

# Asset Manager

Real-time network discovery, identification, and threat detection

## Problem Statement

- How can you be sure you are maintaining 100% visibility across your network?
- How do you discover & eliminate visibility gaps across your entire network?
- How do you achieve and maintain an accurate and real time view of your attack surface?

## FireMon's Answer

- Continuous discovery of the entire network infrastructure for every device and connection including firewalls, routers, end points, and cloud devices
- Multiple discovery protocols to support active, passive & targeted discovery methods
- Automatic device profiling, including IoT & operational technology

## Business Outcomes

- Single source of reliable, consistent global asset and network data
- Reduced risk of exposure due to data breaches or network compromise
- Verified network and device data model; not just collected from other sources

## Data Extensibility

- Swagger-based, bi-directional RESTful API simplifies integration
- Extend data to other solutions across security landscape, including CMBD, vulnerability scanners, network modeling/simulation, data lakes and more
- Accelerate incident response and reduce risk with SOAR and ITSM integrations

## Key Differentiators

- Unmatched speed, scalability, and accuracy, using non-disruptive techniques
- API first approach with leading security vendors to support integration of newly found devices
- Agent-less mapping, reporting, and visualization

## A Complete View of All Assets

FireMon Asset Manager provides unmatched, real-time cyber situational awareness that enables network and security teams to discover the darkest corners of their often-obscure infrastructure.

Technique	Used By	Limitations
Agents	<ul style="list-style-type: none"> <li>- Endpoint Mgt.</li> <li>- Asset Mgt.</li> </ul>	<ul style="list-style-type: none"> <li>- Ports can be closed</li> <li>- Not all devices support agents</li> <li>- Typically miss ~30%</li> </ul>
Credentials	<ul style="list-style-type: none"> <li>- Vulnerability Mgt.</li> <li>- Network Modeling</li> <li>- Network Device Mgt.</li> </ul>	<ul style="list-style-type: none"> <li>- Creds = Access, not Discovery</li> <li>- Typically miss ~30%</li> </ul>
Traffic Flow (network choke points)	<ul style="list-style-type: none"> <li>- Network Access Control</li> </ul>	<ul style="list-style-type: none"> <li>- Must know ALL choke points</li> <li>- Extensive deployment</li> <li>- Typically miss ~50%</li> </ul>

## Success Stories

### Defence Organisation with Over 100 Million IPs

#### Challenges

- Lack of visibility across their environment; couldn't see assets that needed management, higher risk of threat actors
- Unable to support ongoing operations with existing security stack
- High number of personnel, at high cost, needed to achieve reporting

#### Outcomes

- 100 million IP spaces scanned
- Identified security boundaries, reduced threat actor risk, eliminated blind spots
- Identified inactive network segments to be shut down, reducing the cost of operations
- Staff members can be reassigned to other, more pressing projects

### Global Banking and Financial Services Firm Managing Nearly \$2 Trillion in Assets

#### Challenges

- M&A activity negatively impacted by incomplete, inaccurate IT asset information: lack of "cyber due diligence"
- Inability to visualize the entire network complicated security decisions, increased attack surface, opened new avenues for risk

#### Outcomes

- 17 million IP spaces scanned daily
- 300,000+ IP devices monitored in real-time
- 100,000+ previously unknown devices discovered

### US Health Insurance Provider to Over 4.3 Million Members

#### Challenges

- Legacy endpoint management systems lacked adequate discovery, making accurate asset audit impossible
- Unable to validate security policies applied on all assets, dramatically increasing risk

#### Outcomes

- 240% increase in IP addresses discovered for complete visibility (40K to over 100K)
- 100% automatic discovery and identification of all assets on the network
- 0 unexpected compliance breaches

For more information about FireMon Asset Manager  
please email: [sales@firemon.com](mailto:sales@firemon.com)

# FIREMON

FireMon improves security operations that will in turn lead to better security outcomes. FireMon delivers industry-leading security policy management, cloud security operations, and asset management solutions. Our platform is the only real-time solution that reduces firewall and cloud security policy-related risks, manages policy changes, and enforces compliance. Learn more at [FireMon.com](https://www.firemon.com).