

# 25 Years of Vulnerability *Mis*management

*CypherCon 2024*

HD Moore



# Introduction

## HD Moore

- Co-founder & CEO of runZero
- Previously founder & developer of Metasploit
- Recovering penetration tester

## Get in touch!

Email: [hdm/at/runZero.com](mailto:hdm@runZero.com)

Mastodon: [@hdm@infosec.exchange](https://mastodon.social/@hdm)

WWW: <https://hdm.io>





# 25 Years of Vulnerability *Mis*management

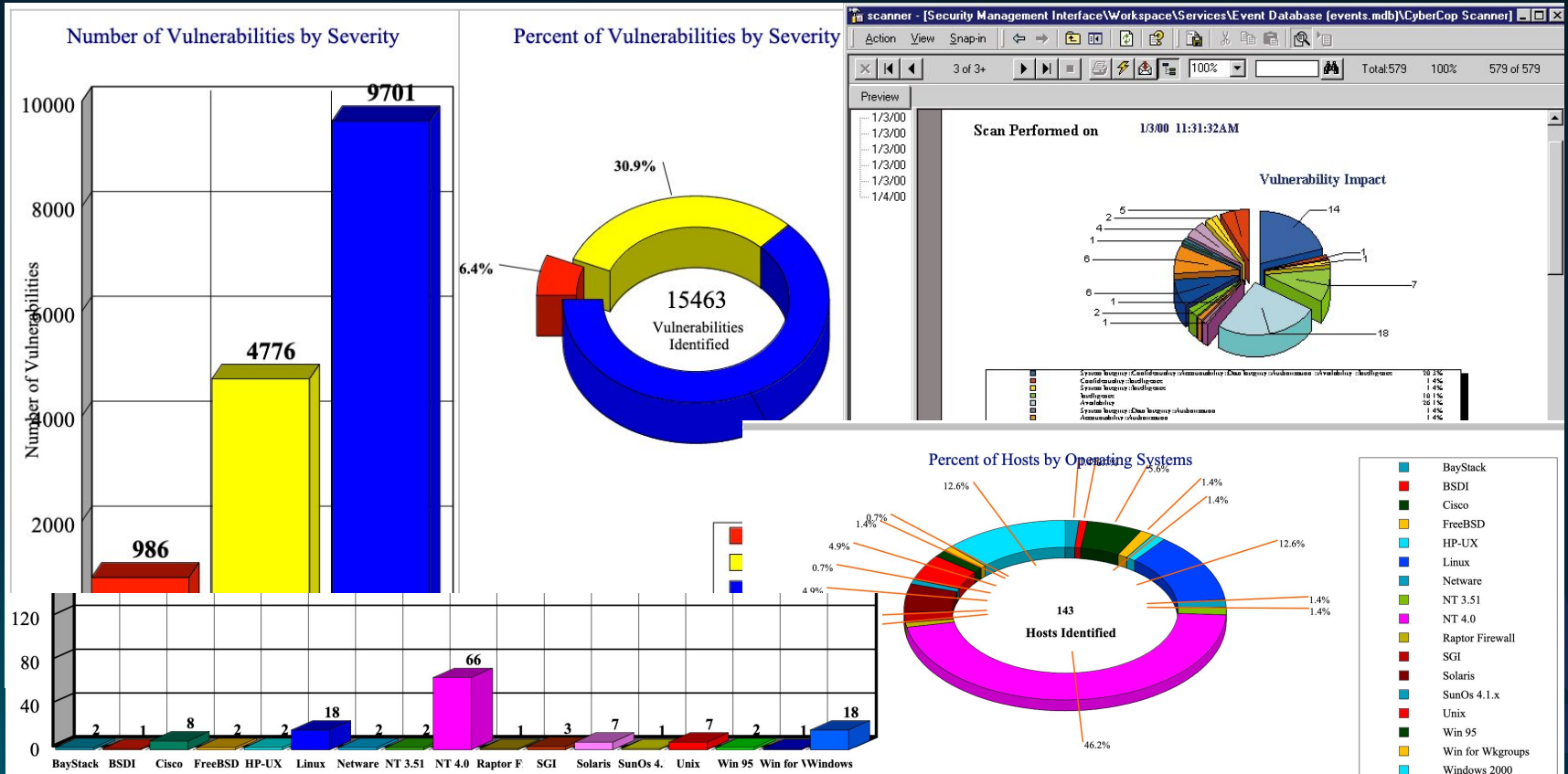
## Agenda

- Vulnerability management today
- The winding road to Enterprise
- Chronicles of a near future
- Building a better path
- Q & A





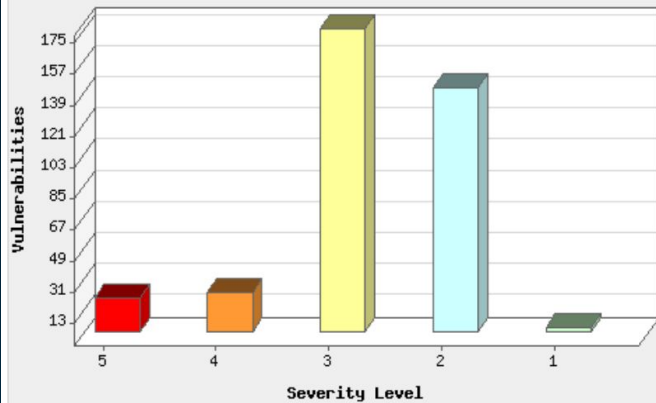
# Vulnerability management in 1999





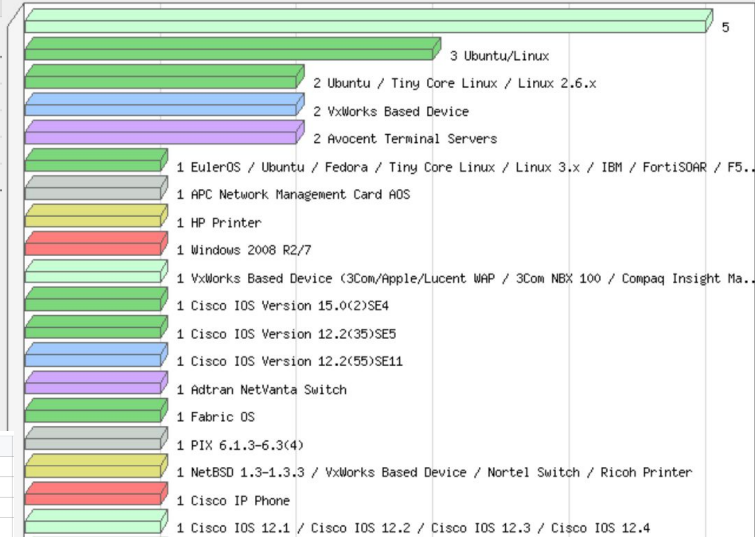
# Vulnerability management in 2024

### Vulnerabilities by Severity



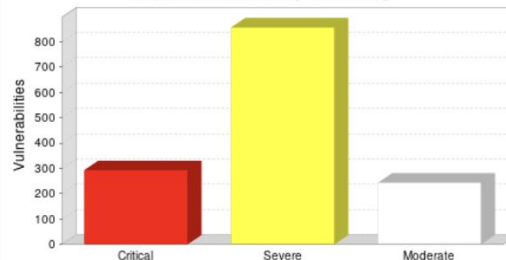
### Severity Level

- 20 Severity 5
  - 23 Severity 4
  - 175 Severity 3
  - 141 Severity 2
  - 3 Severity 1
- 362 Total

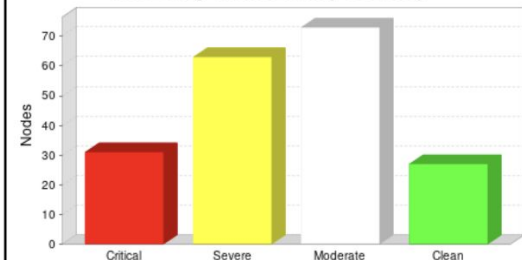


Severity (CVSS v3.0)	Plugin ID	Plugin Name	CVE ID	CVSS	CVSS3	CVSS3
HIGH	35291	SSL Certificate Signed Using Weak Hashing Algorithm		7.5	7.5	7.5
LOW	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)		2.0	2.0	2.0
CRITICAL	97991	Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp)		9.8	9.8	9.8
CRITICAL	103565	Cisco IOS Software DHCP Remote Code Execution Vulnerability		9.8	9.8	9.8
MEDIUM	57608	SMB Signing not required		6.5	6.5	6.5
CRITICAL	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)		9.8	9.8	9.8
CRITICAL	108722	Cisco IOS Software Smart Install Remote Code Execution Vulnerability		9.8	9.8	9.8
HIGH	93736	Cisco IOS iKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN)		7.5	7.5	7.5
HIGH	103670	Cisco IOS Software PROFINET denial of service (cisco-sa-20170927-profinet)		7.5	7.5	7.5
HIGH	108880	Cisco IOS Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities (cisco-sa-20180328-lldp)		7.5	7.5	7.5
HIGH	109087	Cisco IOS DHCP Multiple Vulnerabilities		7.5	7.5	7.5
HIGH	131322	Cisco IOS Software Smart Install DoS (cisco-sa-20180328-smi)		7.5	7.5	7.5
CRITICAL	11356	NFS Exported Share Information Disclosure		9.8	9.8	9.8
CRITICAL	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness		9.8	9.8	9.8

### Vulnerabilities by Severity

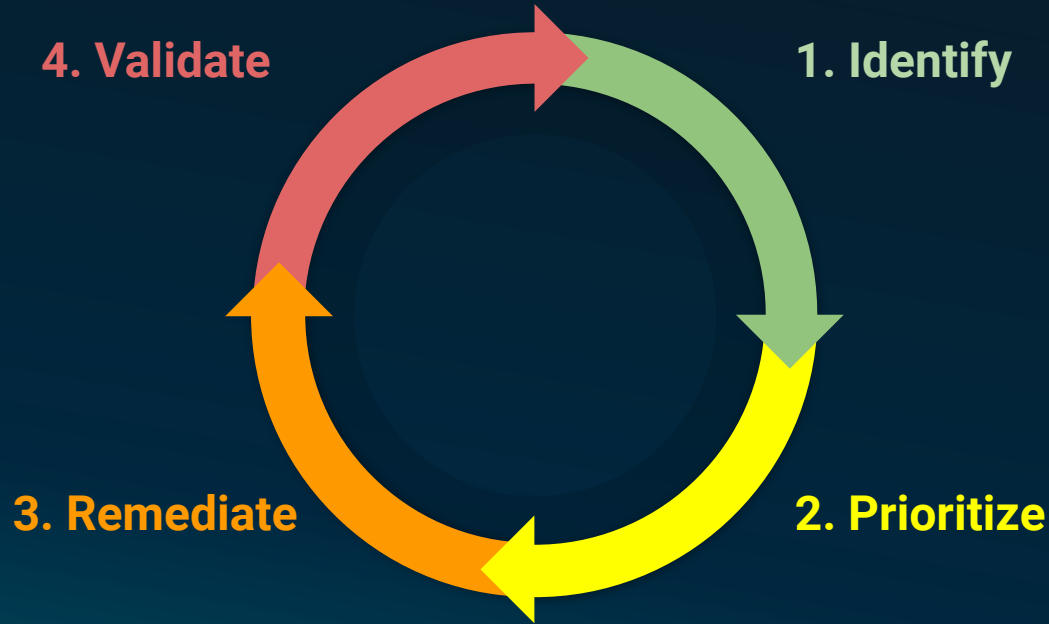


### Nodes by Vulnerability Severity





# Vulnerability management lifecycle





# Vulnerability management metrics

How do you measure performance?

- Time to detect, to remediate, to verify
- Absolute vuln counts and risk scores
- Number of exceptions & re-opens
- Inventory & coverage ratios
- Scan frequency

Demonstrating impact is tough





# Vulnerability management loses steam

30000  
Scan and patch started to break by 2005

- Increase in endpoint firewalls, segmentation, cloud, and BYOD
- Unauthenticated vulnerability checks are expensive to write
- Authenticated scans became the standard
- Leading vendors ship over 100k+ checks (!)
- Agent-based is new normal
- Still FPs!

20000

10000

0

2000

2005

2010

2015

2020

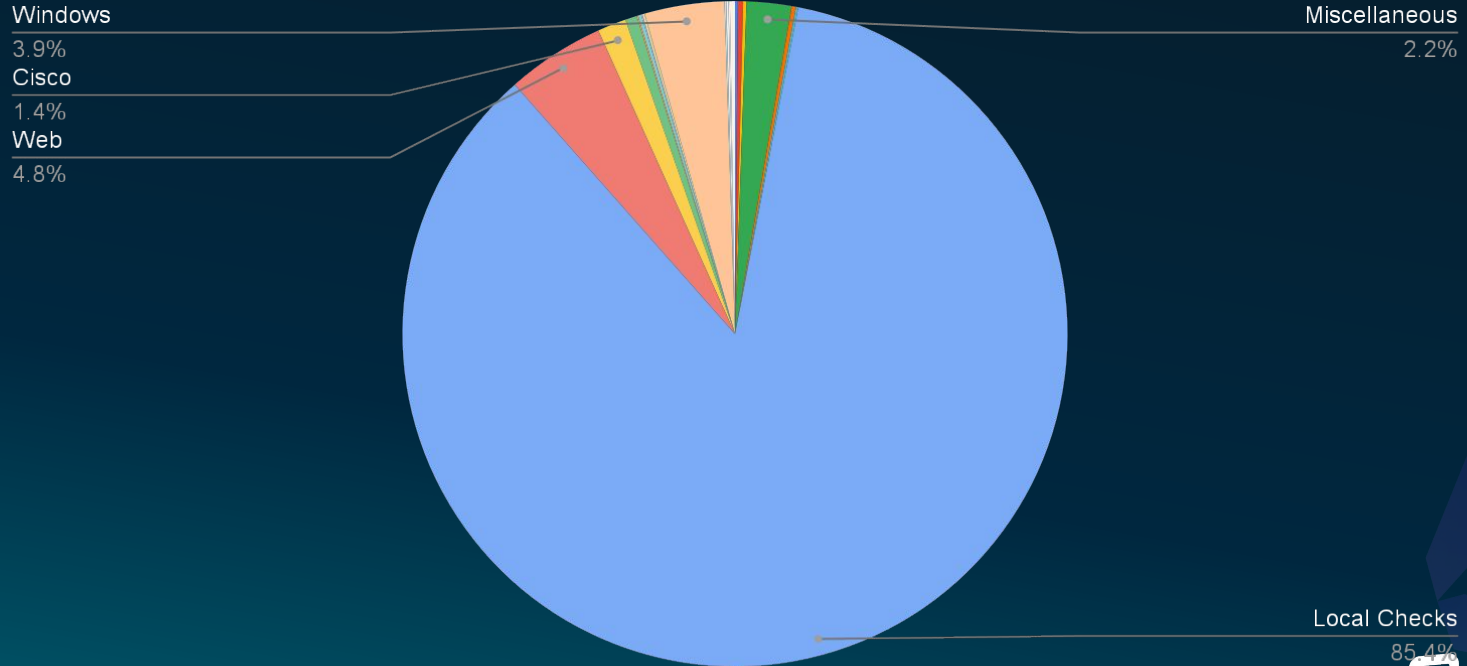






# Vulnerability management is mostly authenticated

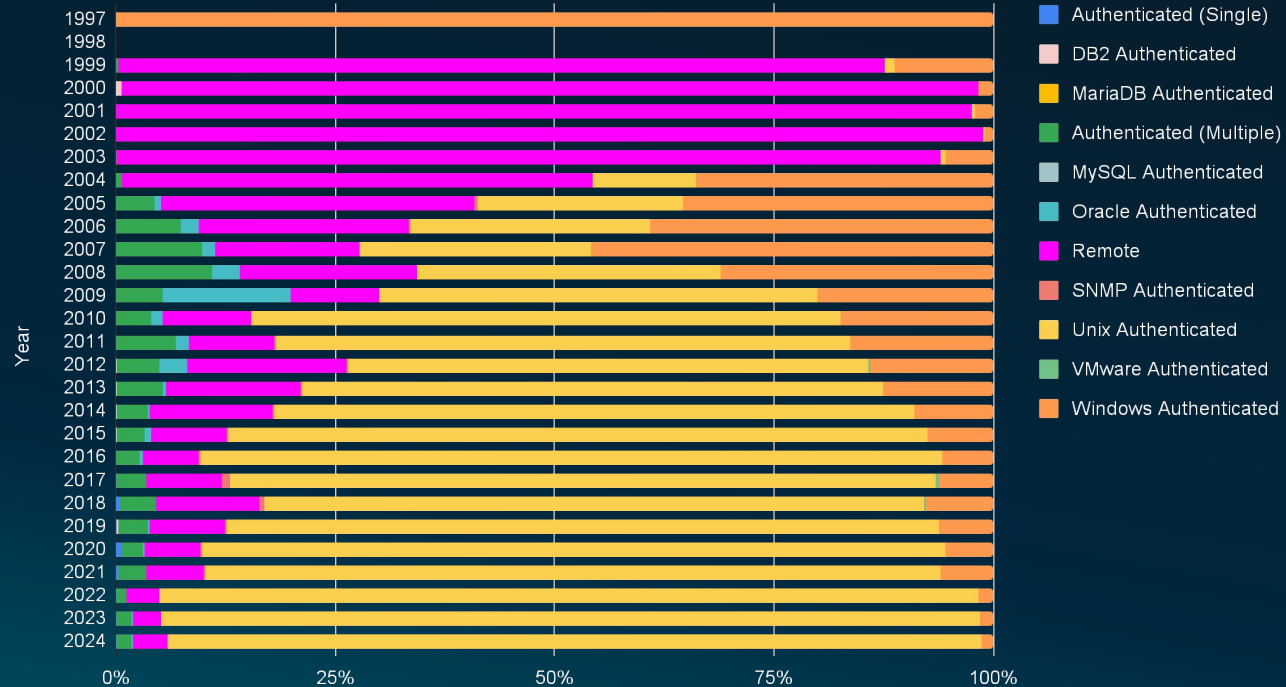
## Vulnerability Checks by Category





# Remote checks went from majority to minority

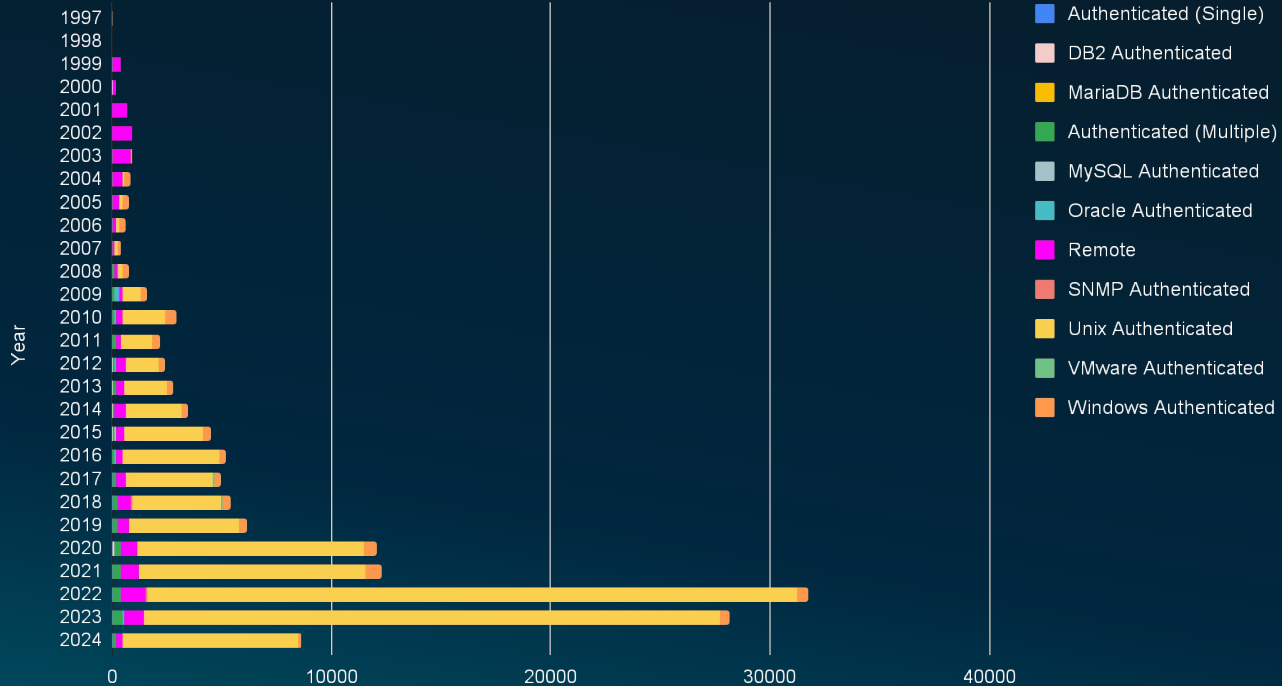
New Checks - Remote vs Authenticated - Percent (1997-2024)





# New remote checks by year

New Checks - Remote vs Authenticated - Absolute (1997-2024)





# Vulnerability management is falling behind

Systems are being exploited faster than scan cycles

- Scanners are now mostly authenticated patch checkers
- Unmanaged assets are being left behind
- Agents are now replacing scanners
- *Prioritization* is it's own market
- How did we get here?





**The winding road to Enterprise**



# The winding road to Enterprise

In the beginning, there were hackers

- Plenty of soft targets and almost no detection
- Scanners made intrusions quick and easy
- Businesses hired consultants for defense
- Hackers became security consultants
- Security consultants built tools
- Tools evolved into products
- Products became platforms





# The winding road to Enterpri\$e

## Security assessment platforms matured

- A hacker's view of the organization delivered as software
- Customers needed more than a vulnerability scanner
- Dashboards, reports, and lifecycle management
- Vulnerability management became big business
- Competition heated up





# The winding road to €nterPri\$e

## Regulatory compliance drove commodification

- Regulations rewarded vendors for features, not accuracy
- *“Thou must scan, but we don’t care how”\**
- Vulnerability management alone wasn’t enough
- Vendors built & acquired other products
- Scanners kept adding more checks
- Innovation stalled
- Will PCI save us?





# PCI ASVs

*“An ASV is an organization with a set of security services and tools (“ASV scan solution”) to conduct external vulnerability scanning services to validate adherence with the **external** scanning requirements of PCI DSS Requirement 11.2.2. The scanning vendor’s ASV scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC’s List of Approved Scanning Vendors.”*

accessitgroup.com  
 advantio.com  
 akati.com  
 alertlogic.com  
 ampcuscyber.com  
 aperiasonline.com  
 aperiasonline.com  
 atsec.com  
 1stoppiscan.com  
 edgescan.com  
 bctest.com  
 bmm.com  
 campusguard.com  
 medilogyservices.com  
 clone-systems.com  
 controlcase.com  
 cybersecurityworks.com  
 cyberwise.com.tr  
 experis.com  
 jp.fujitsu.com  
 gaminglabs.com  
 GMSECTEC.com  
 grantthornton.am  
 helpsystems.com

isecauditors.com  
 my-itspecialist.com  
 jet.msk.su  
 dialognauka.ru  
 lac.co.jp  
 lgms.global  
 megaplanit.com  
 nci.ca  
 mossadams.com  
 nccgroup.com  
 netcraft.com  
 nettitude.com  
 nri-secure.co.jp  
 intertek.com  
 intellilink.co.jp  
 nttsecurity.com  
 rangecyberdefense.com  
 orioninc.com  
 outpost24.com  
 paladion.net  
 panaceainfosec.com  
 procheckup.com  
 qualys.com  
 quinel.com.mt

riskassociates.com  
 rsisecurity.com  
 rsmus.com  
 s21sec.com  
 saintcorporation.com  
 sectigo.com  
 securisea.com  
 securitymetrics.com  
 sikich.com  
 sisainfosec.com  
 s3security.com  
 src-gmbh.de  
 stachliu.com  
 strozfriedberg.com  
 sysnetgs.com  
 tacsecurity.com  
 techlockinc.com  
 tenable.com  
 tis.jp  
 halosecurity.com  
 ubsecure.jp  
 pci.usd.de  
 vikingcloud.com

Major changes!



# PCI DSS compliance for internal networks

## Three options for quarterly internal scans

- Download and use an “open source tool”
- Purchase *Product A* or *Product B*
- Use your ASV for internal scans

## Mitigate all Critical and High severity vulnerabilities

- No requirement for quality, accuracy, or risk reporting model
- The resulting data is limited use and immediately stale





**Chronicles of a near future**



# Asset Attack Surface Management

- Even great vuln management didn't prevent incidents
- Security responses need to be faster than ever
- CAASM became a thing!

*“Cyber asset attack surface management (CAASM) is focused on enabling IT and security teams to overcome asset visibility and exposure challenges. It enables organizations to see all assets (internal and external), primarily through API integrations with existing tools, query consolidated data. Identify the scope of vulnerabilities then continuously monitor and analyze detected vulnerabilities to drill down the most critical threats to the business and prioritize necessary remediation and mitigation actions for improved cyber security.”*



# CAASM struggles with incomplete source data

Asset ingestion from APIs has serious challenges

- Every sources has its own quirks and conflicts
- Wrong IPs, wrong MACs, duplicates, and gaps
- Variable detail even from the same source
- Disparate collection timelines
- Vendors resist integration

500 Integrations? You're still missing critical assets

- Managed systems are only part of the environment





# Consolidation is accelerating

- Everything depends on and provides “inventory”
- EDR vendors now sell ASM and VM addons
- VM vendors are now selling EDR and SIEM
- Cloud security is now part of everything
- Every product now sells “visibility”



Network & Infrastructure Security

Advanced Threat Protection: Palo Alto Networks, Cisco, Fortinet, Trend Micro, etc.
SDN: Cisco, VMware, Arista, etc.
DDoS Protection: Cloudflare, Akamai, etc.
DNS Security: Cloudflare, etc.
Network Firewall: Palo Alto Networks, Cisco, Fortinet, etc.
Deception: Splunk, etc.

Web Security

ICS + OT: APERIO, Belden, etc.
Web Security: Akamai, Cloudflare, etc.
Endpoint Prevention: AhnLab, Avast, etc.
Network Analysis & Forensics: AWAKE, etc.

Endpoint Security

Endpoint Prevention: AhnLab, Avast, etc.
Endpoint Detection & Response: Palo Alto Networks, Cisco, etc.

Application Security

WAF & Application Security: Akamai, Cloudflare, etc.
Application Security Testing: Fortify, etc.

MSSP

Traditional MSSP: Atos, etc.
Advanced MSS & MDR: Atos, etc.

Data Security

Encryption: Thales, etc.
DLP: IBM, etc.
Data Privacy: OneTrust, etc.
Data Center Security: Dorex, etc.

Mobile Security

Mobile Security: Appdome, etc.

Risk & Compliance

Risk Assessment & Visibility: Armitage, etc.
Risk Quantification: BMC, etc.
Pen Testing & Breach Simulation: Cobalt, etc.
Security Awareness & Training: SANS, etc.

Security Ops & Incident Response

SIEM: Splunk, etc.
Security Incident Response: Palo Alto Networks, etc.



Threat Intelligence

Threat Intelligence: Anomali, etc.

IoT

IoT Devices: BlackBerry, etc.
Automotive: Continental, etc.
Connected Home: CUJOAI, etc.

Messaging Security

Messaging Security: Area 1, etc.

Identity & Access Management

Authentication: Okta, etc.
Privileged Management: CyberArk, etc.
Identity Governance: SailPoint, etc.
Consumer Identity: Auth0, etc.

Security Analytics

Security Analytics: Exabeam, etc.

Digital Risk Management

Digital Risk Management: Cyberint, etc.

Security Consulting & Services

Security Consulting & Services: Accenture, etc.

Fraud & Transaction Security

Fraud & Transaction Security: Bionicatch, etc.

Cloud Security

Cloud Security: AWS, etc.

Container: Anchore, etc.



# Big platforms are getting bigger

- Big tech treats security products like any other business
- Undercut competitors and lock users into the platform
- Driven by economics & hype cycles
- A tough time for innovation





# Sometimes with surprising combinations

Progress.com website showing a dropdown menu with various product categories:

- DATA PLATFORM
  - MarkLogic
  - Semaphore
  - OpenEdge
- DATA CONNECTIVITY
  - DataDirect
- DIGITAL EXPERIENCE
  - Sitefinity
  - Telerik
  - Kendo UI
  - Corticon
  - DataDirect
  - MOVEit
- DEVOPS
  - Chef
- INFRASTRUCTURE MANAGEMENT & OPERATIONS
  - Flowmon
  - Kemp LoadMaster
  - WhatsUp Gold
- UI/UX TOOLS
  - Telerik
  - Kendo UI
  - Fiddler
  - Test Studio
- SECURE FILE TRANSFER
  - MOVEit
  - WS\_FTP

VIEW ALL PRODUCTS

Fortra.com website showing a dropdown menu with various product categories:

- Agari
- Alert Logic
- Automate
- Beyond Security
- Capacity Management
- Clearswift
- Cobalt Strike
- Core Security
- Data Classification
- Digital Defense
- Digital Guardian
- Document Management
- FileCatalyst
- Globalscape
- GoAnywhere
- Halcyon
- Intermapper
- JAMS
- Outflank
- PhishLabs
- Powertech
- Robot
- Sequel
- Showcase
- Terranova Security
- Tripwire
- Product Bundles
- View all products
- Chat live with an expert

HERE'S HOW

Ivanti.com website showing a grid of acquired companies:

- RiskSense
- Cherwell
- MobileIron
- Pulse Secure
- RES Software
- Concorde Solutions
- AppSense
- Heat
- Lumension Security
- Shavlik
- Wavelink
- LANDESK



# Sometimes with surprising combinations

**FORTRA™**

English

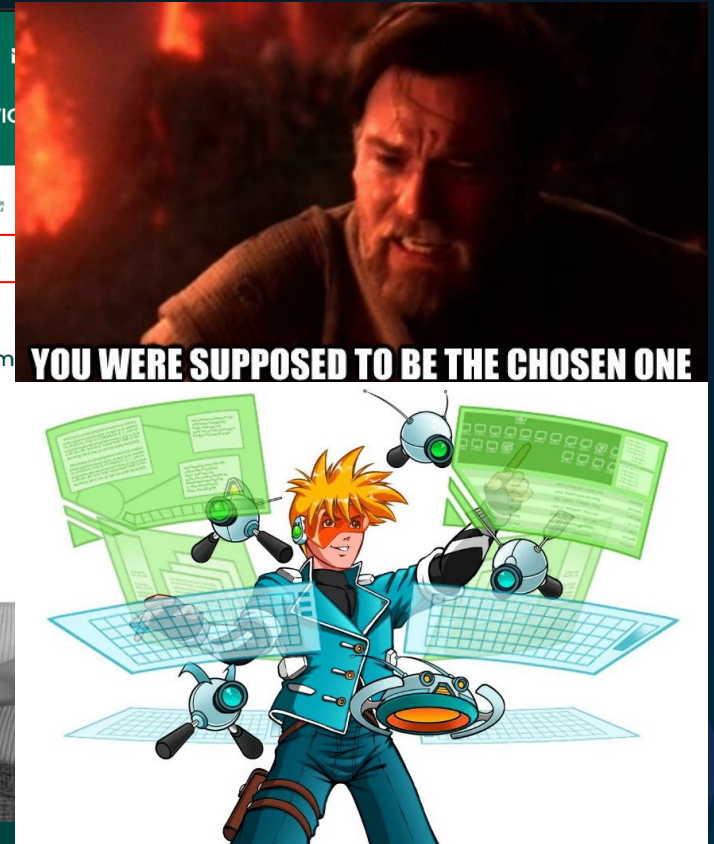
SOLUTIONS ▾ PRODUCTS ▾ SERVICE ▾

## Meet Fortra™

At Fortra™, we're creating a straightforward future for companies of all sizes, helping them escape the gloom of cyberthreats get to work.

**HERE'S HOW**

- Agari
- Alert Logic
- Automate
- Beyond Security
- Capacity Management
- Clearswift
- Cobalt Strike
- Core Security
- Data Classification
- Digital Defense
- Digital Guardian
- Document Management
- FileCatalyst
- Globalscape
- GoAnywhere
- Halcyon





# Bigger, cheaper, and less focused

- Consolidation drives wide and shallow R&D investments
- Very few vendors are trying to improve data sources
- Security firms are now mostly software firms
- Specializations have shifted to web & cloud
- Vulns are still treated as commodity data
- So many single panes of glass
- We can do better!



**Building a better path**



# From vulnerability to exposure management

Our goal is to **minimize attacker opportunities**

- Maintain accurate information on all assets & attributes
- Respond instantly to emerging threats & campaigns
- Track technologies not vulnerabilities
- Reduce exposure anywhere we can
- Maintain a living model



# Baseline assumptions for exposure management

Narrow your scope using modern assumptions

- Patch management and auto-updates are common
- Systems are either **managed** or **unmanaged**
- Managed assets will always have agents
- Assume we can gather data from agents
- AV, EDR, MDM, DLP, VM, ...

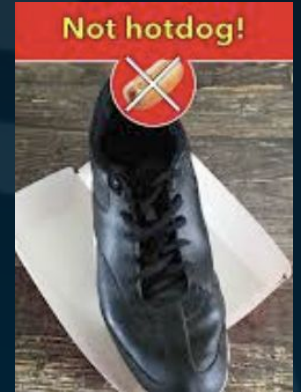




# Unknown and unmanaged are still high risk

First step is knowing where to look

- CAASM tools correlate multiple sources, you can too!
- E/ASM tools do OK for external exposure
- Internal is still really tough



The network is essential for unmanaged inventory

- Use your NDR if you can get a SPAN port
- Active scanners for everything else\*



# Great sources for exposure management data

- “Info” and “Low” vulnerabilities often the most valuable
- SNMP ARP caches from around the network
- Google Workspace “endpoints” (GDrive!)
- DHCP and DNS logs from all subnets
- Less obvious service data
  - SMB 2 Session IDs
  - SNMP counters
  - DCERPC EPM





# Build a detailed model of assets and services

Aggregate data from any managed sources available

Overlay with network & vuln scan sources

Annotate assets with useful attributes

- Subnets & hostnames
- Technology & services
- Hardware & software
- Security controls
- Sensitive of data
- Owners



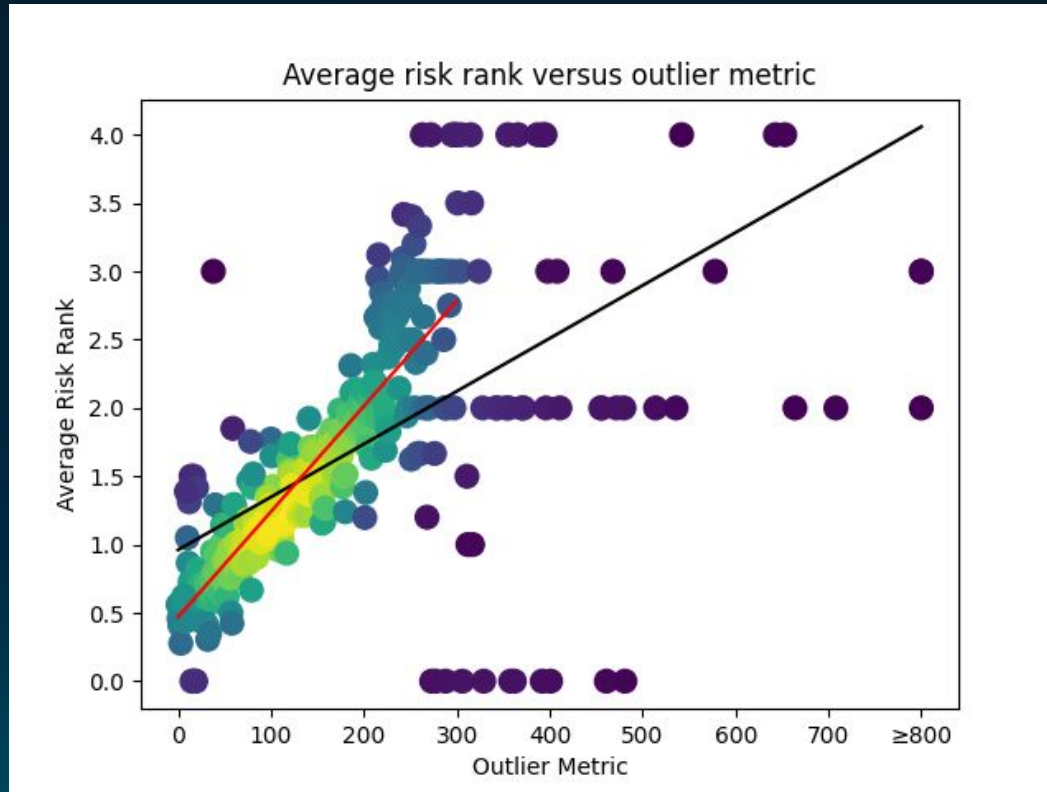
# Shake out the easy stuff

Avoid incidents by clearing the low-hanging fruit

- Managed assets without expected EDR/MDM agents
- Assets with addresses missing from vuln scans
- End-of-Life OS, software, and hardware
- Windows assets not on your domain
- Outliers!



# Outliers scores are strongly predictive of risk





# Instantly respond to emerging threats

There is an actively exploited vulnerability in \$product

- Within seconds, find all potentially affected assets
- Mitigate assets with the most exposure first
- Take into account mitigating controls

```
product:"Policy Secure" OR product:"Connect Secure"
```





# Determine blast radius after an incident

Given a confirmed breach, work out the exposure

- What was reachable from the compromised node?
- What technology was present?
- What data was accessible?

```
net:"10.10.10.0/24" AND NOT source:"CrowdStrike"
```



# Efficient exposure management

## Build!

- Shovel your data into a SIEM or database of choice
  - Elastic + Filebeat, Neo4J, PostgreSQL, etc
- Correlation is tricky, but not a roadblock for use
- Owned by the security operations team
- Accessible to everyone else


## Buy?

- CAASM is turnkey for small-to-medium organizations
- Massive environments are always a mix of both





# Build challenges

- Storage and search needs to scale to your needs
- Shard data and drop old data automatically 
- Source data needs accuracy and detail
- Share your data with other teams
- Monitor ingestion health
- Dashboards!





# Open source & free CAASM tools

## OSS

- CISA CrossFeed [github.com/cisagov/crossfeed](https://github.com/cisagov/crossfeed)
- JupiterOne Starbase [github.com/jupiterone/starbase](https://github.com/jupiterone/starbase)
- DROIDS IVRE [github.com/ivre/ivre](https://github.com/ivre/ivre)
- PryOcc axiom [github.com/pryOcc/axiom](https://github.com/pryOcc/axiom)

## FREE

- runZero Platform (Community Edition): [runZero.com](https://runzero.com)
- Your existing vulnerability management product?







Thank You!

Email: [hdm/at/runZero.com](mailto:hdm@runZero.com)

Mastodon: [@hdm@infosec.exchange](https://mastodon.social/@hdm@infosec.exchange)

WWW: <https://hdm.io>

