya EDGE and allow access only to selected SCION-abled ISPs and their users via Anapaya GATE.

Anapaya GATE your attack surface is smaller and selected - what cannot be seen cannot be attacked.

This makes managing the risk of malicious attacks more economic and prioritizes your business continuity and data security.

SCION via Anapaya GATE is an ideal solution for securing home office applications and IoT services that do not require visibility on the global network. Similarly, for websites, the option to block access provides a protective measure against DDoS attacks, allowing you to confidently control and safeguard your web services – even during security threats – while continuing operations and avoiding incurring in financial losses. Anapaya GATE is a license-based model with no installation and 24/7 support, making it simple for you to adopt it.



Why is GeoIP filtering not enough?

GeoIP filtering may be a common method to limit the exposure of a service to a specific region – but it is not reliable. The reason is that GeoIP databases are not always accurate; due to unreliable data sources, IP address blocks being transferred from one entity to another and infrequent updates to those databases. Furthermore, GeoIP filtering often happens on the application layer when the traffic has already reached the service and thus does not protect the service from being overwhelmed by illegitimate traffic.

Why Anapaya GATE?

Whether your service is on a server or on the cloud, put it on SCION and reduce your attack surface risk. By announcing your path to only selected partners on SCION, you hide your service from the public internet. This is a simple and strategic way to prevent DDoS and intrusion attacks.

Sources:

- Internet Society, ISPs Should Strongly Consider MANRS to Fight Cybercrime: World Economic Forum Report
- Gartner, Gartner Identifies Top Security and Risk Management Trends for 2022
- InfoGuard, Honeypots Zeigen, Wie Unsicher Das Internet Ist – Und Wie Scion Das Angriffsrisiko Reduziert
- IBM, What is an attack surface?
- Fortinet, What Is An Attack Surface?
- Statista, Most common types of cyber attacks experienced by companies in the United States in 2022
- NetScout, Global Highlights
- Netscout, NETSCOUT Identified Nearly 7.9 Million DDoS Attacks in 1H2023 According to Its Latest DDoS Threat Intelligence Report

ANAPAYA

Secure your VPN, IoT service or website with Anapaya GATE

Your service
Always on. Always secure. It’s that simple.

Book a demo today!

www.anapaya.net