FIREDOME

Firedome Endpoint Protection Data sheet

Firedome Endpoint Protection for IoT – Datasheet

Real-time Cybersecurity for IoT Manufacturers

Firedome works with leading manufacturers to differentiate them with proactive, real-time cybersecurity on their device base. An AI-based, software-only solution for autonomous threat resolution to establish device makers as security leaders in their space, while reducing the risk of cyber-attacks and reducing operating costs across functions.

Firedome Endpoint Protection

A multi-layered holistic security platform for IoT manufacturers: autonomous, real-time prevention, detection, and response, eliminating security breaches, decreasing operational costs, and reducing emergency firmware upgrades.

With an AI-powered, software-only agent, 24/7 SOC, and constantly updated threat intelligence, Firedome Endpoint Protection delivers the peace of mind of knowing threats are mitigated in real time, without the need for manufacturer intervention.

Proactive Protection From IoT Cyber Threats

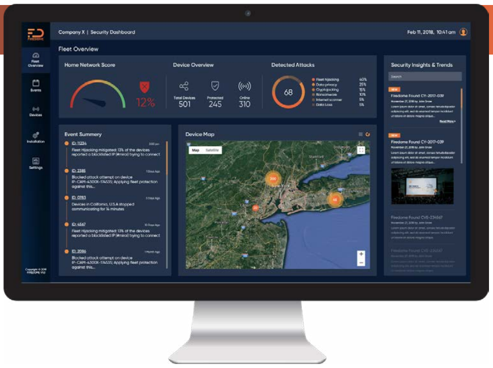
Protect your device base from viruses, malware, rootkits, trojans, and other threats that security built in during manufacturing (Security By Design) can not protect against:

- IoT Botnets
- IoT Malware, Ransomware, Cryptominers, Backdoors
- Network Attacks: Man-In-The-Middle, ARP / DNS Spoofing, DNS Rebinding
- Vulnerability & Online Bot Scanners (Shodan, ZoomEye, etc)
- Unknown 0-Day Exploits (including remote code execution)
- 1-Day Yet-unpatched Vulnerabilities
- Denial of Service (DoS) Attacks

Securing the Connected Future

For on going support and question about Firedome contact:
www.firedome.io | support@firedome.io | +1 (374) 826-6713 |

Management Platform: Monitor, Enforce Policies



Event Summary

- ID: 11234 — 3:00 pm — Fleet Hijacking mitigated: 13% of the devices reported a blacklisted IP (#mirai) trying to connect
- ID: 2385 — 1 Days Ago — Blocked attack attempt on device IP-CAM-4300X-174535; Applying fleet protection against this...
- ID: 0783 — 3 Days Ago — Devices in California, U.S.A stopped communicating for 14 minutes
- ID: 4567 — 10 Days Ago — Fleet Hijacking mitigated: 13% of the devices reported a blacklisted IP (#mirai) trying to connect
- ID: 2086 — 1 Month Ago — Blocked attack attempt on device IP-CAM-4300X-174535; Applying fleet protection against this...

NEW Firedome Found CY-2017-039 — November 21, 2018 by John Snow — Read More ›

NEW Firedome Found CY-2017-039 — November 21, 2018 by John Snow

Firedome Found CVE-234567 — November 21, 2018 by John Snow

Centralized management and enforcement is the key to effective and efficient protection. The Firedome platform provides centralized visibility, policy configuration and enforcement:

- Web Dashboard & API (Full Fleet Visibility)
- Network Communication Enforcement (Firewall)
- Executables Enforcement (Application Whitelisting Control)
- Cyber Protection Capabilities Configuration

Compliance & Regulations

The Firedome platform enables you to obtain compliance against an industry-accepted security standard like PCI DSS, APRA or ISO 27001 by demonstrating that you have applied documented vulnerability & risk management standards against all systems within the scope of assessment.

State of The Art Cyber Protection

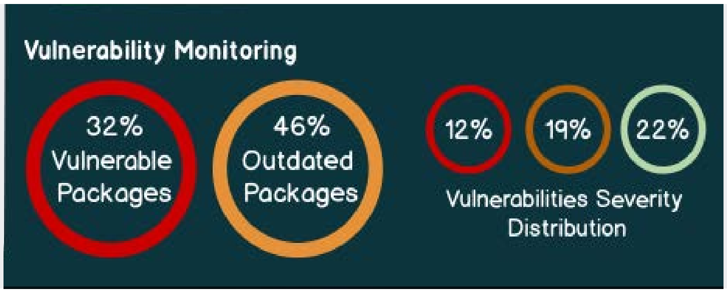
Machine Learning Cloud Engine

The AI-powered engine gathers complex event sequences and processes from the entire fleet and protects devices using three features:

- Threat Intelligence Engine - detecting both Network & OS layer activities
- Behavioral-based Analytics Engine
- Fleet-level Security Heuristics
- Operational Insights (real-time visibility to the fleet’s dynamic behavior. For example data about online, disappeared, network-jittering and constantly crashing devices)
- Deployed Honeypots Worldwide

Fleet Risk Visibility & Prevention

- Real-time Vulnerability Monitoring
  - Receive real-time alerts about installed or used software with existing vulnerabilities
  - Get real-time visibility to the security status of their deployed devices worldwide
  - Save R&D costs related to patch management and vulnerability monitoring



- Real-time Security Hardening
  - Scan for, constantly monitor and fix security misconfigurations in a fleet’s devices based on the most recent *CIS* (the ***C****enter of* ***I****nternet* ***S****ecurity*) *Benchmarks.*

461
Risks Remediated by Firedome
239
Existing Security Configuration Issues

CIS Controls and Benchmarks are global standards for internet security and are recognized as a global best practice for securing systems and data against attacks.

Firedome has implemented thousands of different CIS benchmarks, targeting a variety of OS and Linux distros, in order to provide better protection for our customers..

Securing the Connected Future

For on going support and question about Firedome contact:
www.firedome.io | support@firedome.io | +1 (374) 826-6713 |

Network Intrusion Detection & Protection

- Network Attacks Protection
- SecureDNS - *Encrypting Device's DNS Traffic*
- TCP/IP, DNS & Ports Monitoring
- Bruteforce & Port Scanning Protection
- ARP Poisoning Protection

Host Intrusion Detection & Protection

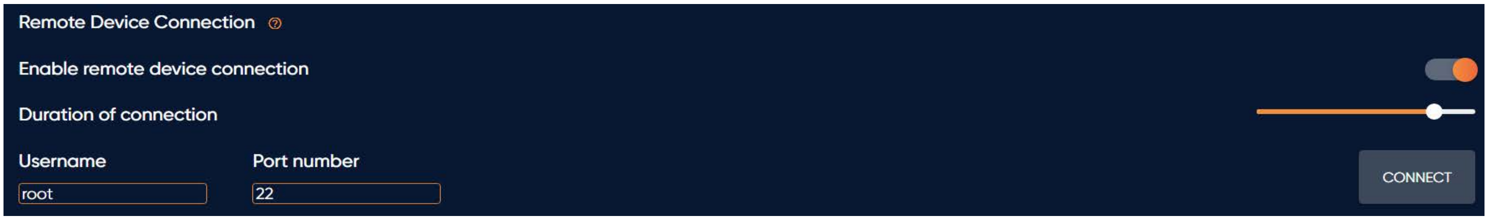
- Abnormal Behavior-based Protection - *0-Day Remote Code Execution & Malwares Protection*
- Signature-based Protection (Antivirus)
- Application Whitelisting
- FireWaf - Embedded Web Server Protection

24/7 Security Operation Center

Our solution includes a dedicated Security Operations Team (SOC) that conducts research, data analysis, security event investigations and offers 24/7 cybersecurity support. SOC teams help IoT manufacturers gain knowledge and make optimal decisions regarding anomalies, intrusion detection, and event analytics. They respond to "grey area" events that are flagged as suspicious but may not necessarily be malicious, so they would not be blocked automatically.

Value Beyond Just Cyber Protection: Secure Remote Access

Allows access to remote devices via an encrypted TCP tunnel, which is secured and provided by Firedome. With this connection, you can access remote devices (for example by SSH), that reside behind a NAT without the security concern and technical difficulty of *port forwarding* or another vulnerable/costly communication method.



Remote Device Connection

Enable remote device connection

Duration of connection

Username: root

Port number: 22

Agent Specifications & Deployment

- OS: any-kind of Linux distribution
- Arch: x86/x64, MIPS, ARM & more
- Storage: < 2MB, Memory: 16MB
- CPU: < 3%

User Mode Package: Added to the device's boot sequence, running in user mode (*root)* without kernel changes, lowering the integration's complexity and risk level.

Aftermarket: Agent can be installed on already deployed devices as part of a firmware/software update.

Securing the Connected Future

For on going support and question about Firedome contact:
www.firedome.io | support@firedome.io | +1 (374) 826-6713 | Copyright © 2020 FIREDOME