



VIBRANIUM[®]

EPS

END POINT SECURITY

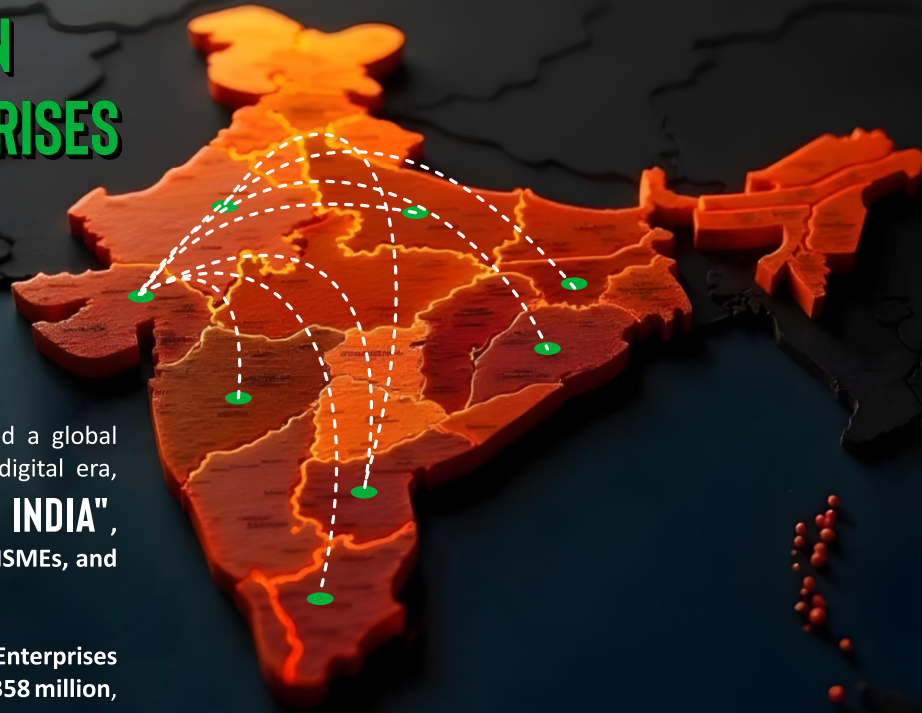
ADMINCONSOLE

ENTERPRISE EDITION

Ai-Cybersecurity - Simple and Strong...

“RANKED **NO.1** ANTIVIRUS GLOBALLY”

A NATION OF INSPIRATION & EMERGING ENTERPRISES



India has always been a nation of inspiration and a global business hub since ancient times. Today, in the digital era, **INDIA HAS EMERGED AS THE "NEW INDIA"**, establishing itself as the **Land of Startups, SMEs, MSMEs, and Medium Enterprises** across the globe.

With approximately **70 million Small and Medium Enterprises (SMEs)** in India alone in 2023, out of a global total of **358 million**, their contribution is monumental. SMEs and MSMEs represent **more than 27% of India's National GDP**, serving as the true backbone of the Indian economy.

THE RISING NEED FOR CYBERSECURITY AND DATA PROTECTION

- The backbone of modern India-SMEs and MSMEs-faces mounting risks in today's interconnected digital landscape.
- Cyberattacks are no longer isolated incidents, they can strike anywhere, at any time.
- Attackers and hackers specifically target Vulnerable businesses with weak Defenses.
- In 2023, 64% of SME organizations in India were hit by cybercriminals and ransomware attacks.
- Alarmingly, 65% of these affected businesses paid the ransom, yet only 8% managed to recover their data even after paying.

VIBRANIUM, committed to the mission of **#ransomfreeindia**, has developed innovative solutions to combat unpredictable cyberattacks and mitigate rising risks, delivering robust protection against emerging threats.

KEY BENEFITS AND FEATURES

AI-DRIVEN CYBERSECURITY

ADVANCED ANTI-RANSOMWARE

ENCRYPTED DATA BACKUP

APPLICATION CONTROL

WEB FILTERING

DATA LEAKAGE PREVENTION

EMPLOYEE TRACKING

ASSET MANAGEMENT

SYSTEM AUDIT

VIBRANIUM® EPS SECURITY | SIMPLICITY | SCALABILITY

Every line of code and each module has been thoughtfully developed and designed based on feedback and suggestions from IT administrators and CEOs-insights gathered through surveys highlighting their biggest challenges in scaling business growth due to data protection requirements, organizational tracking needs, and overall system complexity.

CEO'S

First Choice ✓

VIBRANIUM EPS

Fastest, Lightest, Strongest, Simplest

The Circle of Organizational Growth

“Growth” in today’s interconnected digital world begins with impenetrable data and privacy protection against internal or external threats, ransomware, and unauthorized access. Tracking workforce performance and analysing data drives process improvements and efficiency. This seamless cycle culminates in sustainable growth.

VIBRANIUM EPS & Admin Console empowers Indian businesses & Enterprises with AI-driven cybersecurity, real-time productivity tracking, and effortless policy deployment. Designed for simplicity and strength, it ensures data safety while accelerating organizational excellence.

**E
P
S**

ENHANCED DETECTION

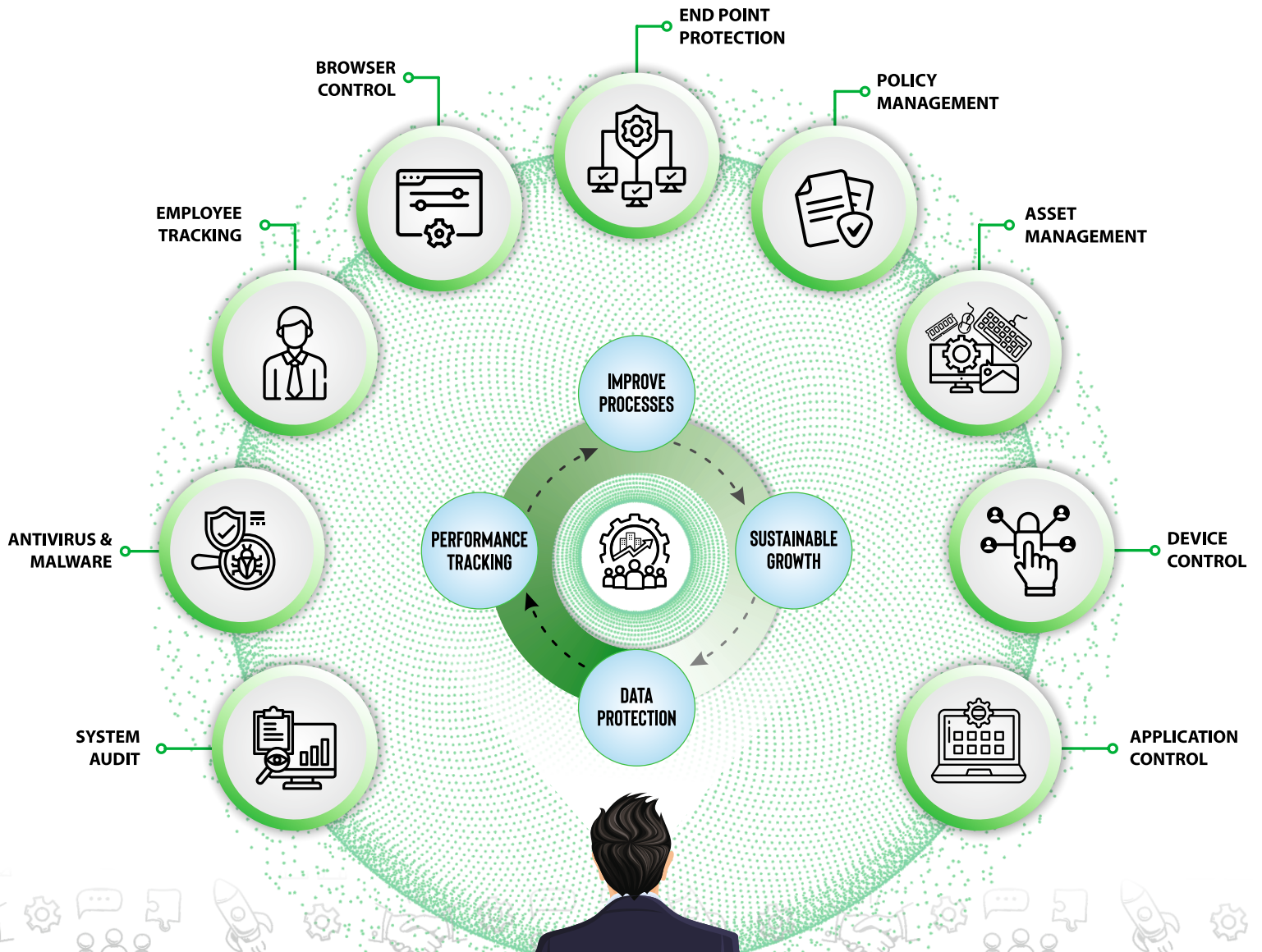
• *Ai-Driven Advanced Malware Detection.*

PRODUCTIVITY TRACKING

• *Real-time measurement of employee activity.*

SIMPLIFIED DEPLOYMENT

• *Effortless installation, easy setup & Deployment.*



Ai-Cybersecurity - Simple and Strong...

 **STRONGEST** **BlueDome.AI**

Ai-Driven **ZERO TRUST** Malware Detection & Remediation Technology

BlueDome.AI Detection

BlueDome.AI utilizes state-of-the-art AI technologies to enhance its threat detection and response functions.

By leveraging the most recent developments in artificial intelligence, BlueDome.AI effectively identifies and categorizes cybersecurity threats, providing prompt alerts and practical insights. This AI-driven approach positions BlueDome.AI as a leader in cybersecurity innovations, equipping users with a robust defense against new emerging cyber threats.

BlueDome.AI Heuristic Detection

Our heuristic detection protocols employ embedded algorithms that incorporate both statistical and analytical approaches to analyze files and their components. These protocols implement targeted rules alongside analytical techniques to optimize the scanning of objects. Although the outcomes may not always be conclusive, they are strong enough to flag potential threats, designating the samples as suspicious and thereby enhancing our overall threat detection effectiveness.

VIBRANIUM, thoroughly tested by



Tested By PC Security Channel – UK (By Private Evaluation Test) in January 2023.

with 10,000 Zero-Hour Malware Detection tests, has been certified with

100% MALWARE DETECTION TESTED ✓



DEEP DIVE



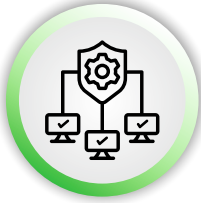
DEEP EXPLOIT



DEEP SCRIPT



DEEP LOOK



END POINT PROTECTION

Vibranium **Endpoint Security (EPS)** redefines endpoint protection with proactive AI detection and behavior-based defense, leveraging heuristic and advanced machine learning technologies.

The **Proactive Behavioral Analysis Engine** provides real-time ransomware defense by monitoring all processes and blocking suspicious activities resembling ransomware or cryptic threats. It also enables **real-time blocking of malicious IP traffic** carrying malware, ensuring comprehensive protection against evolving cyber threats.

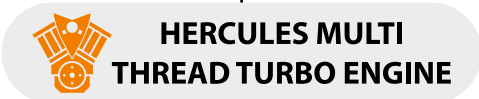
With the **Bludome.AI Live Updater**, EPS ensures instant updates, continuous monitoring, and real-time insights into endpoint security. Administrators can refine event data for targeted analysis, maintaining robust protection across all devices under management.

VIBRANIUM EPS leads the way in cybersecurity innovation, seamlessly integrating traditional malware detection with advanced AI and ML technologies to deliver impenetrable endpoint security and unparalleled data privacy.



TRADITIONAL

MODERN



• Signature-Based Detection

Malware detection identifies threats by comparing files against a database of known malware signatures.

• Heuristic-Based Detection

Malware detection identifies potential threats by examining code for unusual or malicious-like patterns.

• Behavioral-Based Detection

Identifies threats by monitoring and analyzing actions taken by programs during execution.

• Reputation-Based Detection

Assesses threats by evaluating the known credibility or trustworthiness of files, domains, or IP addresses.

• Emulation-Based Detection

Analyzes threats by running code in a virtual environment.

• DEEP DIVE

AI-driven in-depth analysis to detect unknown malware.

• DEEP SCRIPT

AI-driven prevention of cross-site scripting (XSS) and malicious code injection.

• DEEP EXPLOIT

AI-driven vulnerability mitigation and exploit prevention.

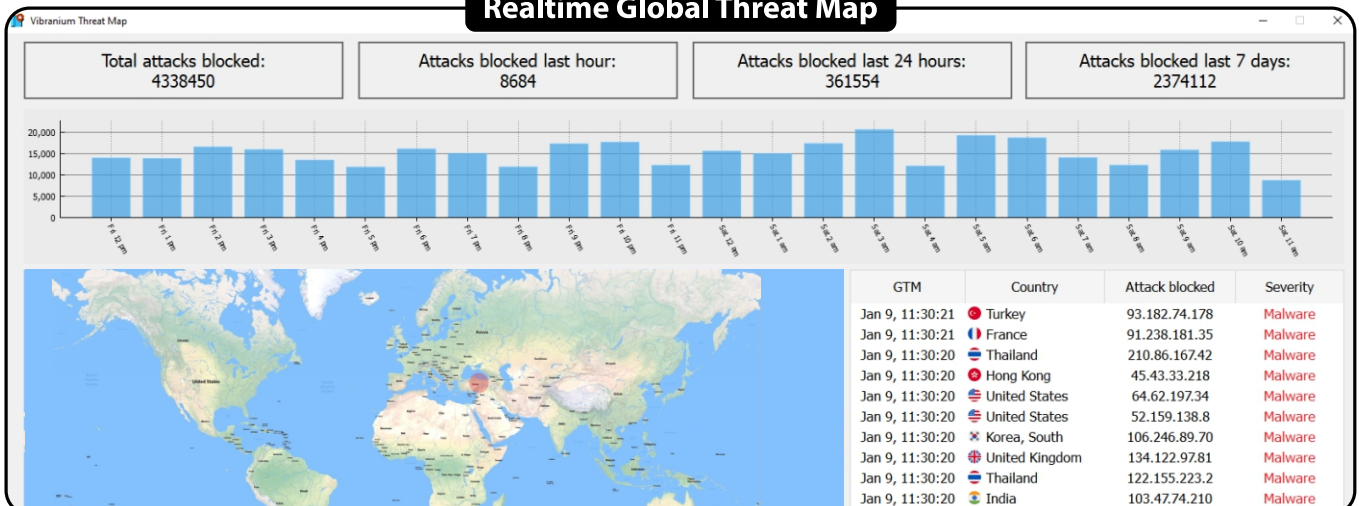
• DEEP LOOK

AI-Driven inspecting network traffic and packet filtering.

• KERNEL PROTECTION

Shielding Windows' core kernel, the spine of system, from threats.

Realtime Global Threat Map






DATAKNOX

**UNBREAKABLE PROTECTION,
EFFORTLESS RESTORATION**

VIBRANIUM DATA KNOX is a highly secure, automated, and easily configurable smart data backup module integrated with VIBRANIUM EPS for endpoint users. It allows seamless access for both endpoint users and administrators, based on policies deployed by the administrator.

With DATA KNOX, you can schedule regular backups of files in an encrypted and compressed format, ensuring data security and efficiency. It supports a wide range of file extensions, including doc, docx, ods, wps, wpd, pdf, xls, xlsx, csv, odp, one, pptx, ppt, ppsx, pps, rels, and more. Backups are stored on the drive with the most available free space, optimizing storage use.

In case of a disaster, DATA KNOX enables hassle-free and efficient restoration of data, ensuring minimal downtime and maximum convenience.



BACKUP

VIBRANIUM DATA KNOX is modern technology that provides highly compressed, military-grade encrypted manual and automatic schedule-configurable smart data backup. It supports auto-backup at the endpoint by extension, folder, or category, offering easy customization. Backed-up data by VIBRANIUM DATA KNOX is impenetrable by any cyberattacks or ransoms.



RESTORE

In the event of a disaster at an endpoint, administrators can effortlessly restore the latest backup using VIBRANIUM DATA Knox. They have the flexibility to choose whether to restore the data to its original location or to a new location of their preference, ensuring seamless and reliable data recovery.

VIBRANIUM DATA Knox is hybrid Data backup and Restoration technology for enterprise cybersecurity.

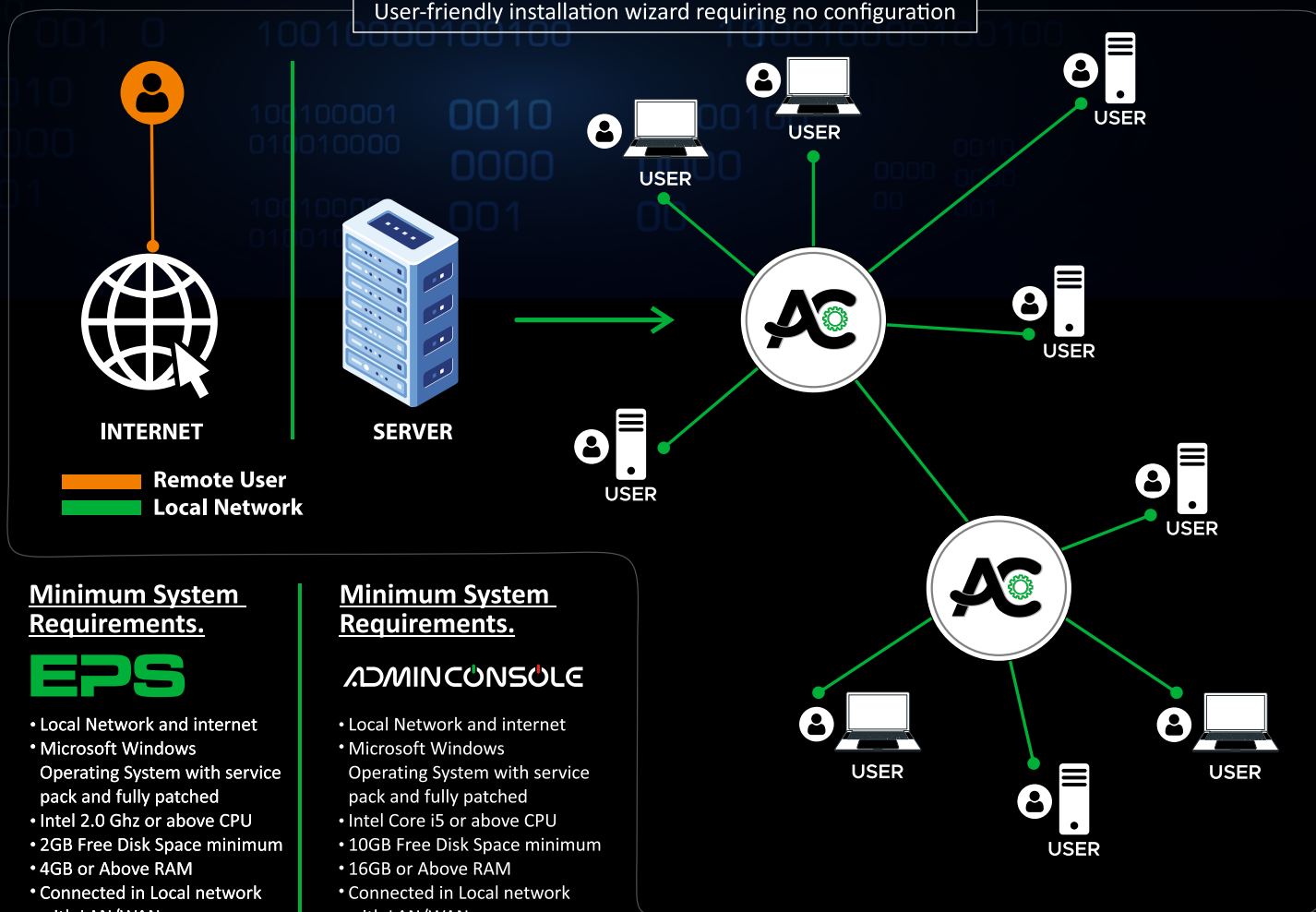
Installing, implementing, and deploying **Vibranium EPS** and the Admin Console is as Simple as making a cup of black coffee



SIMPLEST

The installation of Vibranium EPS and the Admin Console is built on Vibranium's foundational principles, providing advanced security with ease of use. Its user-friendly interface allows both users and administrators to interact seamlessly, maintaining top-notch protection without any complexity.

User-friendly installation wizard requiring no configuration



Minimum System Requirements.

EPS

- Local Network and internet
- Microsoft Windows Operating System with service pack and fully patched
- Intel 2.0 Ghz or above CPU
- 2GB Free Disk Space minimum
- 4GB or Above RAM
- Connected in Local network with LAN/WAN

Minimum System Requirements.

ADMINCONSOLE

- Local Network and internet
- Microsoft Windows Operating System with service pack and fully patched
- Intel Core i5 or above CPU
- 10GB Free Disk Space minimum
- 16GB or Above RAM
- Connected in Local network with LAN/WAN

FEATURES

ADMINCONSOLE



POLICY MANAGEMENT / DEPLOYMENT

Within the VIBRANIUM Admin Console, Policy Management and Deployment is the centralized process of creating, configuring, and distributing security policies to endpoint devices. Leveraging AI-driven automation, VIBRANIUM streamlines every stage of policy handling—from development and customization, to real-time deployment—ensuring that policies are consistently enforced across the network. Administrators can easily push policies to entire user groups or individual users, ensuring the flexibility and responsiveness needed to maintain a robust, enterprise-grade cybersecurity posture.

- **Scan Policy**

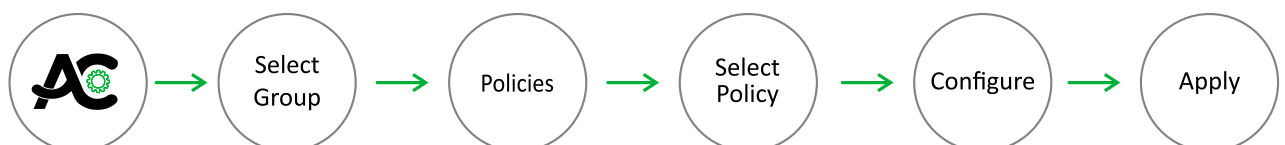
A Scan Policy in the VIBRANIUM Endpoint Security platform is a configurable set of rules that define how and when endpoint devices are scanned for threats. It specifies the scan scope, frequency, detection methods, and remediation actions, ensuring that endpoints remain proactively protected against malware, vulnerabilities, and unauthorized software.

- **Realtime Time Policy**

A Real-Time Threat Detection Policy in VIBRANIUM continuously monitors endpoints to instantly identify, flag, and neutralize potential malware. Guided by AI-driven techniques, it proactively adapts to emerging threats, allowing administrators to customize detection levels, responses, and exceptions—ensuring immediate, on-the-fly defense.

- **Update Policy**

An Update Policy in VIBRANIUM ensures endpoints consistently receive the latest security patches, threat definitions, and feature enhancements. Administrators can define scheduling, prioritize critical updates, and optimize distribution, guaranteeing that every device stays current, secure, and fully aligned with organizational requirements.





POLICY MANAGEMENT / DEPLOYMENT

• Logs Policy

A Logs Policy in VIBRANIUM defines how all endpoint-related logs—including daily user activity, quarantine actions, and various security event records—By determining what information to log, how long to retain it, administrators maintain a comprehensive audit trail for compliance, forensic analysis, and the ongoing enhancement of the organization's security posture

• Password Policy

A Password Policy in VIBRANIUM sets rules for creating and managing user credentials—such as complexity, length, and expiration—ensuring secure, compliant, and controlled access to protected systems.

• USB Policy (DLP)

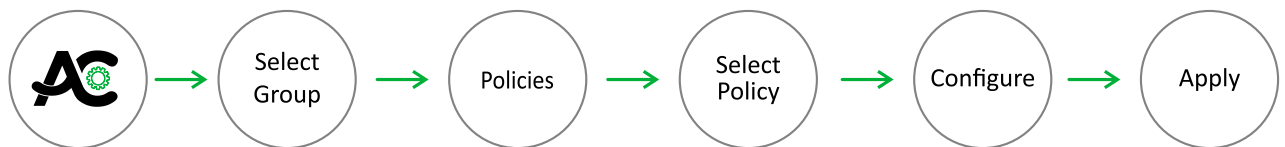
A USB DLP (Data Leakage Prevention) Policy in VIBRANIUM regulates how removable media devices are used on endpoints. It controls data transfer, restricts unauthorized device usage, and monitors file movements to prevent sensitive information leakage—maintaining strong data security and compliance standards.

• Bluedome Policy

A Bluedome.ai Policy in VIBRANIUM leverages advanced, AI-driven real-time malware detection techniques—Deep Dive, Deep Script, Deep Exploit, and Deep Look—to proactively identify and neutralize sophisticated cyber threats. By continuously analyzing code, scripts, and executable behaviors at multiple layers, this policy provides a comprehensive, adaptive defense strategy, ensuring endpoints remain protected against emerging and evasive attacks.

• Optimization Policy

An Optimization Policy in VIBRANIUM focuses on cleaning unnecessary files, removing junk data, and streamlining system resources. By regularly clearing clutter and fine-tuning performance parameters, administrators can ensure endpoints remain efficient, stable, and responsive—enhancing both user productivity and overall security posture.



APPLICATION CONTROL

• Application Blocking

Vibranium EPS robust Application Control module enables you to manage application execution on Windows endpoints by implementing block/whitelist policies and setting time restrictions. This functionality ensures that only approved applications can be accessed, while all other third-party applications are effectively blocked.

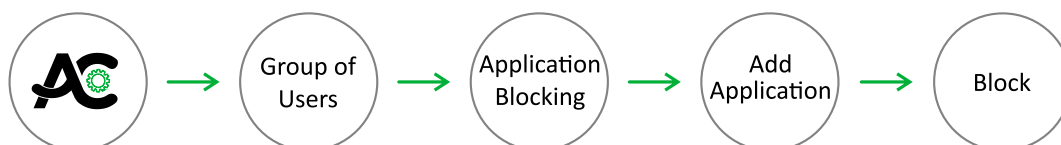
Administrators can effortlessly apply the Application Blocking policy to an entire group of users or individual users, both quickly and intuitively.

• Installed Application

Within the VIBRANIUM Admin Console, administrators can seamlessly view and analyse all applications installed on endpoint users' devices in real time. Detailed information, including application authenticity, publisher, version, and installation date, is readily available, enabling comprehensive oversight and informed decision-making.

• Running Application

Administrator can view and analyse each and every running application at the end point user at any moment of time on Realtime basis.





FASTEST

INSTALLATION TIME

EPS

ADMIN
CONSOLE

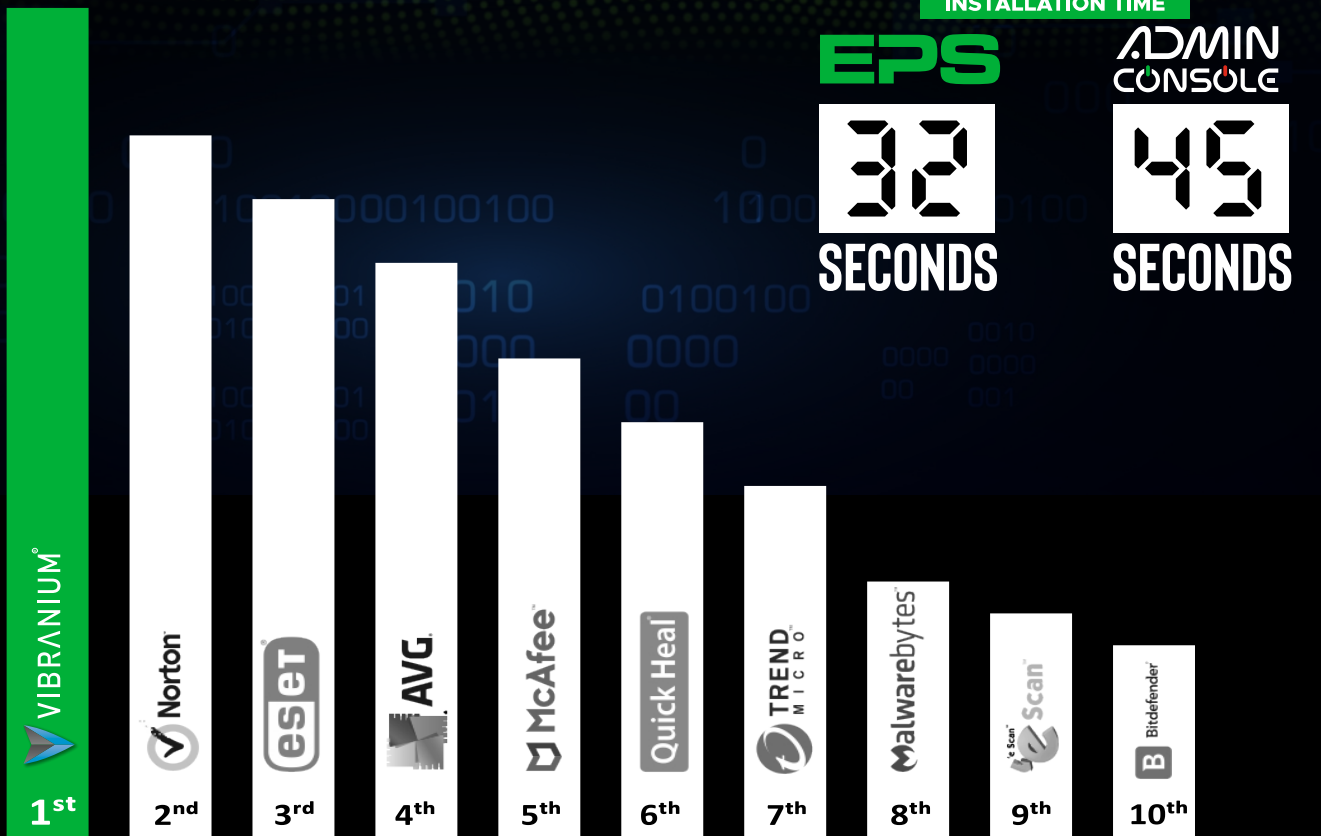
32

45

SECONDS

SECONDS

* HIGHER IS THE FASTEST



Performance test conducted by Passmark Software – Australia

Experience pure velocity with Vibranium-where “fastest” isn’t just a claim, it’s a defining principle. In a world driven by digital acceleration, every second counts. That’s why Vibranium is engineered for lightning-quick installation, seamless implementation, and rapid deployment, putting precious time back into your hands.

“Vibranium doesn’t raise the bar-it forges a whole new one.”

*“Measure What Matters
Proactive and Precise”*



EMPLOYEE TRACKING

What gets measured, gets managed. With proactive and real-time tracking, VIBRANIUM EPS and the Admin Console ensure precision, transforming insights into impactful decisions.

Employee activity and performance tracking not only safeguards data and privacy for enterprise organizations but also drives workforce productivity and operational efficiency, ensuring sustainable organizational growth.

Through VIBRANIUM EPS, administrators can monitor, analyze, and control every employee activity with precision and proactivity, ensuring maximum security and productivity.

Oversee workplace discipline. When an employee is aware that Employee Monitoring Software is active on their computer, they are likely to exhibit greater responsibility in their tasks. This leads to enhanced self-discipline, as individuals naturally desire to present themselves favourably, particularly in the presence of superiors.

Minimize organizational costs. Vibranium EPS for Insider Threat Detection through User Behavior Analytics serves as a cost-effective alternative to expensive measures like video surveillance and access control systems.

Time management in accounting involves monitoring the start and end of the workday, as well as tracking employees' lunch and smoke breaks. The Vibranium EPS User Activity Monitoring Software records the applications utilized by your employees. Through the generated reports, you can assess individual productivity levels, as well as the total hours worked daily, weekly, or over other specified periods.

KEY BENEFITS AND FEATURES

APPLICATION CONTROL

TIME TRACKER

FILE ACTIVITY MONITORING

REMOTE DESKTOP CONTROL

SCREENSHOTS

BROWSER HISTORY TRACKING

USB DEVICE ACTIVITY

DEVICE CONTROL

ASSET MANAGEMENT

WEB FILTERING

DEVICE UPDATES

SYSTEM AUDIT

GRAPHICAL PERFORMANCE VIEW

SCHEDULED DAILY
ACTIVITY REPORTS (EMAIL)



EMPLOYEE TRACKING

• Applications Events

Administrators can review and export real-time logs of applications accessed by endpoint users, complete with all necessary details. If any unauthorized or non-productive applications are detected, the administrator can effortlessly block them directly at the endpoint. By simply right-clicking the application, it can be restricted from further access, ensuring enhanced control and productivity.



• Time Tracker

Revolutionizing Workforce Productivity with VIBRANIUM Admin Console

The Time Tracker feature of the VIBRANIUM Admin Console is a lightning-fast, real-time tool that empowers administrators with actionable insights into employee activities during working hours. Utilizing intuitive color-coded categorization, administrators can effortlessly analyze time allocation across productive, non-productive, and neutral categories. This real-time visualization simplifies pattern identification and optimizes workforce productivity.

This innovative and unique approach not only streamlines monitoring but also provides a clear pathway to enhancing efficiency, making VIBRANIUM an indispensable tool for organizations striving for excellence.

Imagine having a dashboard that acts like a bird's eye view of your workforce's daily activities. With a glance, administrators can spot how employees allocate their time—whether they're deeply immersed in work or distracted by non-productive tasks. The color-coded insights make the data visually intuitive, allowing for faster decision-making and better productivity strategies. This ground-breaking feature transforms workforce management from a guessing game into a strategic advantage.

• File Activity

This feature enables administrators to view, analyze, and export user-wise and group-wise logs with customizable durations and filters for files accessed by users. It provides complete details, File name, Type, including time stamps, access duration, file source, path, process name, and file size. This comprehensive monitoring allows administrators to track file activity, preventing data leakage, unauthorized access, and ensuring productivity is maintained.

• Remote Control

With this feature of the VIBRANIUM Admin Console, administrators can instantly view or control an endpoint user's live desktop at any time, without requiring prior permission or notification. This facilitates efficient troubleshooting, centralized monitoring, and improved productivity for endpoint clients. The key advantage of this high-speed, lightweight, inbuilt, and integrated Remote Desktop feature is enhanced security, which is often compromised when using third-party remote desktop tools.

• Screenshot

The Screenshot feature in the VIBRANIUM Admin Console allows administrators to capture and view screenshots of endpoint users at specified intervals, providing a visual record of user activity. Administrators can configure the frequency of screenshots based on their monitoring needs, ensuring continuous oversight without unnecessary disruptions. This integrated feature enables real-time monitoring, helping to identify potential security risks, ensure compliance, and optimize productivity. With the ability to track user activity through screenshots, administrators have a powerful tool to maintain control over endpoint usage and prevent unauthorized actions.



SYSTEM AUDIT (SIEM) & Asset Management

• Safeguard Infrastructure

- Endpoint Monitoring: Track and evaluate all endpoint activities.
- Vulnerability Detection: Identify misconfigurations and outdated systems.
- Automated Remediation: Respond instantly to threats

• Regulatory Compliance

- Centralized Logging: Collect and store endpoint and system activity logs.
- Audit Trails: Maintain secure records for easy compliance reporting.
- Policy Enforcement: Flag non-compliant systems and unauthorized activities.

• Real-Time System Oversight

- Precise Tracking: Monitor all system elements for current status and anomalies.
- Customizable Dashboards: Tailor interfaces for actionable insights with minimal resource usage.

• Logs Review and Export

- Scan Logs
- Quarantine logs
- Realtime Logs

• Employee tracking

- Employee Tracking Capabilities
- Measure the total hours dedicated to various programs and websites.
- Assess total working hours for employees, including lateness, overtime, and breaks.
- Generate reports on employee productivity.
- Display the amount of time allocated to business applications.



DEVICE CONTROL

• USB DLP

USB DLP is part of a broader Data Leakage Prevention solution that focuses on preventing sensitive data from being copied, transferred, or leaked through USB devices such as flash drives, external hard drives, or any other peripheral storage media.

• Data Monitoring

- Track data transfers to and from USB devices.
- Generate logs for all USB activities.

• Policy Enforcement

- Implement granular access policies based on user roles, devices, or data sensitivity.
- For example, allow IT staff USB access while blocking it for other departments.

• Malware Protection

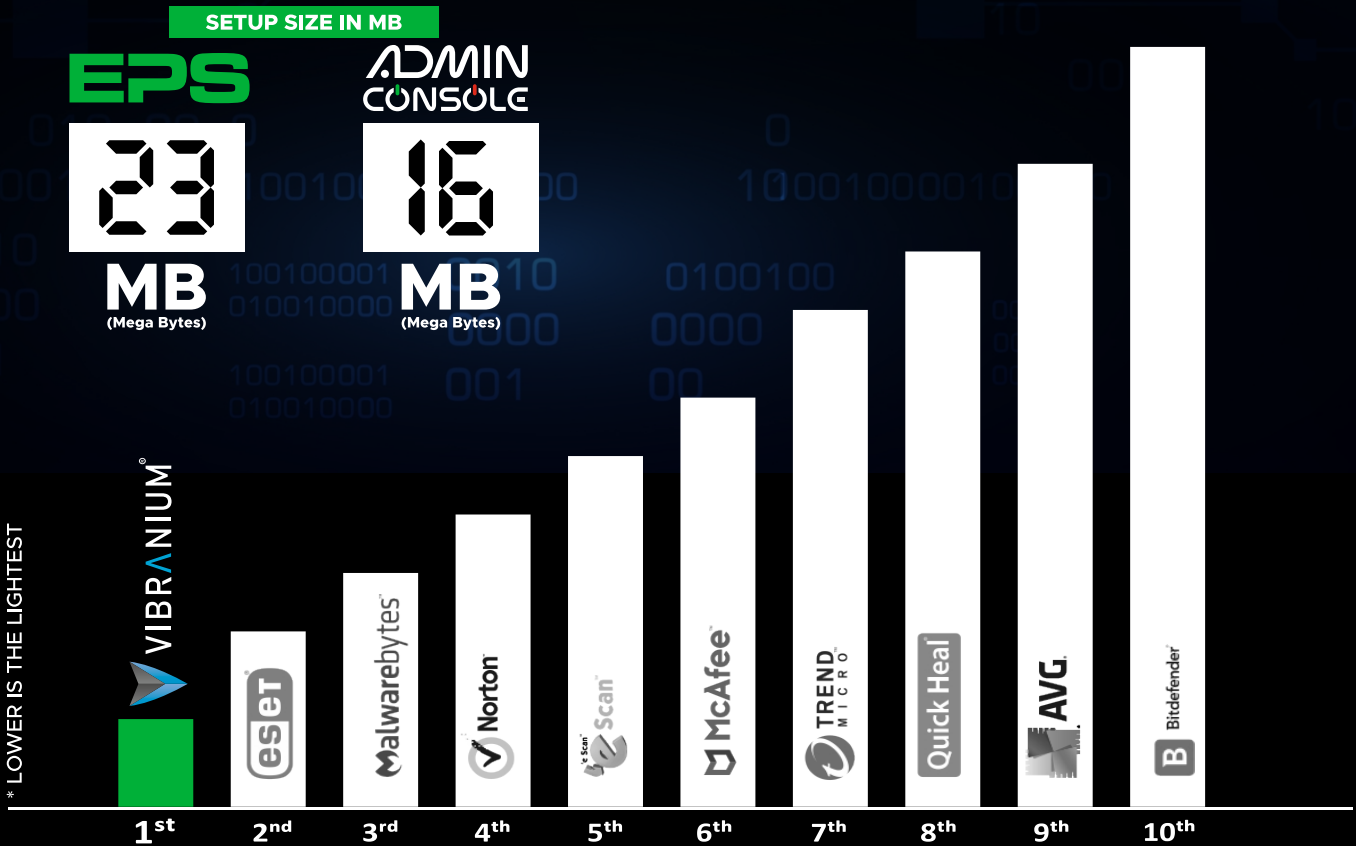
- Detect and prevent the use of malicious USB devices that could carry malware or ransomware.

• Audit Trails & Reporting

- Maintain detailed logs of file transfers, user activities, and device usage.
- Generate compliance reports for auditing purposes.



LIGHTEST



Performance test conducted by Passmark Software – Australia

Experience Feather-Light Performance with Vibranium

At Vibranium, every line of code is meticulously crafted to make our product lighter and smoother. “Lightest” isn’t just a feature - it’s our design philosophy. By minimizing resource consumption, Vibranium ensures your systems run efficiently without compromising performance. Just as a feather glides effortlessly through the air, our streamlined architecture delivers seamless operations and unparalleled smoothness.



WEB FILTERING



BROWSER CONTROL

Cybercriminals exploit websites to spread malware, execute phishing schemes, and compromise sensitive information. Implementing web filtering can effectively block access to dangerous domains, thereby minimizing the likelihood of cyber threats.

Web filtering serves a dual purpose: it shields users from detrimental content and mitigates the risk of online dangers like phishing and malware. By regulating website access, it fosters a safer and more secure browsing environment, customized to meet the unique requirements within corporate environments.

WebContent Filtering moderation

Utilize AI and machine learning to eliminate unsuitable content, including pornography, violence, hate speech, racism, weapons, alcohol, drugs, gambling, and more, from our extensive database of million websites spanning categories.

Instant filtering deployment

Zero cost implementation and free tech support make the installation as easy as it can be. It takes a couple of minutes to deploy & start filtering your internet. You need no IT background or special training needed to manage it.

Boosting Productivity

Distractions from social media, gaming, and video streaming significantly hinder productivity levels. Implementing web filtering enables organizations to restrict access to these non-work-related sites, thereby reinforcing Internet Acceptable Use Policies.

Safeguarding Internet Access

Employees may unintentionally put the organization at risk by visiting phishing sites or insecure websites. Implementing web filtering adds an extra layer of security, helping to block these interactions and safeguard the network.

Real-time Surveillance

To effectively combat online threats, ongoing surveillance is essential. Web filtering solutions offer insights into users' internet activities, allowing organizations to detect potential hazards and proactively modify their policies.

FEATURES

Feature List	BUSINESS EDITION	CORPORATE EDITION	ENTERPRISE EDITION
Antivirus & Antimalware	✓	✓	✓
Bluedome.Ai Advanced Anti ransomware	✓	✓	✓
Phishing Protection	✓	✓	✓
Realtime Protection	✓	✓	✓
Password Management	✓	✓	✓
DLP (Usb blocking)	✓	✓	✓
SIEM (System Audit Report)	✓	✓	✓
Reports Notification	✓	✓	✓
Policy Management	✓	✓	✓
File Activity Management	✓	✓	✓
Application Control	✓	✓	✓
Open Ports Monitoring	✓	✓	✓
Remote Control	✓	✓	✓
Threat Map	✓	✓	✓
Sandbox With EDR & XDR	✓	✓	✓
Network Custom Whitelist	✓	✓	✓
Encrypted Data backup (Data KNOX)	✓	✓	✓
Asset Management	✓	✓	✓
System Tuneup	✓	✓	✓
Kernal protection	✓	✓	✓
Firewall Protection	✓	✓	✓
Web Protection	✓	✓	✓
Realtime Log Viewer	✓	✓	✓
End Point Screenshots	✗	✓	✓
Web Browser History	✗	✓	✓
Employee Tracking	✗	✗	✓
Application Monitoring	✗	✗	✓
Web Filtering(website blocking)	✗	✗	✓
Time Tracking	✗	✗	✓
Application Events	✗	✗	✓
Url blocking	✗	✗	✓
Application Blocking	✗	✗	✓



#ransomfreeindia



EPS ADMIN CONSOLE
END POINT SECURITY

For more info. : 90990 04067  eps@vibranium.co.in

Developed and Marketed by :

VIBRANIUM ALLTECH PRIVATE LIMITED
AHMEDABAD - 380052. GUJARAT. INDIA.

 Toll Free : 1800 270 2599
 +91 98250 49745 (Chat only)

 www.vibranium.co.in
 support@vibranium.co.in


MADE IN INDIA

