ANAPAYA

Scaling the SCION Revolution Globally

Martin Bosshardt

CEO, Anapaya

SCION Association Board Member

The Internet - the most powerful, most used, most attacked, fastest growing network – for critical applications

- *Internet keeps growing at an ever-increasing pace while attacks are getting easier & cheaper to execute*

Swiss website hit by DDoS attack ahead of Zelenskiy video address

By **Reuters** | June 12, 2023 12:18 PM GMT+2 – Updated a year ago

- *With lack of alternatives, critical infrastructures have become dependent on the Internet*

- Financial services
- Energy
- Healthcare
- Gov. / Defense
- Transport
- Communication

ANAPAYA

20 major cyberattacks that targeted critical infrastructure in 2023 and 2024:

1. Colonial Pipeline Ransomware Attack (USA)
2. Water Treatment Plant Hack (USA)
3. Hospital System Ransomware (USA)
4. Energy Grid DDoS Attack (Global)
5. Railway System Hack (Germany)
6. Airport Cyber Breach (USA)
7. Healthcare System Attack (Australia)
8. Telecom Service Outage (Denmark)
9. Nuclear Plant Cyber Intrusion (USA)
10. Oil Refinery Cyber Attack (Middle East)
11. Transportation System Ransomware (Sweden)
12. Financial Institutions Hack (Kenya)
13. Gas Supply Chain Breach (Europe)
14. Defence Contractor Cyber Attack (USA)
15. Smart City Infrastructure Hack (China)
16. Healthcare Data Breach (UK)
17. Chemical Plant Malware Attack (Russia)
18. Electricity Grid Ransomware (South America)
19. Smart Grid Malware (USA)
20. Defence Infrastructure DDoS (Canada)

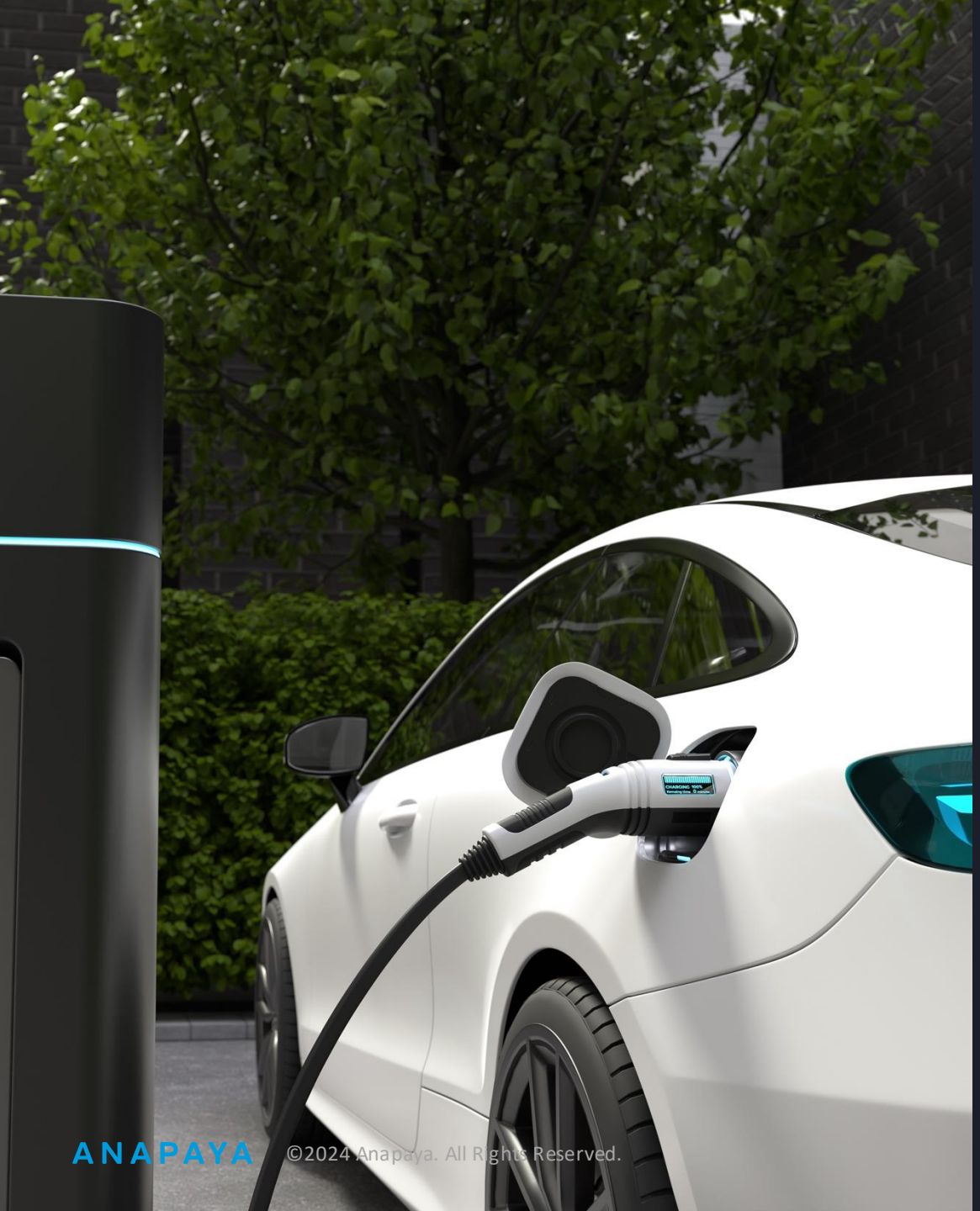
ANAPAYA

Source: Manufacturing.net, CSIS, Industrial Cyber

The gigantic unprotected and unregulated power plants in the cloud

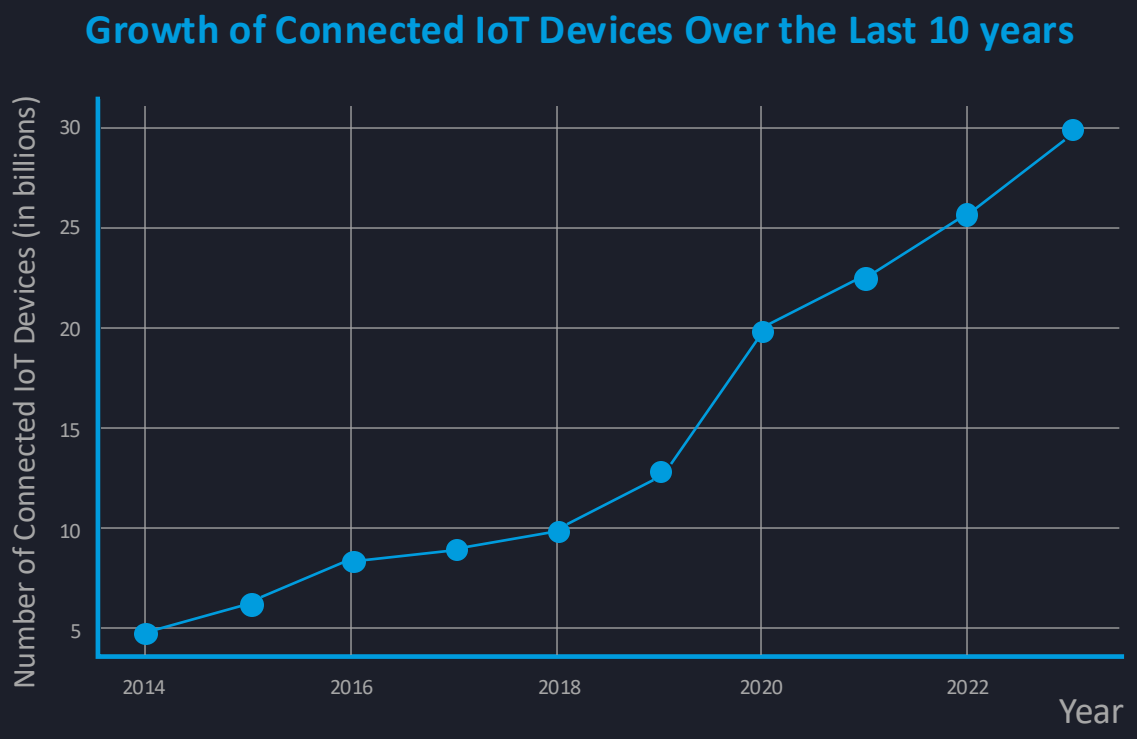
"Dutch hacker takes control of 4 million solar panel installations."

ANAPAYA



Internet of Things (IoT) dangerous growth factor

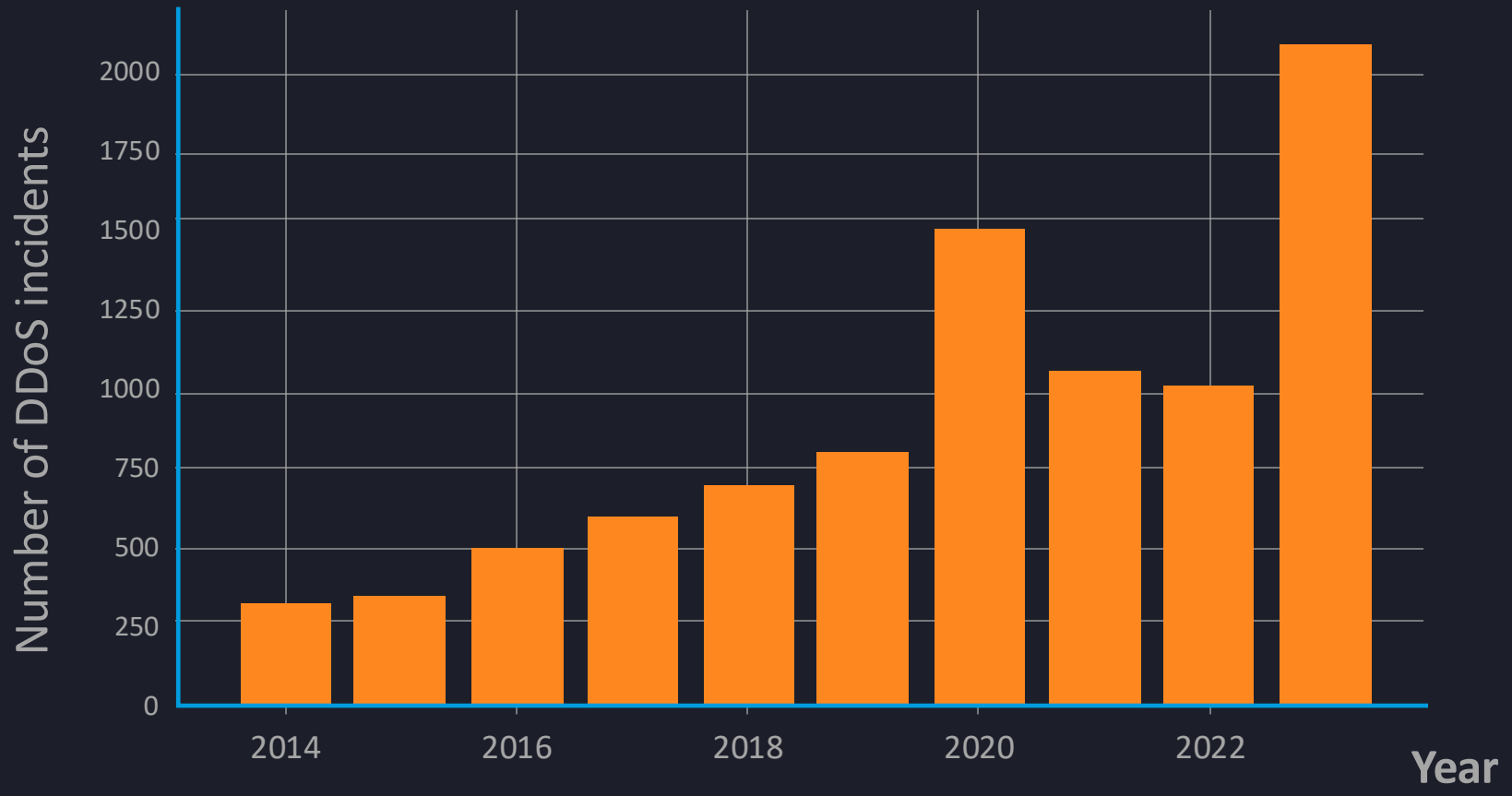
Charging stations, solar panels, wind turbines, heating units…



Source: IoT Analytics, Statista

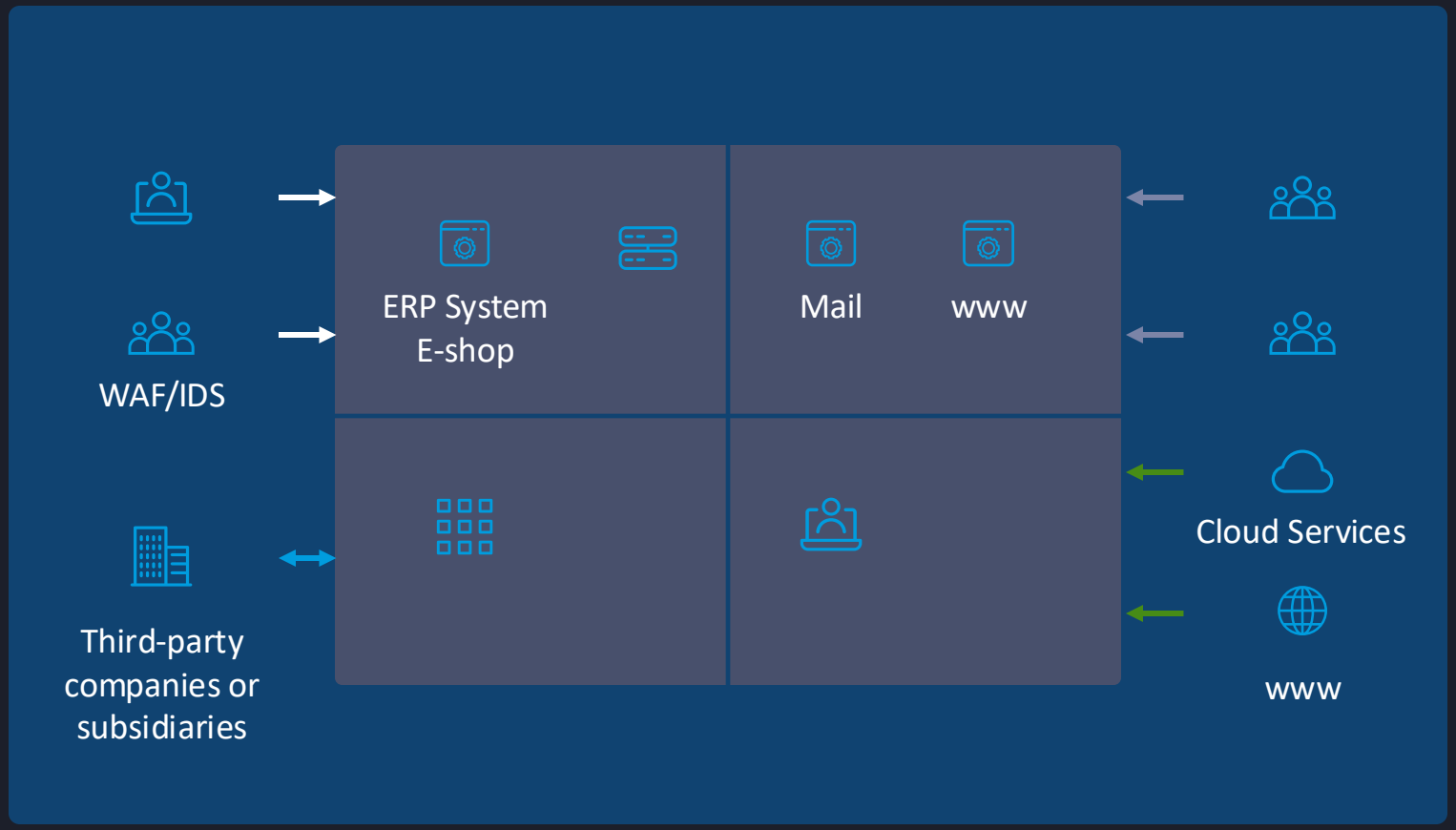
DDoS attacks have been increasing in frequency
The Internet eats itself…

DDoS Attacks
Over the Last
10 Years



Sources: Akamai, F5, Comparitech

Where and how are we attacked?



The four main service classes:

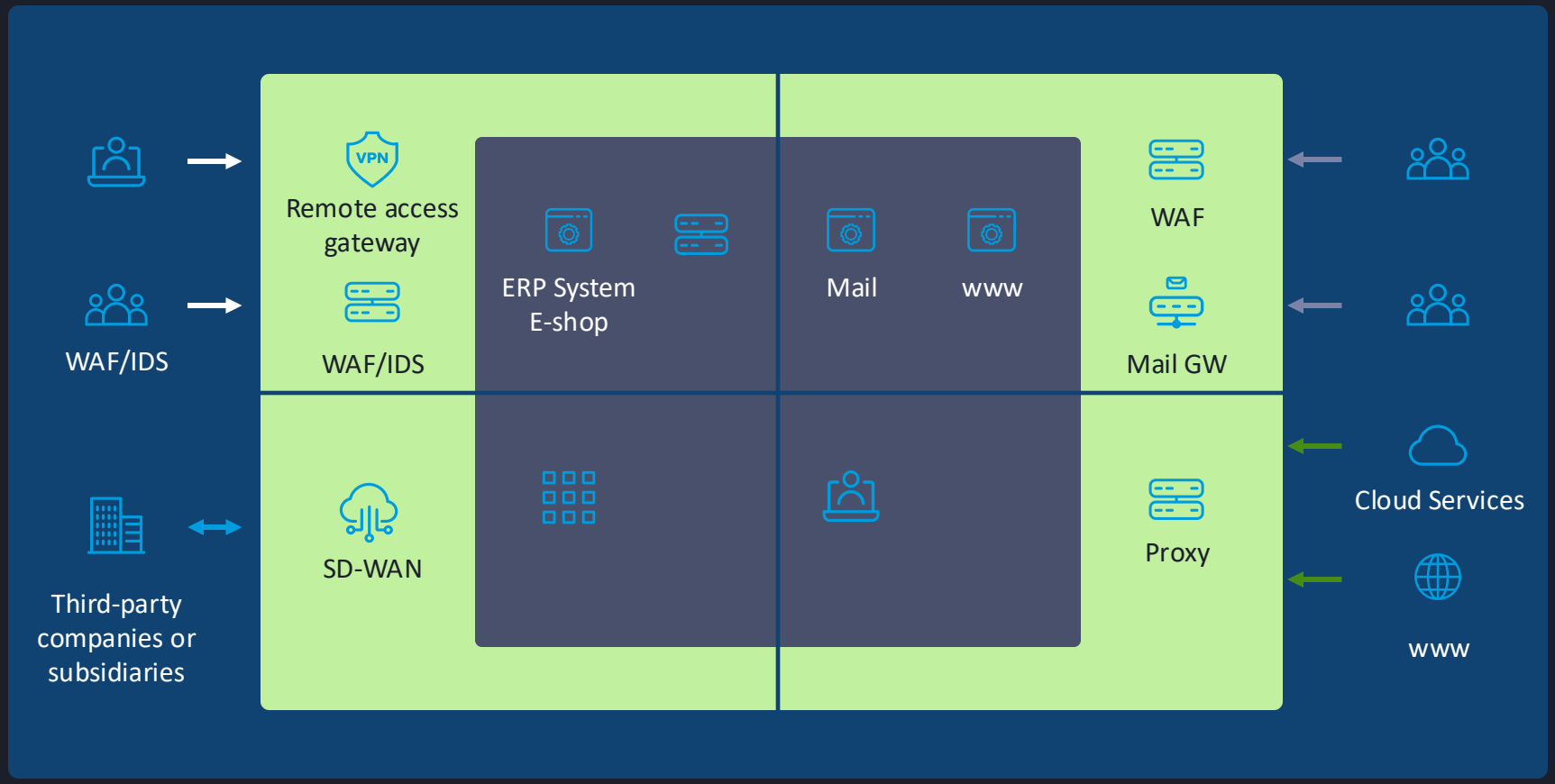
→ Incoming Connections
To **critical** services like an E-Shop or remote access for home office to an ERP system etc.

← Incoming Connections
to **non-critical** services like the corporate website.

↔ Isolated connections
using the Internet as a corporate network to connect subsidiaries or partner sites.

← Outgoing Connections
To use information websites, and cloud services, accessible through Internet connections

Attack Costs vs. Defence Costs – an unfortunate trend



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

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

2023:

Specific incidents:

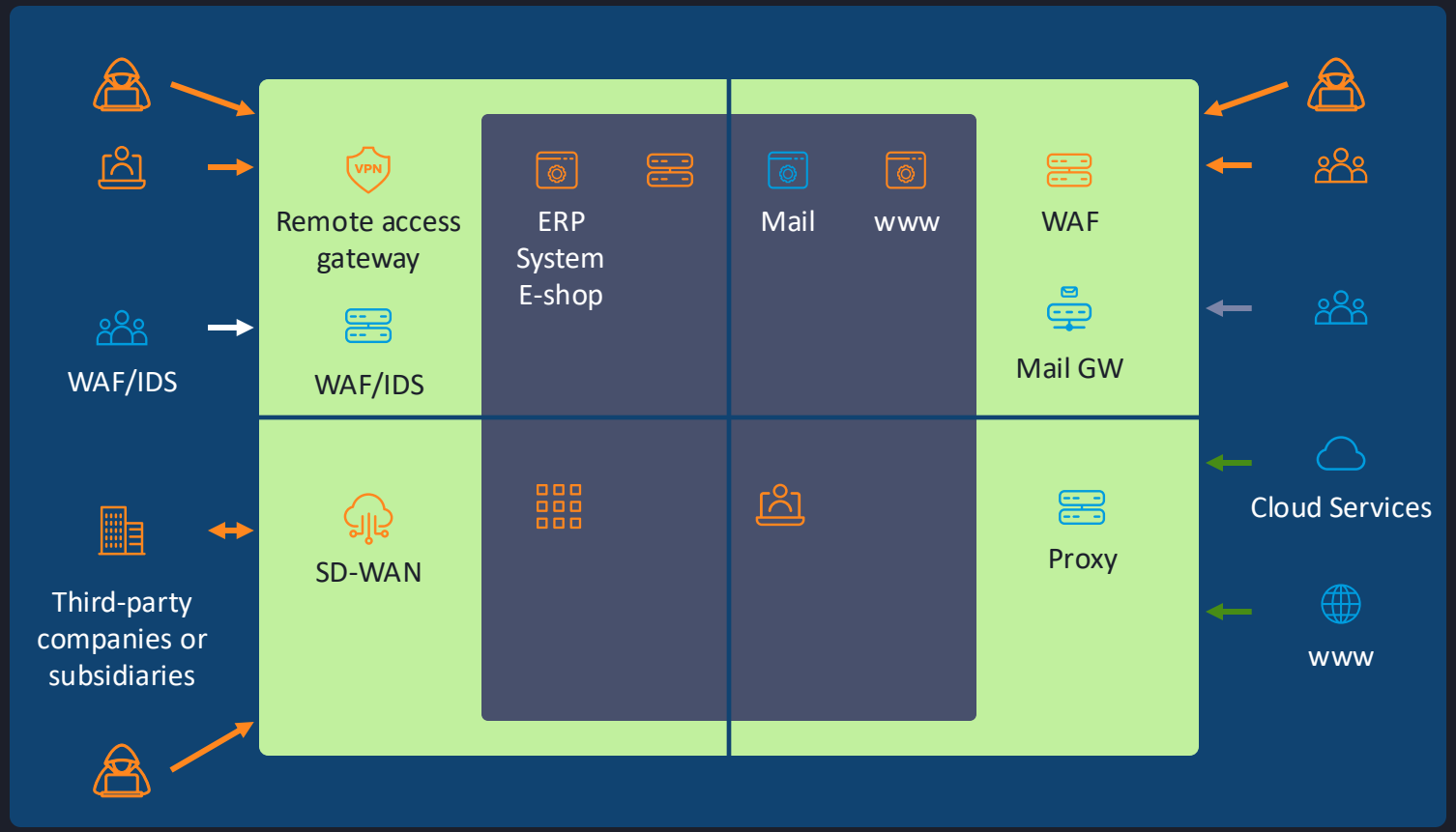
- **Cisco** ASA and FTD (CVE-2023-20269): Ransomware attacks, exact user count not specified.
- **Ivanti** VPN (CVE-2023-46805, CVE-2024-21887): Exploited by nation-state attackers, exact user count not specified.
- **Fortinet** FortiOS (CVE-2023-27997): Heap-based buffer overflow, exact user count not specified.

2024:

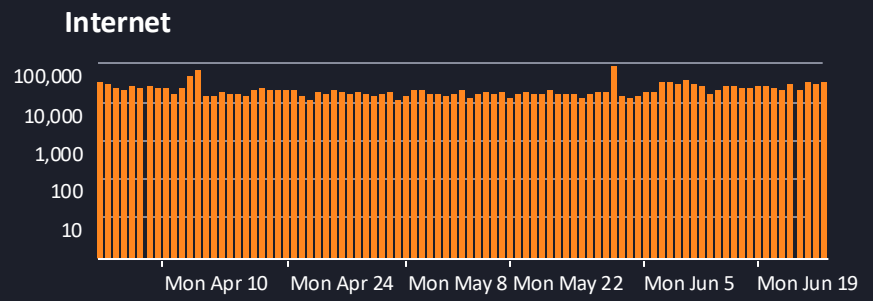
Continued security issues and attacks affecting numerous organizations and users.

- **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.

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

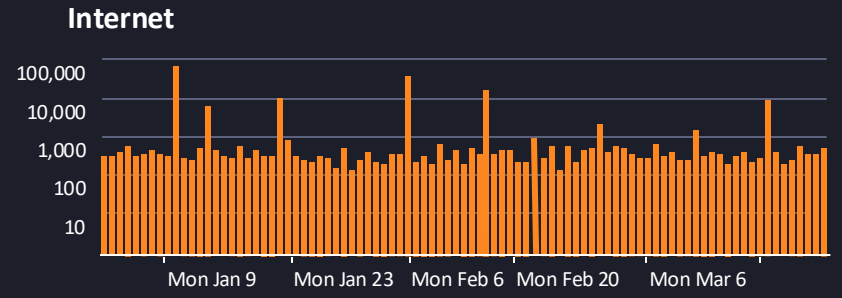


Attacks with unspecific intent



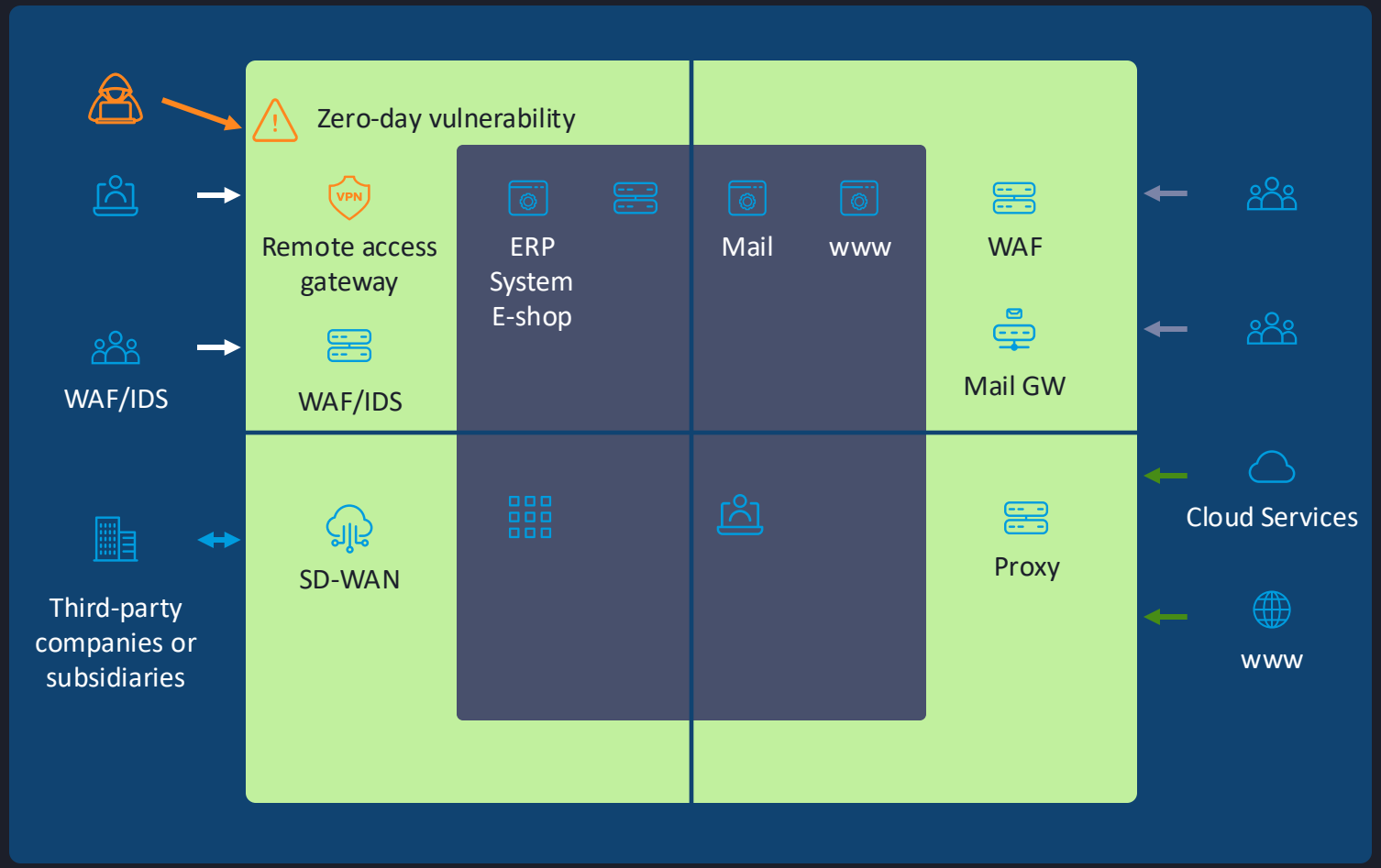
Total 8,837,232 2023

Attacks with malicious intent



Total 85,895 2023

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

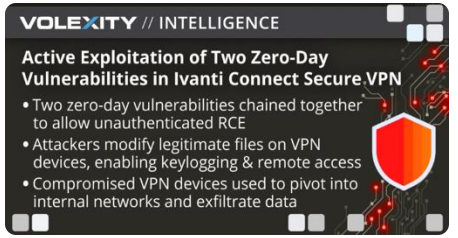


On **January 10th** 2024, a zero-day vulnerability on Ivanti remote access product is discovered…

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

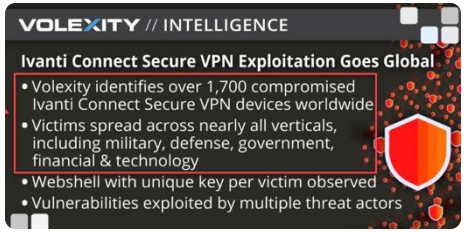


By **January 15th** at least **1,700 corporates** were reported to be compromised!

Ivanti Connect Secure VPN Exploitation Goes Global

January 15, 2024

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



Internet **Security Tech** **Corporation**

ANAPAYA

SCION – the next Generation Internet - solving the root causes

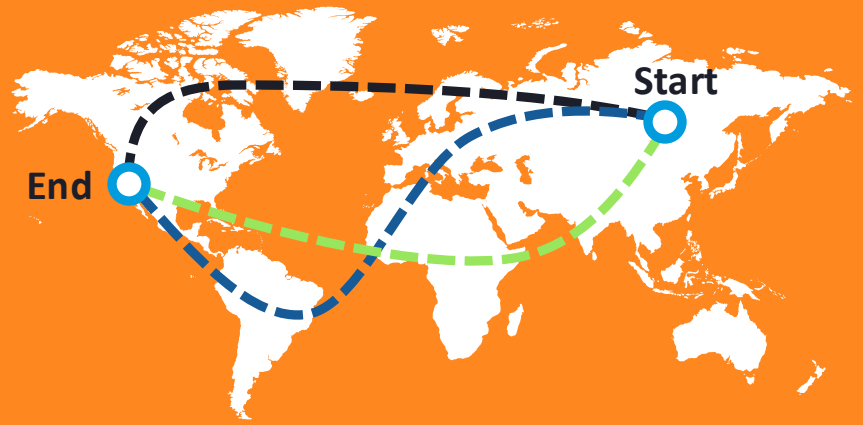
Governance: Control the exact route your data will travel

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

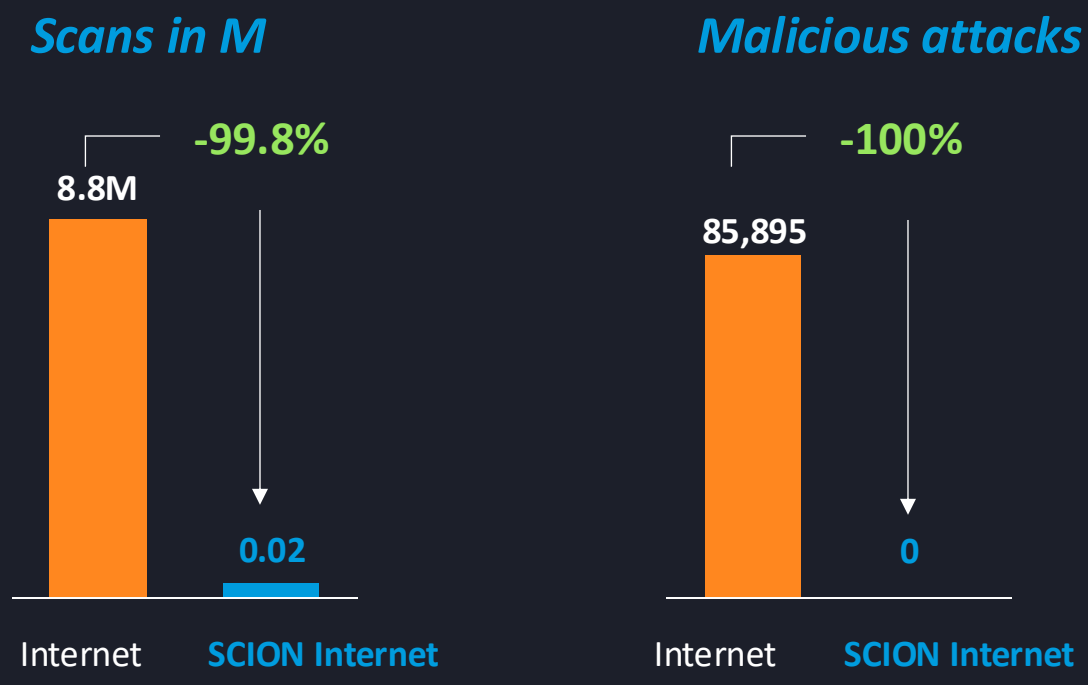
The SCION Internet

Traveling with a GPS.

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



SCION: Full coverage in CH & expanding internationally

axpo
cyberlink
Sunrise BUSINESS
swisscom
SWITCH
vtx

BT
colt
bics
InterCloud
GÉANT
LG U+
telindus

Benelux expansion driven by Anapaya in cooperation with BICS

- **10M**
  in Switzerland
- **40M**
  in Benelux

New partnership announcement

Carl Morris
CTO, BT Switzerland

Come say hi to the team!

Lukas Bischofberger
Head of Customer Success

Kyveli Mavromati
Customer Success and Software Engineer

David Carnal
Product Manager

Check out our Anapaya Console demo!

ANAPAYA