

# Angriff aus der Schattenwelt:

## Externe Schwachstellen durch Hackeraugen

**Halle 7 Stand 610**

Andreas Schmid

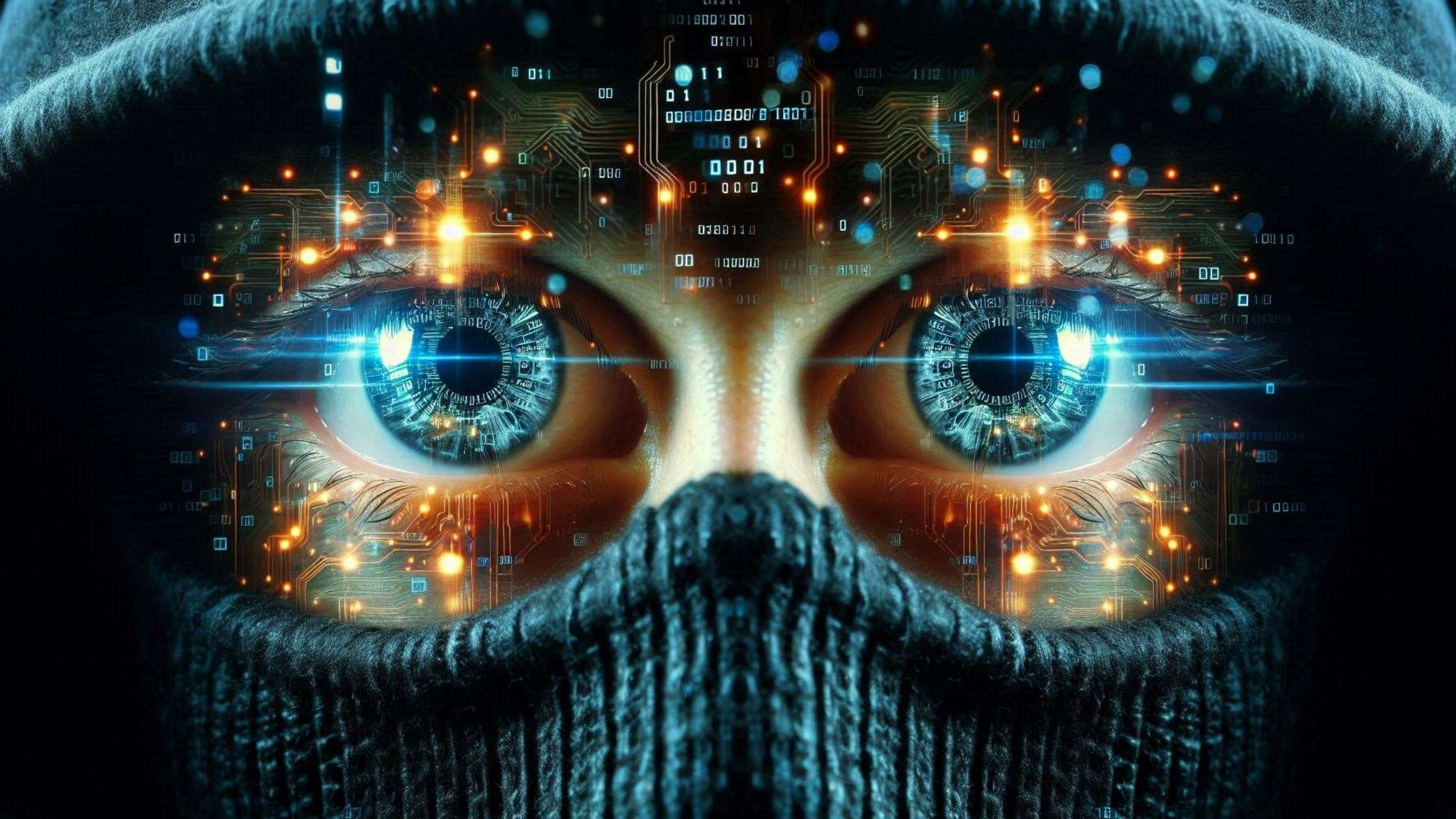
Director, Sales Engineering

[andreas.schmid@ivanti.com](mailto:andreas.schmid@ivanti.com)



**ivanti**







# Andreas Schmid

**Director Sales Engineering - EMEA Central**

Passionate golfer, hobby chef and world traveler.

More than 7 years with Ivanti and over 20 years know-how in Ivanti Solutions.



# Agenda

- **Attack surfaces expanding out of view**
- **External attack surface management (EASM)**
- **Product overview**
- **EASM use cases**

# **Attack surfaces expanding out of view**

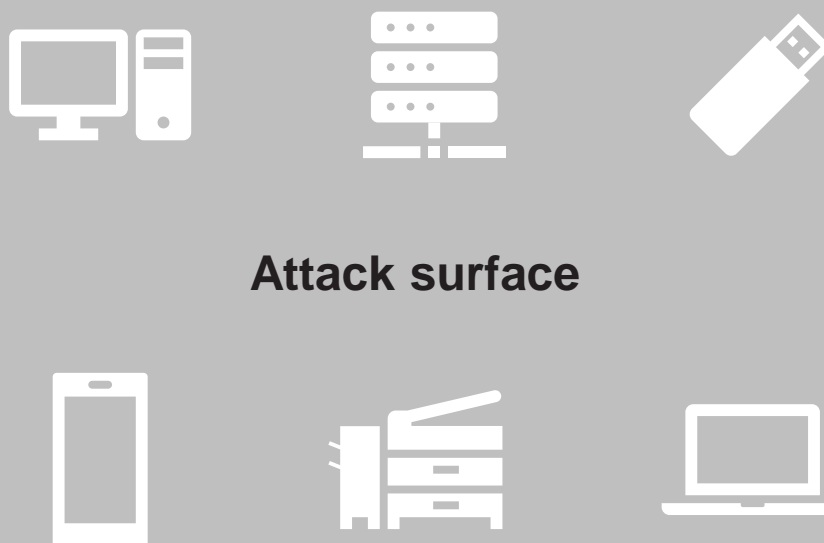
**Shadow IT**



**Cloud-based tools**



**Attack surface**



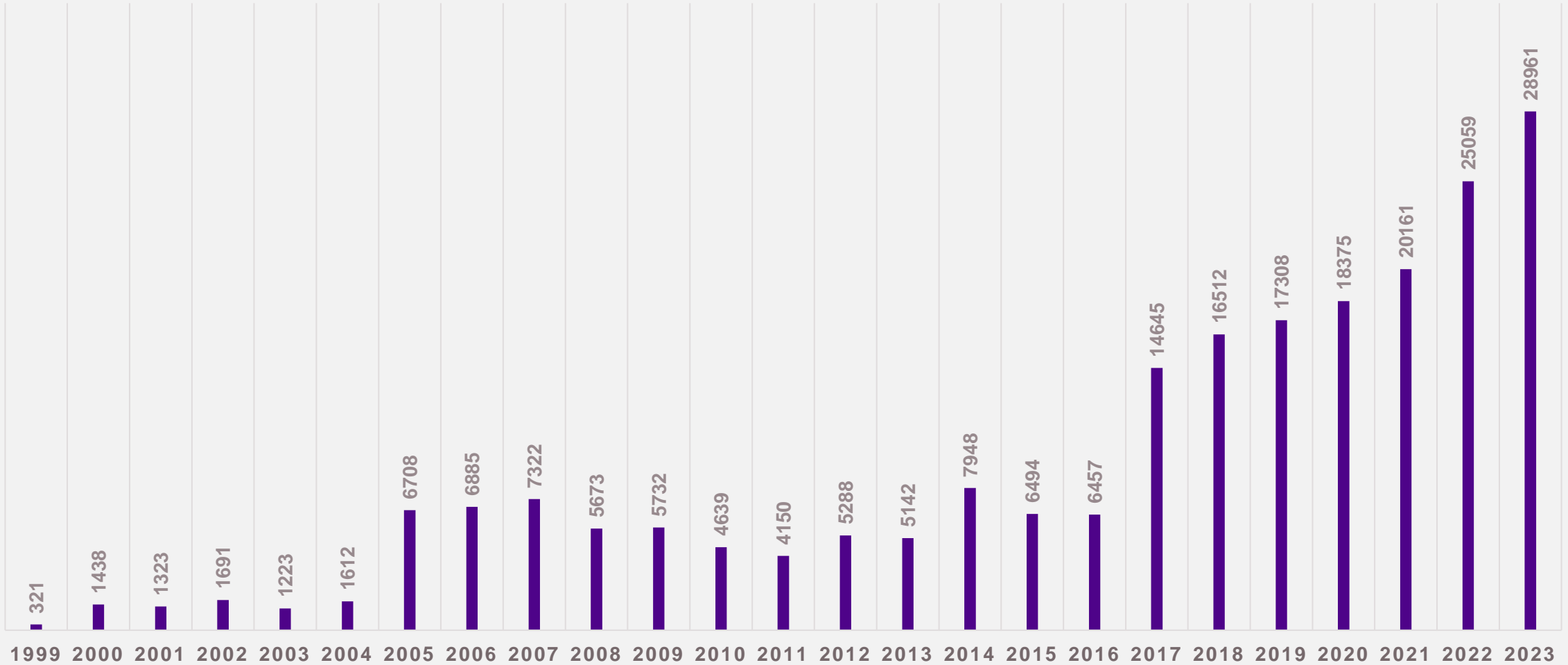
**Interconnected supply chain partners**



**IoT devices**



# CVEs by Year

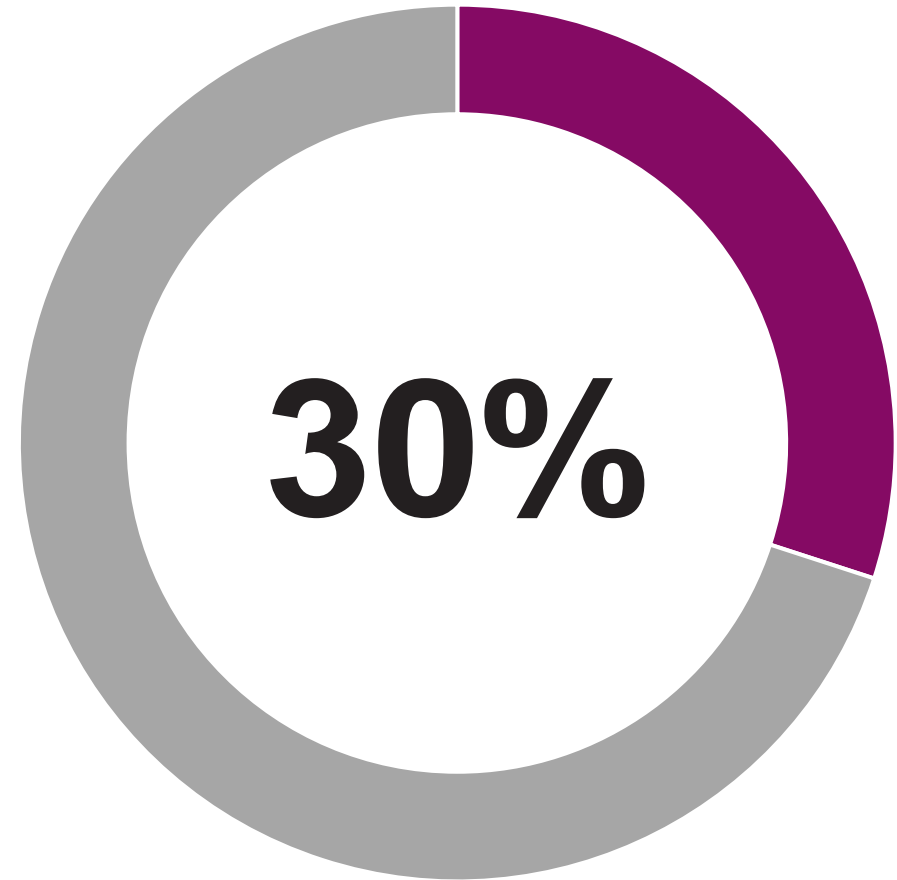


# **External attack surface management (EASM)**



# EASM effectiveness

On average, organizations using **EASM** tools discover 30% more assets than they knew they had.



# Ivanti Neurons for EASM



# Product overview

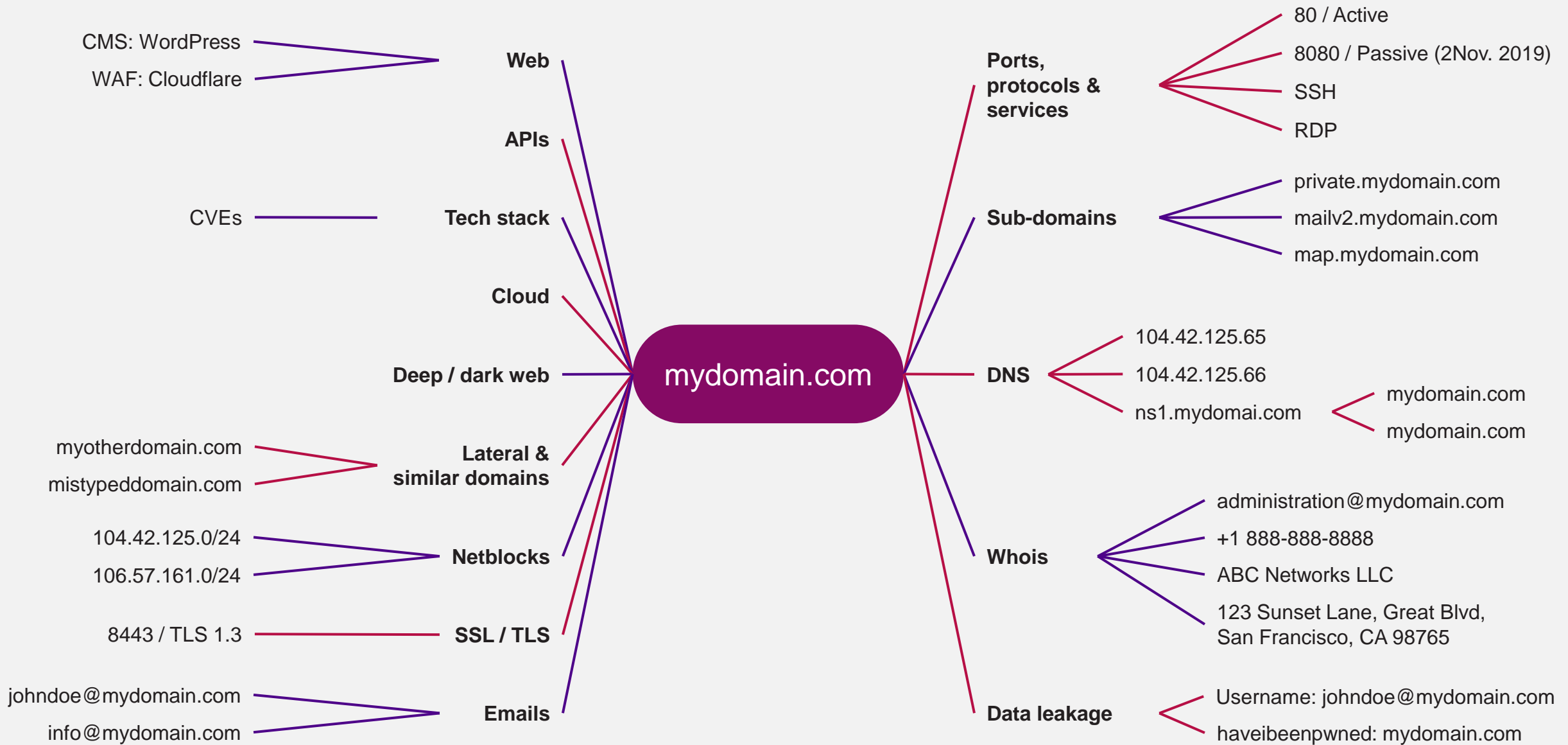
# Full visibility of internet-facing assets & exposures

## Asset types

- API
- Domain
- Host
- Netblock
- SSL certificate
- URL

## Exposure vectors

- Application security
- Data leaks
- DNS health
- Email security
- Network security
- Patching cadence
- Social engineering





# Actionable intelligence on exposures

The image displays a security dashboard with two main components. The background shows an 'Exposures' overview with metrics for 'Exposed internal assets' (36), 'High risk services' (236), and other categories. A table lists specific exposures, including CVE-2023-38408 with a VRS score of 9.29 and a severity of Critical. The foreground shows a detailed view of CVE-2023-38408, including its VRS Score (9.29), Severity (Critical), CVSS 3.0 (9.8), and CVSS 2.0 (10.0). It also lists impacted assets (1), threats (4), attack vectors, status (Open), publication date (Jul 19, 2023), age (71 days), first seen (Dec 21, 2023), last seen (Dec 21, 2023), and tags (Unclassified Exploit). The summary section describes the issue as a PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2, leading to remote code execution. Recommendations include patching and links to GitHub commits, release notes, and vendor advisories.

**Exposures**

36 ↑13 Exposed internal assets

236 ↑164 High risk services

3 →0 R/

5 ↑3

1 →0

2 ↑1

Resolve Export Filter

Exposure	VRS	Severity
<a href="#">CVE-2023-38408</a>	9.29	Critical
<a href="#">CVE-2014-0229</a>	8.98	High

Total 2265 exposures

## CVE-2023-38408

**VRS Score**  
9.29

**Severity**  
Critical

**CVSS 3.0**  
9.8

**CVSS 2.0**  
10.0

**Impacted Assets**  
1

**Threats**  
4

**Attack Vector**

**Status**  
Open

**Patching Cadence**

**Publication Date**  
Jul 19, 2023

**Age (Time of Exposure)**  
71 days

**First Seen**  
Dec 21, 2023, 8:51:23 AM

**Last Seen**  
Dec 21, 2023, 8:51:23 AM

**Tags**  
Unclassified Exploit

### Summary

**Securin ASM**

**Description**  
The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

**Recommendation**

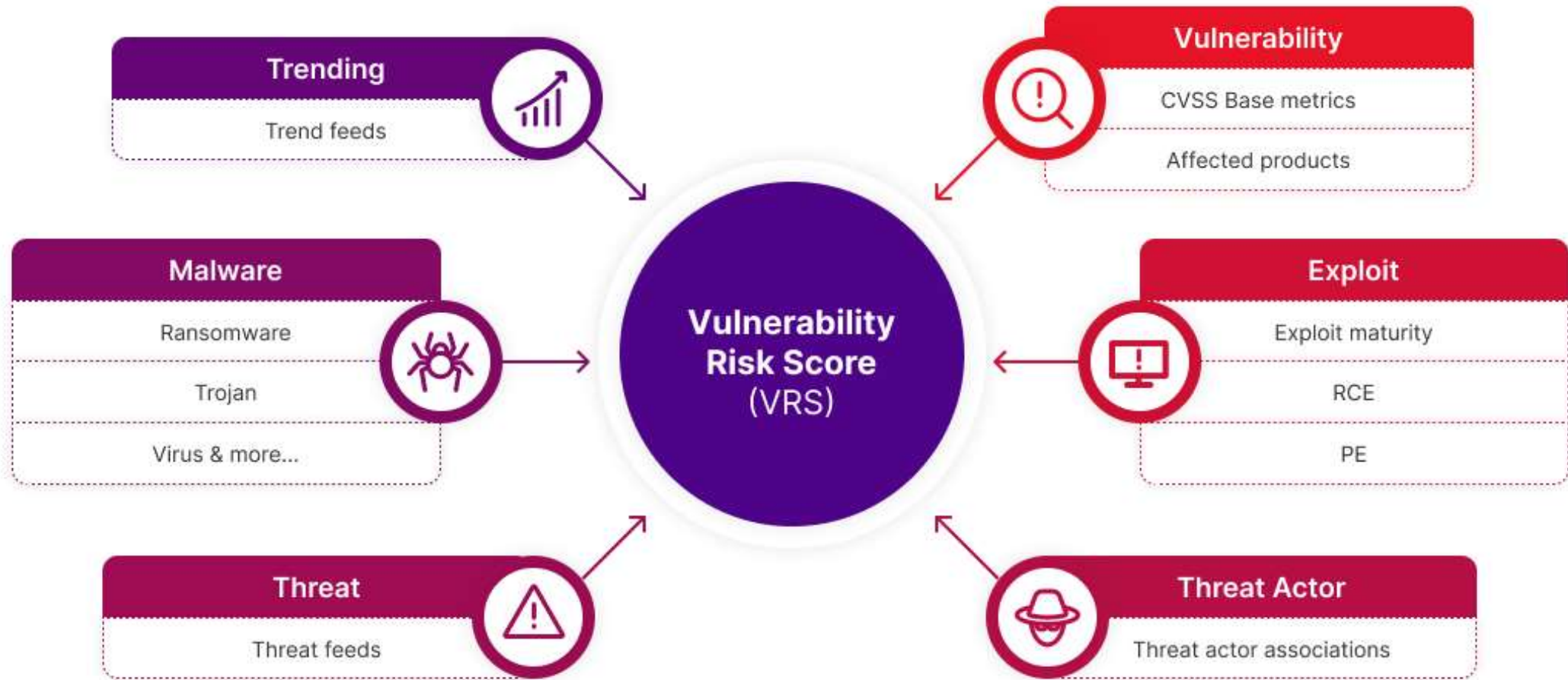
**Patch**  
<https://github.com/openbsd/src/commit/7bc29a9d5cd697290aa056e94ecee6253d3425f8>  
<https://github.com/openbsd/src/commit/f03a4faa55c4ce0818324701dadbf91988d7351d>  
<https://github.com/openbsd/src/commit/f8f5a6b003981bb824329dc987d101977beda7ca>  
<https://news.ycombinator.com/item?id=36790196>

**Release Notes**  
<https://www.openssh.com/txt/release-9.3p2>

**Vendor Advisory**  
<https://www.openssh.com/security.html>

**Third Party Advisory**

# Vulnerability Risk Score (VRS)



# Extensive EASM use cases



**Discover  
& inventory  
digital assets**



**Analyze  
& prioritize  
exposures**



**Curb  
cloud sprawl  
& shadow IT**



**Detect data  
leakage**



**Conduct risk  
assessment on  
subsidiaries,  
M&A targets &  
third parties**



**Reduce  
phishing & social  
engineering  
attacks**



**Adhere to  
regulatory  
compliance  
requirements**

# Bringing it all together



# Everywhere Work. Elevated.





## Endpoint & Risk Management

**Unified Endpoint Management + Security solutions** that enable you to delight your users with a personalized, secure work experience—everywhere.

Endpoint Mgmt.  
Modern Device Mgmt.  
Mobile Device Mgmt.  
User Workspace Mgmt.

Medical Device Mgmt.  
IIOT Device Mgmt.  
Rugged Device Mgmt.



Patch Mgmt.  
Risk & Vulnerability Mgmt.  
External Attack Surface Mgmt.  
Zero Trust Access  
Secure Access

Mobile Threat Defense  
Network Access Mgmt.  
Web Application Firewall

IT Service Mgmt.  
IT Asset Mgmt.  
Software License Optimization

Enterprise Service Management

- Human Resources
- Facilities
- Project Management
- Governance, Risk & Compliance

## Service & Asset Management

**Service & Asset Management solutions** that give users consistently great experiences—and outcomes—across your organization.

**ivanti**

# Attack Surface Management

## Executive Summary Report

Den Report finden Sie unter <http://ivanti.com/asm-report>



# **Danke!**

**Halle 7 Stand 610**