JupiterOne

THE State of Cyber Assets Report

2023

JupiterOne Research

Contents

JupiterOne

Contents

Scaling security to a fragmented attack surface

Goal

Understand cyber assets, liabilities, attack surfaces, and their relationships to each other in the modern enterprise.

Summary

Not only is the attack surface growing, but the scale of the problem is now untenable.

"By redefining the cybersecurity control plane, we can better adapt to our environments' growing complexity."

Understand cyber assets, liabilities, attack surfaces, and their relationships to each other in the modern enterprise."

The evolving state of the modern cyber attack surface is the reason we created The State of Cyber Assets Report (SCAR). It's one of many annual reports to understand cyber assets, liabilities, attack surfaces, and their relationships to each other in the modern enterprise.

In the era of increasingly destructive and disruptive cyber threats, centralized cyber assets are a business liability. Threats to the confidentiality, integrity, and availability of organizations have made it necessary to adapt by decentralizing our cyber assets across a growing number of cloud service providers, environments, and services.

Not only is the attack surface growing, but the scale of the problem is now untenable. That's why we've set out to conduct and write this research.

Cybersecurity practitioners are grappling with an unprecedented amount of complexity in 2023. Continuous integration and deployment (CI/CD) pipelines result in a steady stream of changes that can each introduce new possibilities for misconfigurations, policy exceptions, or human error. Security teams need context to scale security policy and enforcement to the distributed evolving attack surface.

Striving for reduced complexity is not possible for cybersecurity teams. Instead, we must learn to accept our increasingly complex environments by rethinking our definition of the cybersecurity control plane. Achieving consistent situational awareness across new asset types and environments requires a shift toward unified cyber insights. Its flexibility is especially suitable for increasingly modular approaches consistent with hybrid multicloud architectures. CSMA enables a more composable, flexible and resilient security ecosystem. Rather than every security tool running in a silo, a cybersecurity mesh enables tools to interoperate through several supportive layers, such as consolidated policy management, security intelligence and identity fabric.

Jasmine Henry
Lead Researcher
Senior Director of Data Security and Privacy

Research questions

The following questions formed the basis of the research conducted for the 2023 State of Cyber Assets Report. All of the findings in this report derive from these core questions.

01 What is the composition of cyber asset inventories?

- What are the average number of **APPLICATIONS**, **DATA**, **DEVICES**, **NETWORKS**, and **USERS**?
- How many assets and accounts are in an AWS, GCP, or Azure environment?
- Are security practitioners inventorying all types of cyber assets?
- What is the value of a cyber asset?

02 How do security practitioners interact with security data?

- What is the composition and volume of security data?
- What are the most leveraged types of security technologies?
- How many security data sources are being correlated and aggregated?
- Do security teams have comprehensive, data-driven visibility across the attack surface?

Research questions

The following questions formed the basis of the research conducted for the 2023 State of Cyber Assets Report. All of the findings in this report derive from these core questions.

03 Which assets tend to have more liabilities (or vulnerabilities)?

- What tools are security practitioners using to identify and detect vulnerabilities?
- What is the ratio of vulnerabilities to assets, and which types of assets have the most vulnerabilities?
- Which assets are the most critically vulnerable?

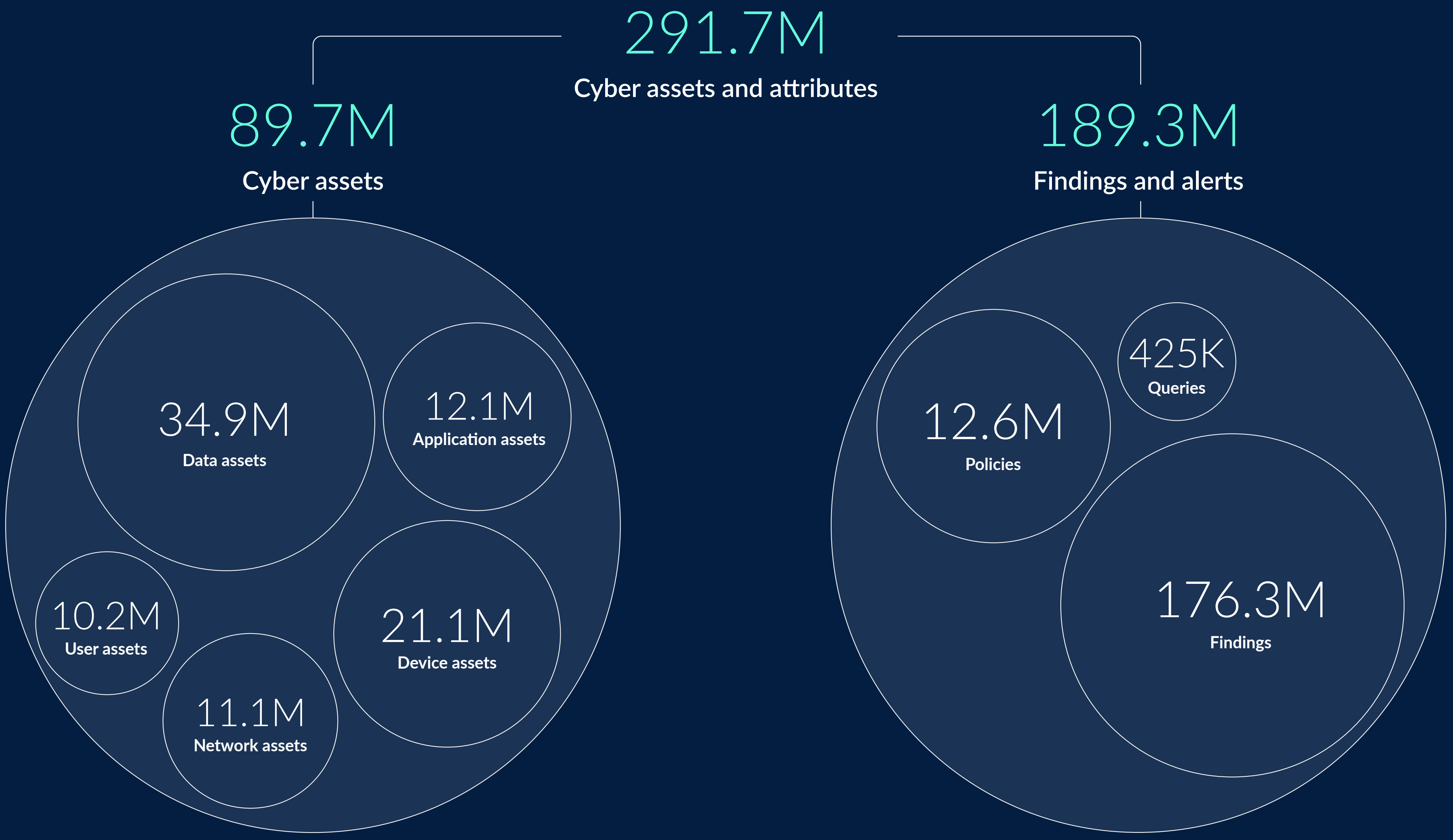
04 How do security practitioners navigate their attack surface and data sources?

- What assets do security practitioners query?
- Which assets are most related?

Introduction

Executive summary and key findings

Our research included an analysis of:



291.7M
Cyber assets and attributes

89.7M
Cyber assets

34.9M
Data assets

12.1M
Application assets

10.2M
User assets

11.1M
Network assets

21.1M
Device assets

189.3M
Findings and alerts

12.6M
Policies

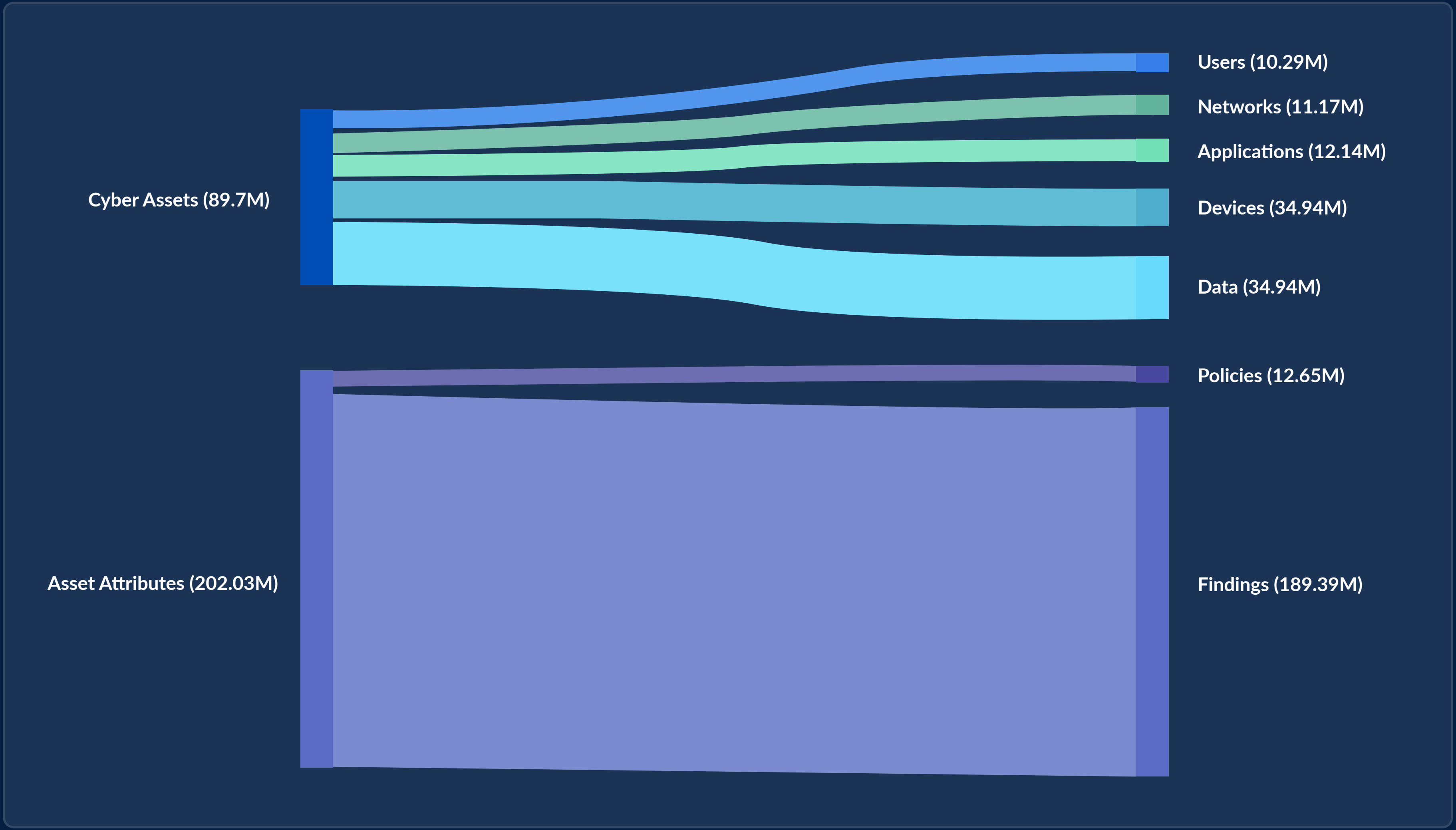
425K
Queries

176.3M
Findings

Introduction

Overview of SCAR data

Executive summary chart 1: ratio of cyber assets to attributes



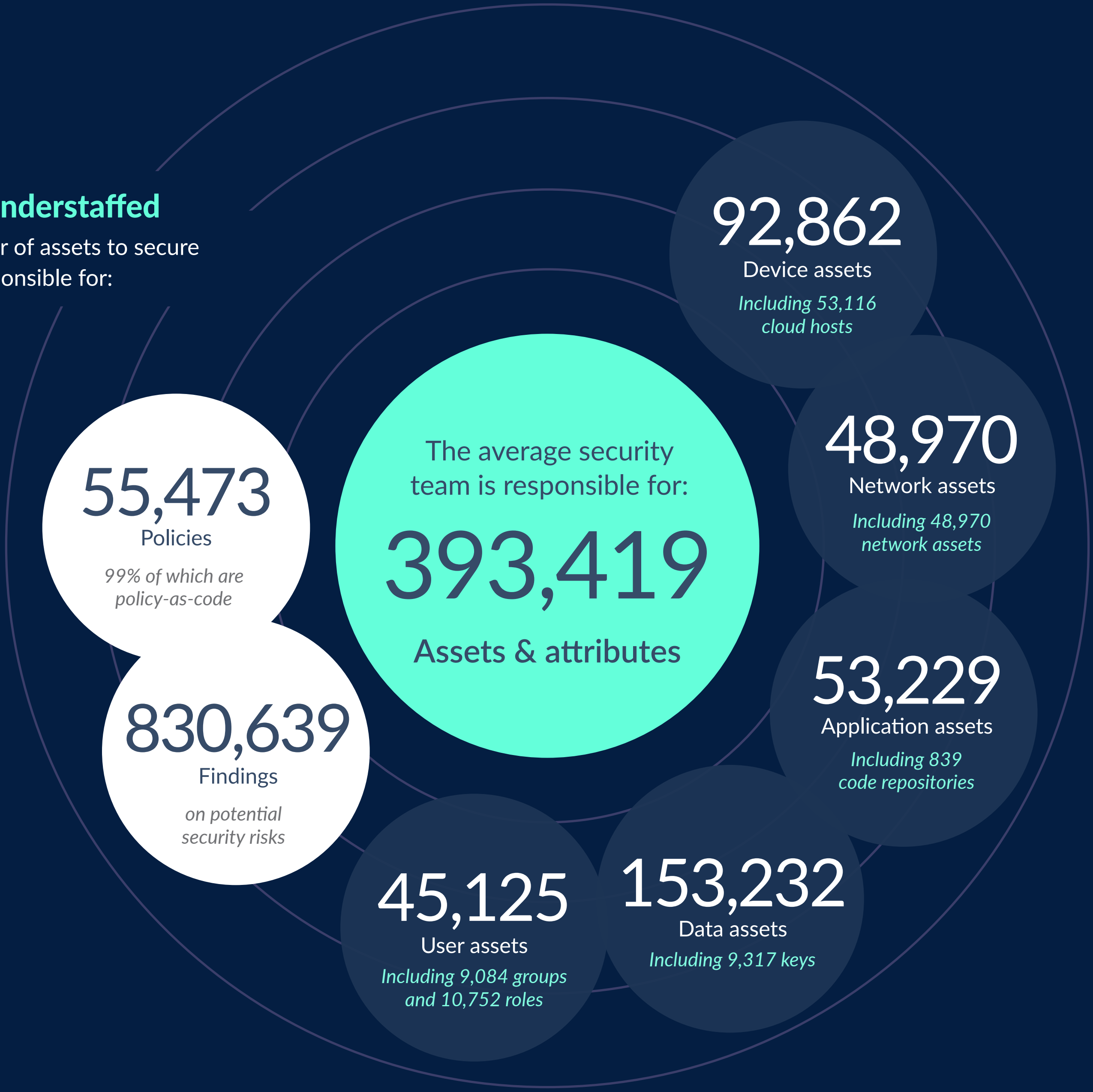
On average

Security teams are fatigued and understaffed

Security teams have an unprecedented number of assets to secure and manage. The average security team is responsible for:

Year-over-year, the average security organization has experienced a **132.86%** increase in cyber assets and a **588.98%** increase in security findings.

The mean value of a cyber asset is **$17,711**, a staggering number considering the volume of both assets and findings (or liabilities) that security practitioners must oversee.



The average security team is responsible for:

393,419

Assets & attributes

55,473
Policies
99% of which are policy-as-code

830,639
Findings
on potential security risks

92,862
Device assets
Including 53,116 cloud hosts

48,970
Network assets
Including 48,970 network assets

53,229
Application assets
Including 839 code repositories

153,232
Data assets
Including 9,317 keys

45,125
User assets
Including 9,084 groups and 10,752 roles