DATA SHEET

Building Defender™ Platform

Detect and prevent cyberattacks on building management systems (BMS) with Building Defender™.

INDUSTRIAL DEFENDER®

Building Defender Platform

CYBER THREAT DETECTION FOR BMS

Buildings are a critical asset that need cybersecurity protection. In the average large commercial or institutional building, there are more building management system (BMS) devices than user computers. Thousands of BMS devices are installed on corporate networks, making them an easy attack vector into critical building systems, and a potential launching pad to compromise valuable enterprise data. With Building Defender™, facilities engineers and IT professionals can address the ever-expanding cyber threat landscape with safe and effective cybersecurity data collection, monitoring, and management for BMS systems and devices.

By combining multiple applications on a single platform, it provides a consolidated real-time view to secure and manage your BMS environment. Building Defender™ sensors analyze systems, devices and network traffic using popular building management system protocols such as BACnet and Modbus. Using this information, our platform creates an asset baseline, which can then be continuously monitored for any changes that could indicate a cyberattack. After an anomaly is detected, it's immediately delivered to the central management console, and an alert is sent to the appropriate parties with actionable data for remediation actions.

Building Defender can be deployed either as a dedicated appliance or optionally as a Virtual Machine (VM).

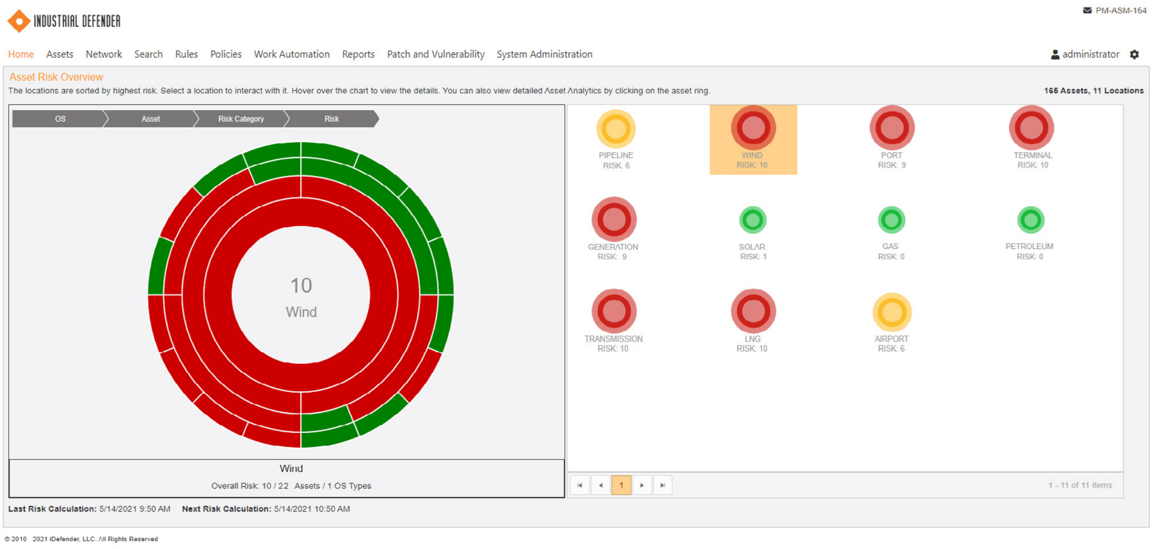
Building Defender Features and Capabilities

- Building management system cybersecurity, operations, and compliance in a single view
- Cyber threat detection and alerting
- Event logging, correlation and archiving
- Collect baselines and report on settings, accounts and configurations
- Analyze changes across the BMS
- Vulnerability monitoring to reduce risk from emerging threats
- Software inventory
- User account change identification
- Report subscriptions
- Customizable user interface dashboards

- Scalable architecture, virtual machines to dedicated appliances
- Monitor file level changes
- Network traffic monitoring
- Critical process and service monitoring
- Systems health and performance monitoring
- Manage hardened security perimeter
- Interoperable with 3rd party security technologies
- Default policies for the NIST CSF
- Automated configuration change notification
- Automate change management processes
- Device configuration file archiving

Key Benefits

- Visualize your BMS device health using our asset topology and Endpoint Risk Analytics Suite
- Drill down to monitor trends, manage events and investigate anomalies
- Reduce cybersecurity risks to BMS devices with on-demand vulnerability management
- Monitor systems performance including application and process failures, registry and file changes
- Detect cyber threats across your BMS and at your perimeter
- Improve situational awareness and reduce total cost of ownership with multiple applications on a single platform
- Streamline compliance reporting with automated data collection and storage
- Leverage built-in NIST policy libraries and reporting templates
- Reduction of BMS operating costs by automating system integrity and revision level reporting



Asset Risk Overview

The locations are sorted by highest risk. Select a location to interact with it. Hover over the chart to view the details. You can also view detailed Asset Analytics by clicking on the asset ring.

165 Assets, 11 Locations

Wind

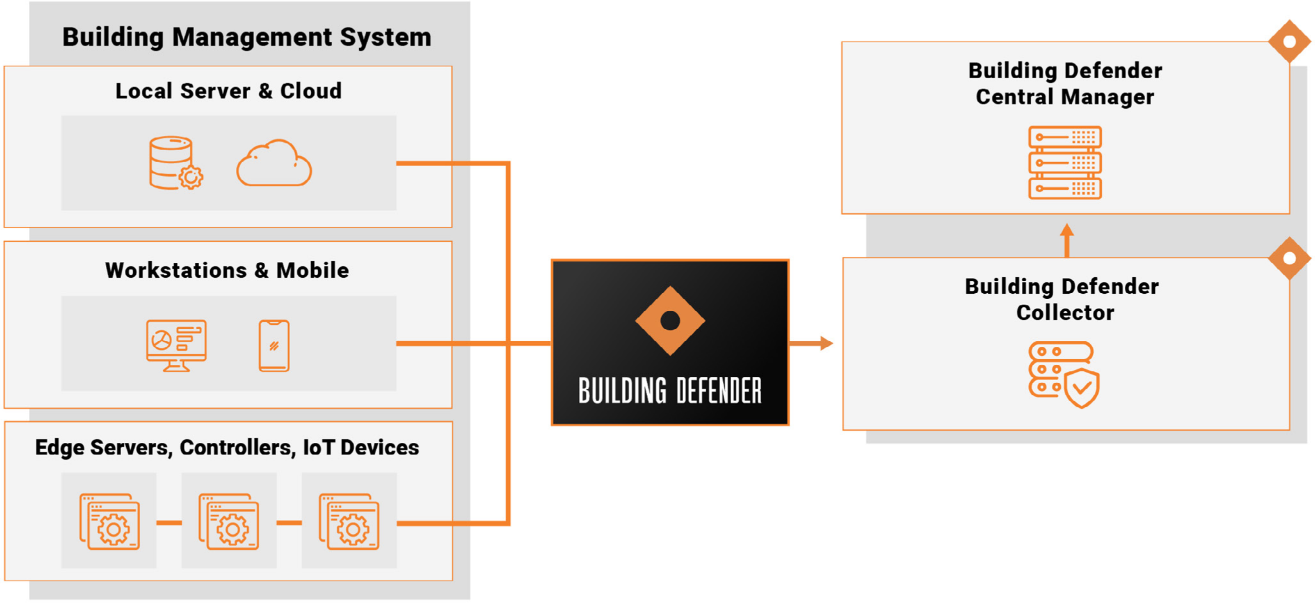
Overall Risk: 10 / 22 Assets / 1 OS Types

Last Risk Calculation: 5/14/2021 9:50 AM **Next Risk Calculation:** 5/14/2021 10:50 AM

© 2010 2021 iDefender, LLC. All Rights Reserved

The Endpoint Risk Analytics Suite

Building Defender Architecture


Building Management System
Local Server & Cloud
Workstations & Mobile
Edge Servers, Controllers, IoT Devices
BUILDING DEFENDER
Building Defender Central Manager
Building Defender Collector

Building Defender Components

The Building Defender infrastructure consists of two interrelated components:

- **Building Defender Central Manager (BDCM)**
- **Building Defender Collector (BDC)**

This infrastructure can be deployed at your locations with no disruption to operations and no reboot required. The vendor-agnostic solution is tuned to collect data from 100+ types of industrial endpoints and report on baseline deviations, alert on priority security events and flag policy violations. With up-todate information operators can confidently manage users, compliance reporting, patches, security events and incident response from a single, unified view.

Building Defender Central Manager (BDCM)

The BDCM can be deployed either as a dedicated appliance or optionally as a Virtual Machine (VM) providing aggregation, analysis, visualization, alerting and reporting to security teams. Once the appliance is turned on, users can immediately start receiving data out-of-the-box without complicated set up or third party integrations, like a well-tuned control system.

BDCM Appliance Specifications

Platform Feature	Normal Throughput	Extreme Throughput
Rack Configuration	2U Server	2U Server
Processor	2 x Intel® Xeon®; 8 core; 1.7 Ghz	2 x Intel® Xeon® E5 v3; 8 core; 2.6 Ghz
Memory	48GB DDR4-2666	384GB DDR4-2666
Network	4 x 100/1000/10GBase-T	4 x 100/1000/10GBase-T
Network Adapter	RJ-45 Copper	RJ-45 Copper
Storage	14 x 960GB SSD SATA drives	14 x 1.9TB SSD SATA
Data Storage Method	RAID-1 and RAID-6	RAID-10
USB	4 x USB, 1 x Serial	4 x USB, 1 x Serial
Drive Insertion Strategy	Hot Swap	Hot Swap
Video	Integrated VGA	Integrated VGA
Power Supplies	Dual, Hot-Swappable	Dual, Hot-Swappable
Power Input	100—240 VAC; 50-60Hz	100—240 VAC; 50-60Hz
Power Output	920 Watts	920 Watts
BTU Output	3137 BTU/Hour	3137 BTU/Hour
Mechanical Cooling	Fan cooled; redundant fans	Fan cooled; redundant fans
Dimensions (H X W X D)	3.5 x 17.2 x 24.8 in.; 89 x 437 x 630 mm	3.5 x 17.2 x 24.8 in.; 89 x 437 x 630 mm
Weight	61 lbs; 27.7 Kg	61 lbs; 27.7 Kg

Building Defender Collector (BDC)

The Building Defender Collector (BDC) monitor all network traffic within the control network security perimeter, enabling detection of internally generated attacks, as well as any attacks that may have circumvented perimeter defenses. The BDC includes the ability to monitor industry standard protocols used by process control systems such as Modbus TCP, DNP3, Profibus, ODVA Ethernet/IP, and ICCP, and generate alarms that are sent to the BDCM for logging and diagnosis.

BDC Appliance Specifications

Platform Feature	Normal Throughput	Extreme Throughput
Rack Configuration	1U Appliance	1U Appliance
Processor	Intel® Xeon® Silver; 8 cores; 1.8 Ghz	Intel® Xeon® Scalable Bronze; 6 cores; 1.7 Ghz
Memory	48GB DDR4-2666	96GB DDR4-2400
Network	2 x 100/1000/10GBase-T; 4 x 10/100/1000Base-T	8 x 100/1000/10GBase-T
Network Ports	RJ-45 Copper	RJ-45 Copper
Storage	1 x 960GB SATA SSD	2 x 960GB SATA SSD; RAID-1
USB	4 x USB; 1 x Serial	2 x USB; 1 x Serial
Drive Insertion Strategy	Fixed	Hot Swap
Video	Integrated VGA	Integrated VGA
Power Supplies	Single, auto-sensing	Redundant pair, auto-sensing; Hot swappable
Power Input	100—240 VAC; 50-60Hz	100—240 VAC; 50-60Hz
Power Output	350 Watts	750 Watts
BTU Output	1200 BTU/Hour	2,560 BTU/Hour
Mechanical Cooling	Air Cooled, 2 x fans	Air Cooled, 8 x heavy duty fans
Dimensions (H X W X D)	1.7 x 17.2 x 14.5 inches; 43 x 437 x 368 mm	1.7 x 17.2 x 28.5 inches; 43 x 437 x 724 mm
Weight	14 lbs; 6.35 Kg	26 lbs; 11.8 Kg

THE INDUSTRIAL DEFENDER DIFFERENCE

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. They secure some of the largest critical control system deployments with vendors such as GE, Honeywell, ABB, Siemens, Schneider Electric, Yokogawa and others to protect the availability and safety of these systems, simplify standards and regulatory requirements, and unite OT and IT teams.

Planning an OT Security Project?

SCHEDULE A DEMO

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com
225 Foxborough Blvd, Foxborough, MA 02035
industrialdefender.com

INDUSTRIAL DEFENDER®