
analyzet
SafeLinx
Securing the Invisible:
Closing IoT & OT
Security Gaps

SafeLinx

Introduction

The modern IoT and OT landscape is rapidly expanding, connecting billions of devices across industries. While this connectivity drives efficiency and innovation, it also introduces critical security gaps:

Limited Visibility

Most organizations lack a complete inventory of their IoT/OT assets, leaving blind spots in the network.

Unusual Protocols & Traffic Blindness

IoT devices communicate using niche and proprietary protocols. Traditional IT security tools often fail to recognize or monitor these, creating opportunities for undetected malicious activity.

Threat Detection Gaps

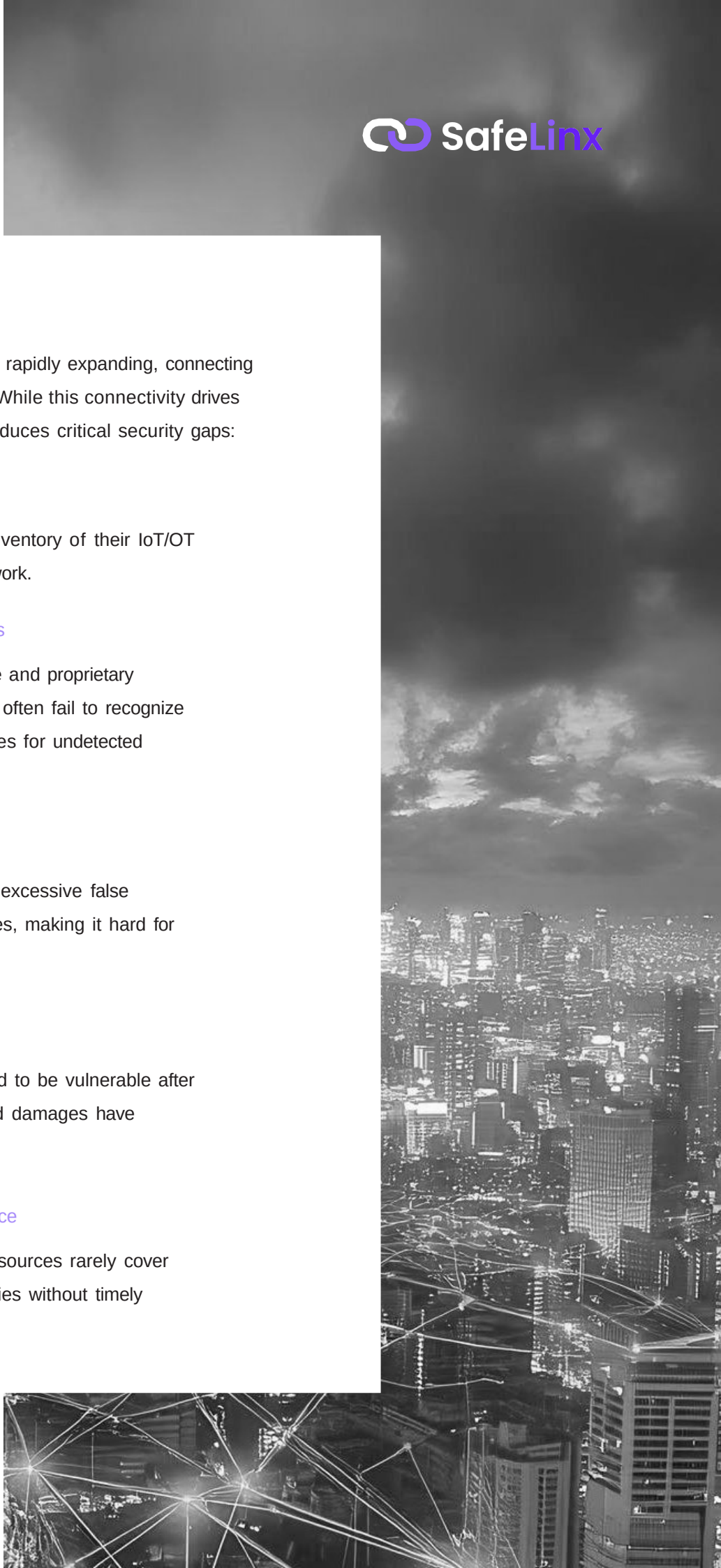
Standard security platforms generate excessive false positives or miss IoT-specific anomalies, making it hard for SOC teams to respond effectively.

Hidden Vulnerabilities

Many IoT systems are only discovered to be vulnerable after an attack occurs, when downtime and damages have already taken place.

Lack of IoT-Specific Threat Intelligence

Existing cyber threat intelligence (TI) sources rarely cover IoT/OT attack vectors, leaving industries without timely warnings about targeted exploits.



SafeLinx

Why SafeLinx?

SafeLinx is an advanced IoT/OT security platform designed to protect critical infrastructure and connected devices. It delivers full visibility, real-time threat detection, and continuous operational integrity with simplicity and scalability.

- **Asset Visibility:** Automatically discover OT/IoT devices, map network topology, and monitor communications to eliminate blind spots.
- **Threat Detection:** Identify anomalies and malicious activity using both behavioral and signature-based analysis across niche protocols.
- **Continuous Monitoring:** Analyze real-time traffic across key industrial protocols like Modbus, DNP3, BACnet, and OPC.

Comprehensive Asset Explorer

Continuously identifies, classifies, and monitors every IT, IoT, and OT device. Access full technical context, network statistics, and activity insights for complete situational awareness.

Centralized Alert Management

Unifies alerts into a single intuitive interface. Correlates events, contextualizes risk, provides root cause insights, and delivers actionable response guidance for immediate mitigation.

Vulnerability Management

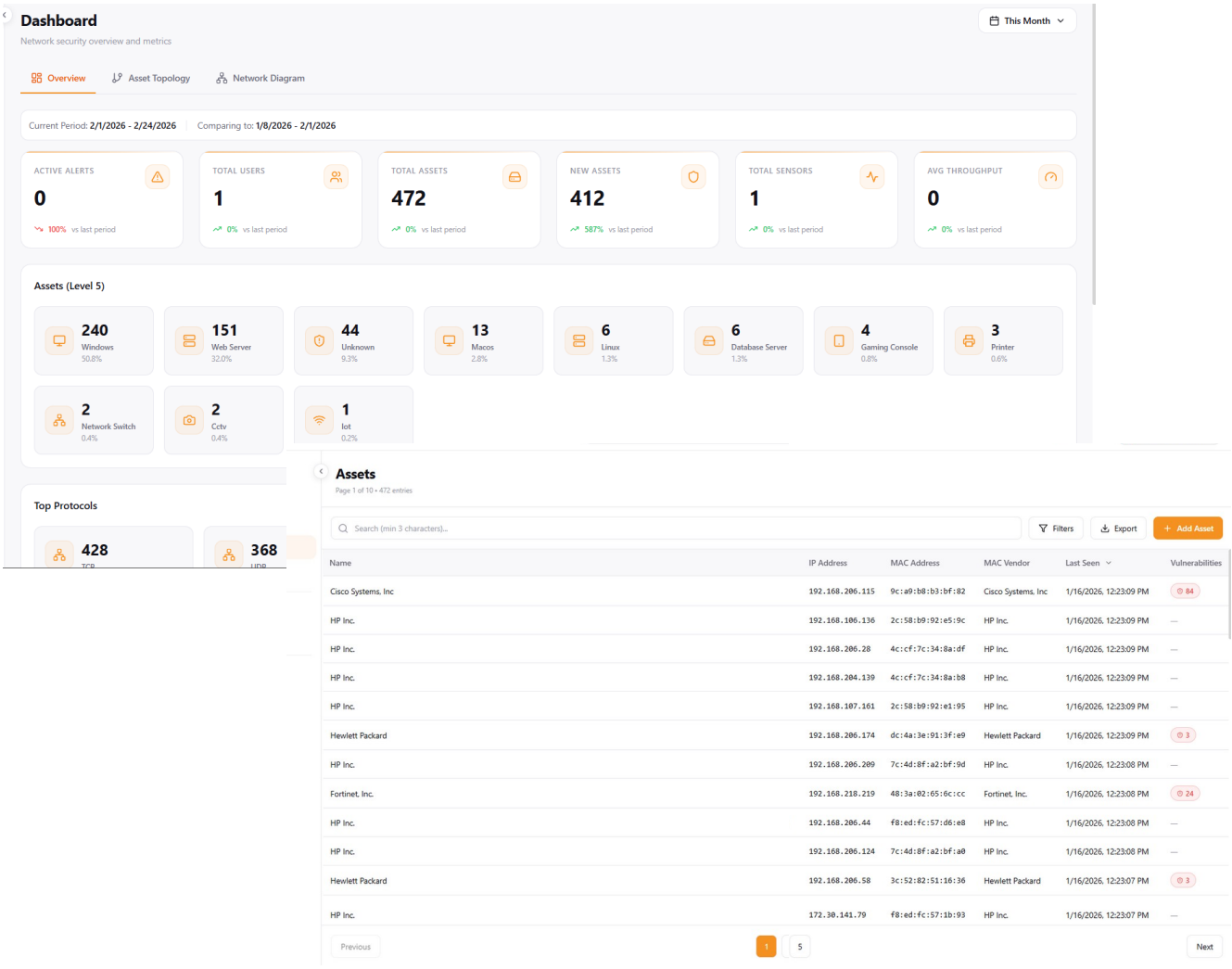
Scans and correlates vulnerabilities across connected assets. Focuses on exploitable CVEs and Known Exploited Vulnerabilities (KEVs) to provide a prioritized, risk-based remediation roadmap.

IoT-Focused Threat Intelligence

Matches global threat feeds with internal assets and network protocols. Delivers sector-specific intelligence and filters events by malware, threat actor, or vulnerability for context-aware defense.

Unified IoT Security Dashboard

The SafeLinx dashboard provides a centralized, single-pane-of-glass view of your IoT and OT ecosystem. It continuously discovers new assets as they appear on the network and automatically classifies them by type, vendor, and role. This eliminates blind spots and ensures teams always know exactly what devices are active and how they interact.

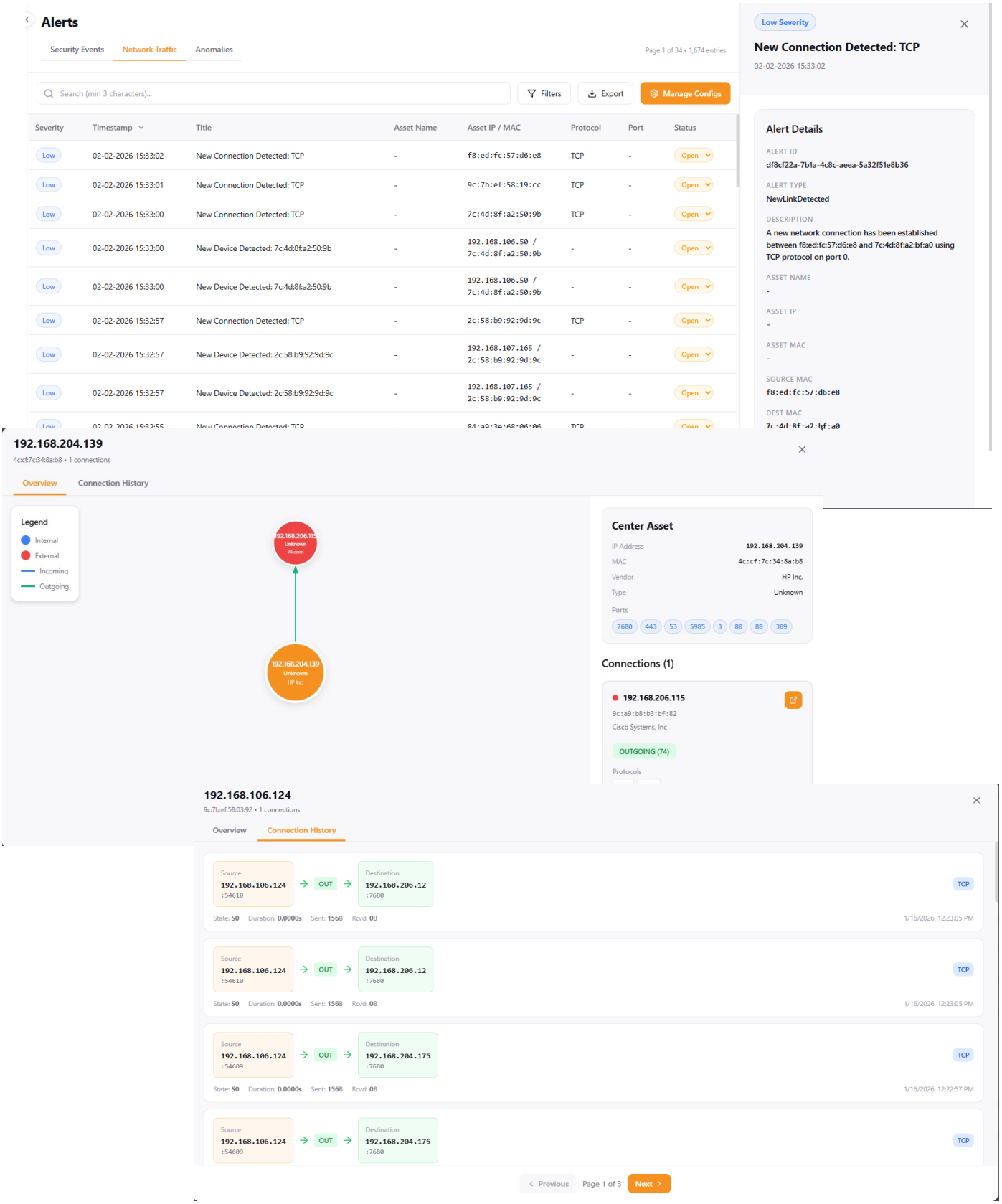


Beyond visibility, the dashboard correlates alerts, vulnerabilities, communication flows, and detected protocols into intuitive graphs and charts. Security teams can quickly spot unusual behavior, prioritize high-risk threats, and make informed decisions with confidence.

- Real-time asset discovery and classification of all IoT/OT devices
- Interactive visualization of device relationships and communication links
- Consolidated view of threats, anomalies, and vulnerabilities
- Risk-based prioritization to focus on what matters most
- IoT-specific threat intelligence integrated into every alert

Advanced Threat and Anomaly Detection

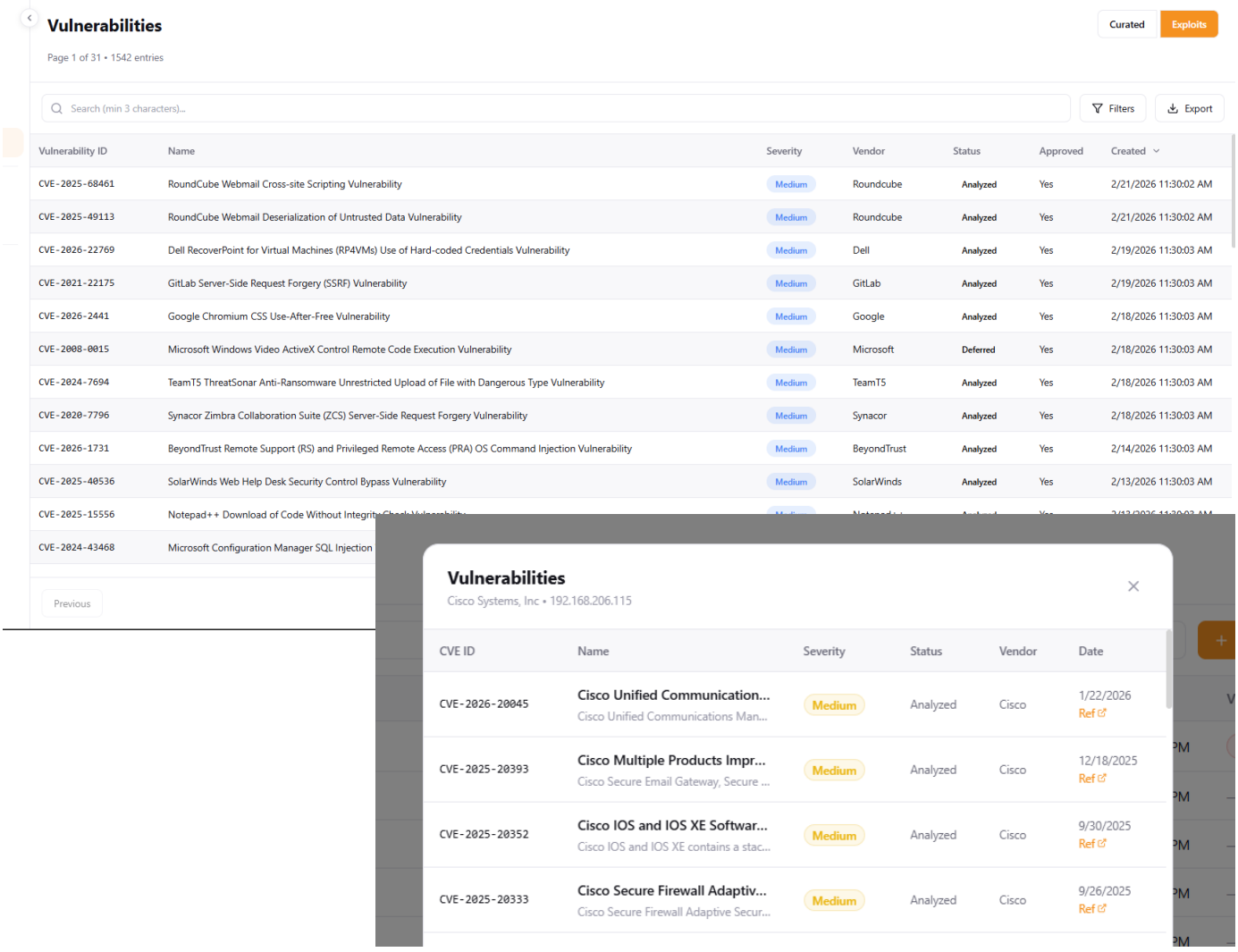
SafeLinx uses behavioural analytics, signature-based detection, and anomaly monitoring to identify known and unknown threats. It provides automatic detection of new hosts, devices, or communication links. The solution also detects new protocols and behavioural changes in IoT devices. For forensics purposes, alerts include packet capture (PCAP) files of the event that triggered the alert.



Comprehensive Vulnerability Management

SafeLinx consolidates all known vulnerabilities across IoT and OT assets into a single, centralized view. From high-level dashboards to device-level details, the platform provides the insights needed to understand exposure and take corrective action.

SafeLinx delivers threat intelligence that is purpose-built for IoT and OT environments, going beyond generic IT feeds. Every asset, alert, and vulnerability is automatically enriched with context on known exploits, vendor-specific CVEs, and real-world attack data.



SafeLinx delivers unified visibility, in-depth asset intelligence, and IoT-specific threat detection to secure your connected environment. By combining real-time monitoring, actionable alerts, and proactive vulnerability management, SafeLinx empowers security teams to reduce risk, streamline operations, and confidently protect their IoT and OT assets against evolving threats.

- SafeLinx gives you complete visibility, real-time threat detection, and actionable intelligence — all in one unified IoT security platform.
- Protect your connected devices, secure your operations, and reduce risk with a solution built specifically for IoT and OT environments.
- With SafeLinx, gain confidence in your IoT security posture and stay ahead of emerging threats.
- From asset discovery to vulnerability management and threat intelligence, SafeLinx empowers teams to see more, understand faster, and respond smarter.
- Simple to deploy, strong in protection — SafeLinx secures your IoT ecosystem without adding operational complexity.
- Turn IoT visibility and insights into proactive defense, minimizing downtime and maximizing operational resilience.

analyzet

Protecting and Empowering the IoT Industry

At Analyzet, we understand that IoT and OT environments are the backbone of modern industries — from manufacturing and energy to healthcare and smart cities. These connected devices drive operational efficiency, but they also introduce unique security challenges that traditional IT security tools are not designed to handle.

SafeLinx reflects our commitment to protecting every layer of the IoT ecosystem. By providing unified visibility, real-time threat detection, and actionable intelligence, SafeLinx enables organizations to:

Enhance Operational Awareness – Know exactly what devices are connected, how they communicate, and where vulnerabilities exist.

Reduce Risk Exposure – Identify and remediate high-risk devices before they are exploited.

Improve Security Efficiency – Minimize false positives, prioritize alerts, and accelerate incident response.

Ensure Business Continuity – Protect critical operations and industrial processes from cyber disruptions.

Future-Proof IoT Security – Adapt to evolving IoT threats and emerging devices with continuous updates and intelligence.

With SafeLinx, Analyzet empowers organizations to operate IoT and OT environments safely and confidently, strengthening both security posture and operational performance.

Notice

This document contains information about the proprietary property of Analyzet. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of Analyzet.

Nothing in this document constitutes a guarantee, warranty, or license, express or implied. Analyzet disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to Fitness for a particular purpose; merchantability; not infringement of intellectual property or other rights of any third party or of Analyzet; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technology discussed
herein and is advised to seek the advice of competent legal counsel, without obligation of Analyzet.

Analyzet retains the right to make changes to this document at any time, without notice. Analyzet makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein.

Copyright

Analyzet

Dubai Silicon Oasis, Dubai, United Arab Emirates.
analyzet.com | contact@analyzet.com | +971 50 513 3973