Bacon Unlimited Datasheet

Bacon Unlimited® is an Endpoint Management & Vulnerability Remediation platform that allows system administrators to automate away the deluge of admin tasks that needed on their endpoints each week.

When you select Bacon for your environment you will be able to Proactively optimize your endpoints en masse and react in real-time to user problems.

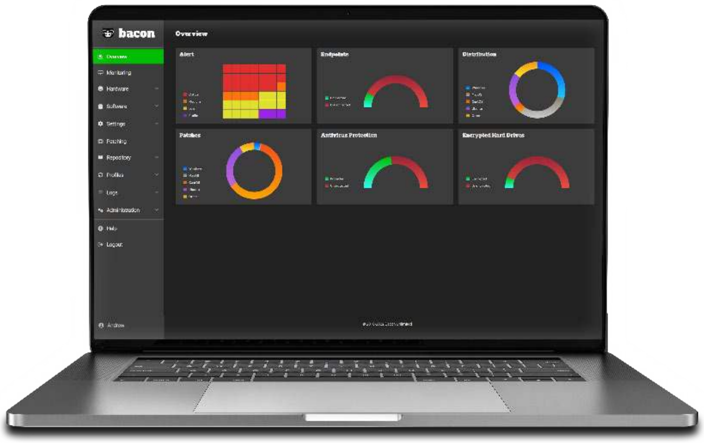
Windows 11 macOS redhat tv
Windows Server debian ubuntu
Windows 10 KALI CentOS iOS
Amazon Linux AlmaLinux Rocky Linux

ARCHITECTURE

Bacon is a **web application** that utilizes a powerful, easy-to-use interface, allowing for the configuration, control, automation, and monitoring of endpoint health and security.

Central to Bacon are **endpoints**—any general-purpose server, workstation, or laptop, that runs a Windows, Linux, or macOS operating system—connected and constantly exchanging information securely with Bacon. Bacon runs background jobs to continuously collect information from its endpoints and remediate vulnerabilities using patch management, package deployment, config control, and script execution.

Made by IT people for IT people.®



Finally, complete vulnerability control from one, easy-to-use platform.

Total Vulnerability Remediation	Cross Platform	Real-Time Reporting	Intuitive Interface
Tenable VM & SC Integrated	Real-Time Configuration	Multi-System Patching	Custom Scripting
NIST CVE Matching	CISA KEV Alerting	3rd Party Software Patching	Remote Control

Bacon v5.0 Features

Vulnerability Remediation

- See all CVEs for endpoints
- See CVEs listed on CISA KEV
- Tenable Integration for added visibility
- Fix all actionable Vulnerabilities
- Adjustable Reporting

Overview Dashboard

- Easy-to-use interface
- Summary of information
- Endpoint connectivity, antivirus, operating platform distribution, encrypted volumes
- Click-through interface

Connected Endpoints

- View/collect/export data
- Supports Windows, macOS, and Linux
- Collected information includes hardware system info, network interface, available patches, installed software, and services
- Static & dynamic groups
- Tracking Kernel version and VM type
- Schedule jobs on endpoint reconnection

Patching

- Windows & Linux—All Updates
- macOS and IOS—System Updates
- Manage updates/patches on all endpoints in use today
- Patch History Reporting
- Relentless mode
- Run when connected
- Proactive third-party application patching

Software Deployment & Scripting

- Manage and automate 3rd party updates
- Push data files to endpoints
- Create pre- and post- install steps
- Perform chained application installations
- Install as user
- Run at a scheduled time or when next connected

Additional Security Features

- Control Every Policy and Setting on Every System
- Active directory authentication
- 2-factor authentication
- Monitor antivirus
- Complete audit logging of admin actions
- Enhanced role-based access control
- SAML based Single Sign-On Support (MS Entra/Azure AD and Okta)

Remote Connection

- Connection to physical and virtual machines
- View and control a desktop connection
- Open a back-end terminal session
- Upload, download, modify files in filesystem browser

Monitoring

- Monitor workstations and servers
- Rules can be created for alerting on connectivity, windows service, memory threshold, CPU threshold, and disk threshold
- Email notifications for triggered alerts
- Out of date or missing software
- Event-based monitors
- Automatic monitoring of configuration compliance

bacon

Upcoming Features

- Advanced Approval & Scheduling
- Vulnerability Exemptions

Installation Requirements

If not using SAAS:

- Direct internet access for initial setup
- Server Minimum Requirements:
  - Operating System: Ubuntu 22.04
  - CPU: 2 Cores
  - RAM: 4GB
  - Storage: 150GB
- The following ports must be opened to the server:
  - Outbound: 25, 53, 389, 587, 2197
  - Inbound: 4505-4509
  - Inbound (for admin network): 22 , 443

Schedule Your Bacon Demo Today @

baconunlimited.com