



Product Knowledge

Easily Manage, Secure, and Optimize Your Business Computers!

Support for



Windows



Ubuntu



vostra.co.id



[PT Vostra Internasional](https://www.linkedin.com/company/pt-vostra-internasional)



[vostra_id](https://www.instagram.com/vostra_id)

Problem #1

Security Breach and Data Leakage Occur Due to Unmanaged Employee Devices

01

Threat #1 Malware and Phishing Attacks

Devices must be monitored to prevent access to harmful sites and malware.

02

Threat #2 Policy Violation

Devices must restrict access to certain applications and websites.

03

Threat #3 Outdated Software and OS

Devices must always be updated to prevent security exploits and cyber attacks.

Problem #2

Employee Management for boost Productivity

01

Challenge #1
Maintain employee productivity.

02

Challenge #2
Ensure employee use applications that are allowed only for work.

03

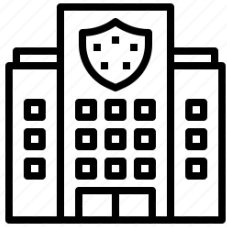
Challenge #3
Slow, inconsistent, or manual software deployment across multiple devices in a network.

What is Vanguard Desktop Management?

Vanguard Desktop Management (Vanguard DM) is a powerful, all-in-one solution designed to help businesses and organizations take full control of their Windows and Linux devices. From enforcing policies and distributing apps and patches to providing remote support and detailed hardware/software inventory, Vanguard DM simplifies desktop management. It boosts security, ensures compliance, and drives productivity — all from a centralized platform.

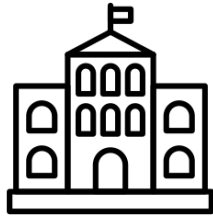


Who Should Use Vanguard DM?



Companies and Corporates

Empower IT teams to seamlessly monitor, control, and secure all office devices across departments.



Educational Institutions (Schools & Universities)

Simplify the management of student devices and computer labs with centralized control and automation.



Government Agencies & SOEs (State-Owned Enterprises)

Maintain strict IT security standards and meet regulatory compliance with full oversight of endpoints.



Startups & MSMEs (Micro, Small, and Medium Enterprises)

An affordable and scalable solution for small businesses seeking simple, effective desktop management.

Why Vanguard DM?

The leading solution for managing Windows & Linux devices in businesses and organizations.



Centralized Management

Manage all Windows and Linux devices from a single dashboard.



Security and Policy Control

Restrict access, control software, and prevent unauthorized usage.



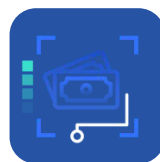
Remote Management

Execute commands, install applications, and monitor devices from anywhere.



Monitoring and Insight

Track software and device health in a single platform.

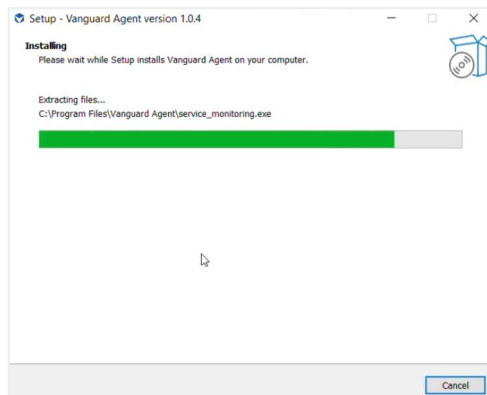


Affordable

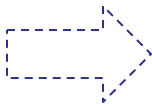
Effective and efficient solutions at affordable costs.

Easy Registration

Deploy Vanguard Agent silently in just a few clicks — no user interaction required. Once installed, the device is instantly registered and ready to be managed.



Install Vanguard Agent



Device is now managed

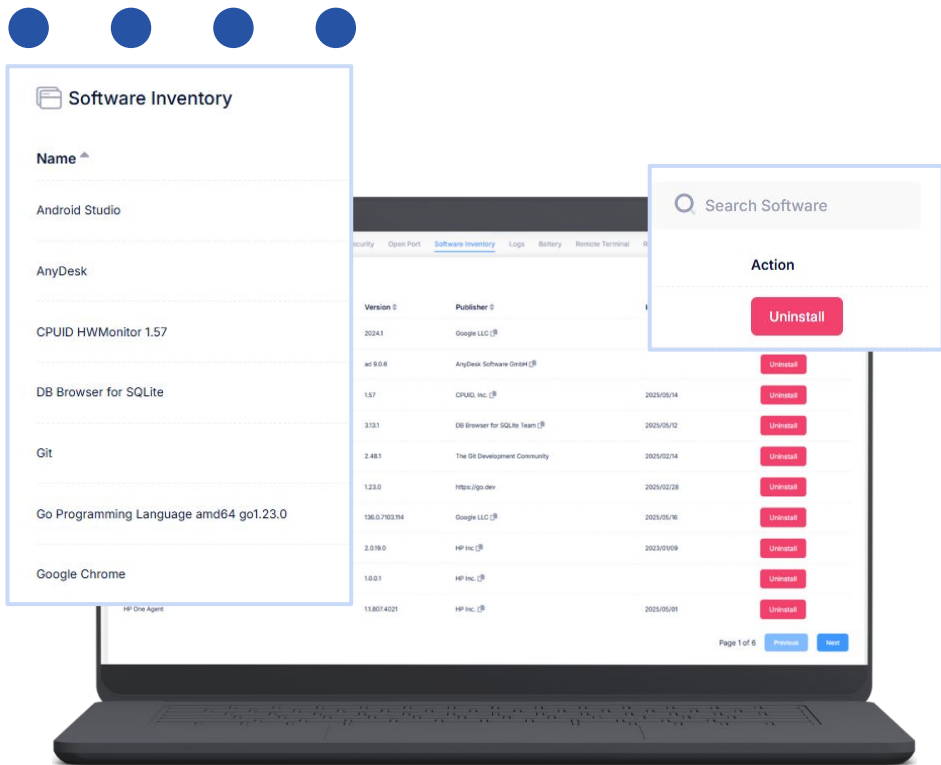
Supported Devices



Windows 10 & Windows 11
(Pro, Enterprise, Education editions)



Linux Ubuntu
(22 & 24 version)



App Management

Centralize and streamline application deployment across your organization.

- **Vanguard App Store:** Install or upgrade applications remotely via the centralized App Store.
- **Manage App Store Content:** Configure and customize available applications within the Vanguard App Store.
- **Remote Uninstallation:** Remove unwanted applications from devices without user intervention.

Faster Download with P2P Technology

Optimize bandwidth usage with peer-to-peer file sharing for application distribution.

- **Accelerate software distribution** across your network.
- **Peer-to-peer file sharing** between trusted devices.
- **Reduce bandwidth usage** on central servers.



Features Overview

Distribution App Report

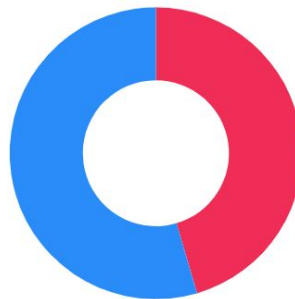
Provide a clear snapshot of application deployment across all managed devices, showing:

- installation status
- app version
- user group
- last seen time

It enable administrators to:

- **Quickly identify** missing or outdated apps
- **Track status** of application updates
- **Ensure seamless and consistency** of application deployment

Microsoft Office Word



● Not Installed ● Installed ● Downloading

Not Installed: 5
Installed: 6
Downloading: 0

Distribution App

Hostname

WIN-18ICI00QPB

KCS3INWJ

WIN-1DDC22O91MQ

Group	Status	Version	Last Connected
inactive2	Not Installed	1.13.194.001	2025-04-11T05:46:19.3
inactive2	Installed	1.13.194.001	2025-06-04T02:46:28
inactive2	Not Installed	1.13.194.001	2025-05-05T10:33:08
nita windows	Not Installed	1.13.194.001	2025-06-03T08:33:41
Lunika-PC	Not Installed	1.13.194.001	2025-05-15T09:21:36
DESKTOP-GOUBOTH	Not Installed	1.13.194.001	2025-06-04T03:18:46
Selfi	Installed	1.13.194.001	2025-06-04T03:23:58
SelfiLenovo	Installed	1.13.194.001	2025-06-04T03:22:06

Page 1 of 1

Prev

Features Overview

Prevent unauthorized apps

The screenshot shows the 'Create Blocklist Rule' dialog in Windows Software Control. At the top, there are buttons for '+ Add Allowlist' and '+ Add Blocklist'. Below, the 'Default Policy' is set to 'Allow'. A link 'Create Blocklist Rule' is present. The 'Rule Name' field contains 'Blocklist App', and the 'Description' field is empty with the placeholder 'Enter description (optional)'. Under 'Select File Type', four categories are listed: 'Executable Files' (Applications (.exe) and command files (.com)), 'Script Files' (Script-based files like .ps1, .vbs, .bat), 'Installer Files' (Installation files like .msi, .msp, .appx), and 'Packaged Apps' (Microsoft Store apps (.appx, .msix)). At the bottom are 'Cancel' and 'Next' buttons.

Allowlist and blocklist

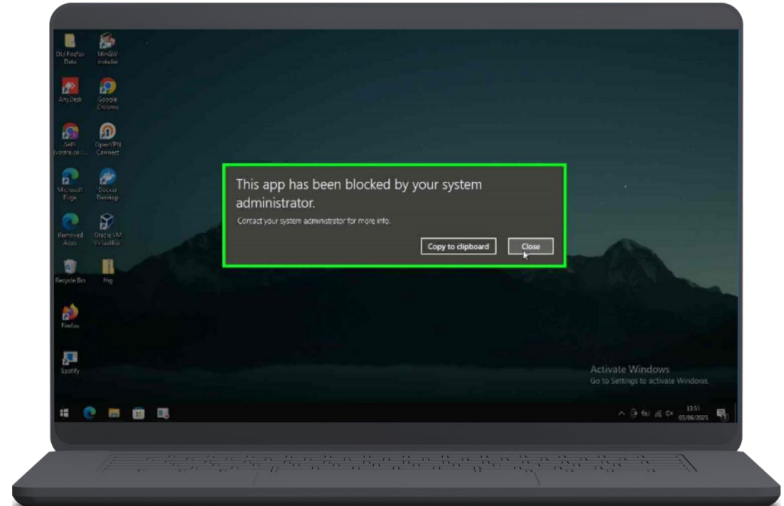
The screenshot shows the 'How do you want to identify the exe?' dialog in Windows Software Control. It has buttons for '+ Add Allowlist' and '+ Add Blocklist'. The 'Default Policy' is 'Allow'. Three options are shown: 'Publisher' (Control software by digital signature), 'Path' (Control software by file location), and 'File Hash' (Control specific file versions). At the bottom are 'Cancel' and 'Next' buttons.

Features Overview

Application Control

Restrict or permit specific applications.

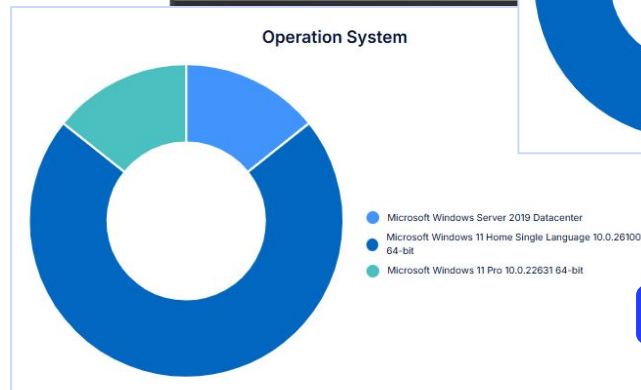
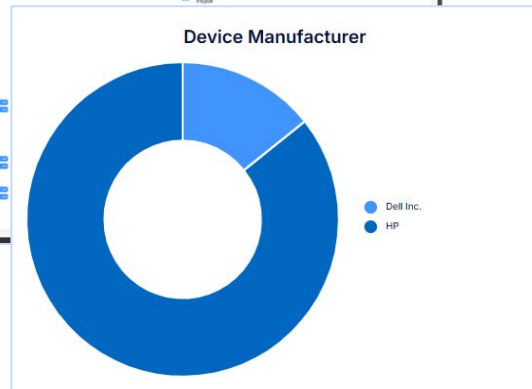
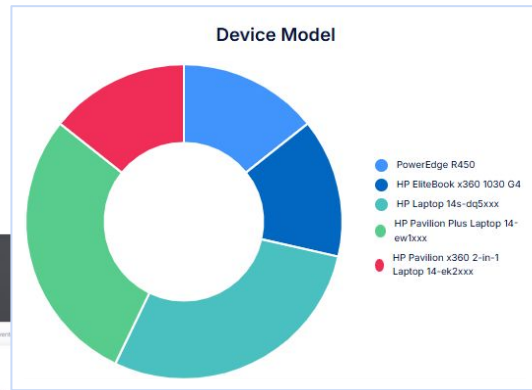
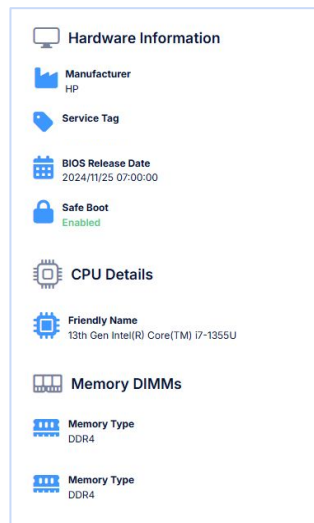
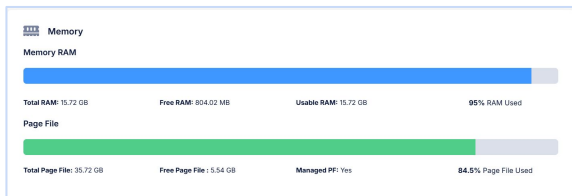
- **Prevent unauthorized** apps, installations, scripts, and portable programs from running.
- **Allowlist and blocklist** specific apps by path, signature publisher, or hash.



Device Information & Monitoring

Gain complete visibility into your device ecosystem with detailed inventories.

- **Hardware Inventory:** Query device specifications including brand, model, manufacturer, OS, and CPU.
- **Software Inventory:** Monitor all installed applications across your device fleet.
- **System Resources:** View memory usage, disk information, and temperature metrics.
- **Network Configuration:** Access network settings, firewall status, and open ports.
- **Security Status:** Monitor Windows Defender and firewall configurations.



Features Overview

Reporting & Analytics

Make data-driven decisions with comprehensive reporting tools.

- **Software Distribution Reports:** Track application deployment status across all devices.
- **Windows Update Status:** Ensure systems remain current with the latest patches.
- **Antivirus Status Monitoring:** Maintain security compliance across all endpoints.
- **Asset Management:** Comprehensive tracking of all IT assets in your organization.

The screenshot displays a web-based interface for managing IT assets. On the left, a 'Device List' sidebar shows a scrollable list of devices, including 'linux1', 'new-VirtualBox', 'DESKTOP-GOUBOTH', 'lunikavostra', and 'kisaserver'. The main area features a table with columns for Status, Group, Manufacturer, Model, CPU, and Last Connected. Below this, a 'Security' section provides a detailed report on 'Antivirus Product' and 'Windows Defender' status for a selected device.

Status	Group	Manufacturer	Model	CPU	Last Connected
DELETING	Vanguard	Oracle Corporation	VirtualBox	AMD Athlon 300U with Radeon Vega Mobile Gfx	2024/12/24 11:42:34
	Vanguard	Oracle Corporation	VirtualBox	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz	2024/12/19 21:15:00
DELETING	Vanguard	VMware, Inc.	VMware201	Apple silicon	2024/12/23 16:28:36
	Vanguard	Oracle Corporation	VirtualBox	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz	2024/12/23 10:27:58
	Vanguard	VMware, Inc.	VMware201	N/A	2024/12/23 15:35:28
	Vanguard	VMware, Inc.	VMware201	Apple silicon	2024/12/24 16:07:40
	Vanguard	Oracle Corporation	VirtualBox	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz	2024/12/24 11:00:37
	Vanguard	Innotek GmbH	VirtualBox	AMD Athlon 300U with Radeon Vega Mobile Gfx	2025/01/02 09:31:12
	Vanguard	Innotek GmbH	VirtualBox	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz	2024/12/24 14:09:00

Display Name	Antivirus State	Signature State	Owner
Windows Defender	On	Up To Date	Windows
McAfee	Off	Up To Date	Non-MS

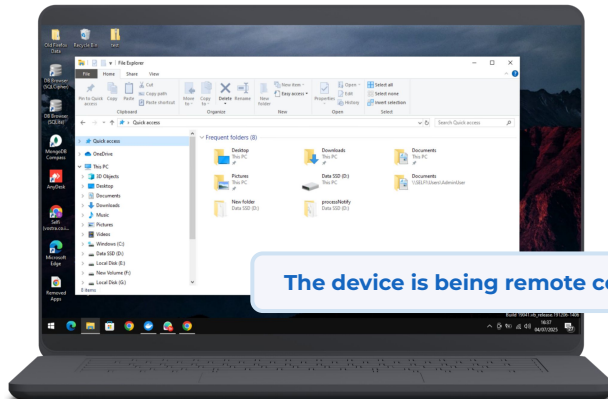
Windows Defender	
Last Quick Scan	2025/05/19 08:49:39
Antimalware Running Mode	Normal
Service Enabled	Enabled
Antispyware Enabled	Enabled
Antivirus Enabled	Enabled
Antivirus Signature Version	1.429.83.0
Real-Time Protection	Enabled

Features Overview

Remote Support Capabilities

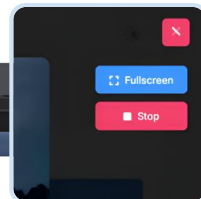
Resolve IT issues quickly without physical access to devices.

- **Remote Control:** View and control devices screen remotely.
- **Remote Terminal:** Execute commands and scripts from anywhere.
- **Remote System Tools:** Access Task Manager and File Explorer remotely.
- **Device Actions:** Perform shutdown, restart, send notifications, and manage synchronization.



The device is being remote controlled

Remote Control



Device Details

Data	
Last Connected:	2025/05/20 17:48:04
Model	
OS	HP Laptop 14-ef01v
OS Version	Microsoft Windows 11 Home Single Language
OS Architecture	10.0.26100
CPU	64-bit
CPU Cores	13th Gen Intel(R) Core(TM) i7-1385U
Total Thread CPU	10
Memory(RAM)	15.72 GB
IP Address	
Last Boot Up Time	2025/05/20 09:46:28
Group	Vanguard
Enrollment Date	2025/05/20 17:45:54

Action

- Synchronize
- Shutdown
- Restart
- Send Notification
- Remote Control
- Unmanage

Remote Task Manager

Process Startup App Services

Name

MsMpEng.exe (1)

NisSrv.exe (1)

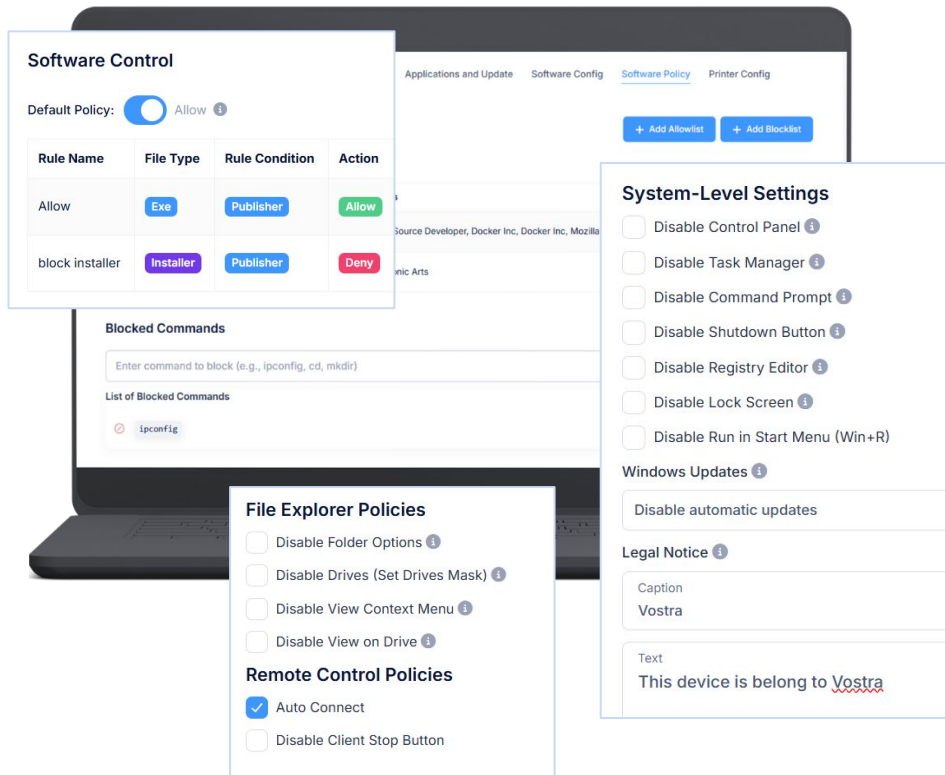
PID CPU Memory

9448 0.0% 120.0 MB

OneDrive.exe	9448	0.0%	120.0 MB
PDAG.AutomationServer.exe (1)	0.0%	36.03 MB	0.0 MB/s
PDAG.BridgeToolAutomation2.exe (1)	0.0%	320.16 MB	0.0 MB/s
PDAG.Console.Host.exe (1)	0.2%	106.69 MB	0.0 MB/s
RuntimeBroker.exe (5)	0.0%	208.7 MB	0.0 MB/s
SearchHost.exe (1)	0.2%	16.5 MB	0.0 MB/s

Features Overview

End task



Features Overview



Policy Management

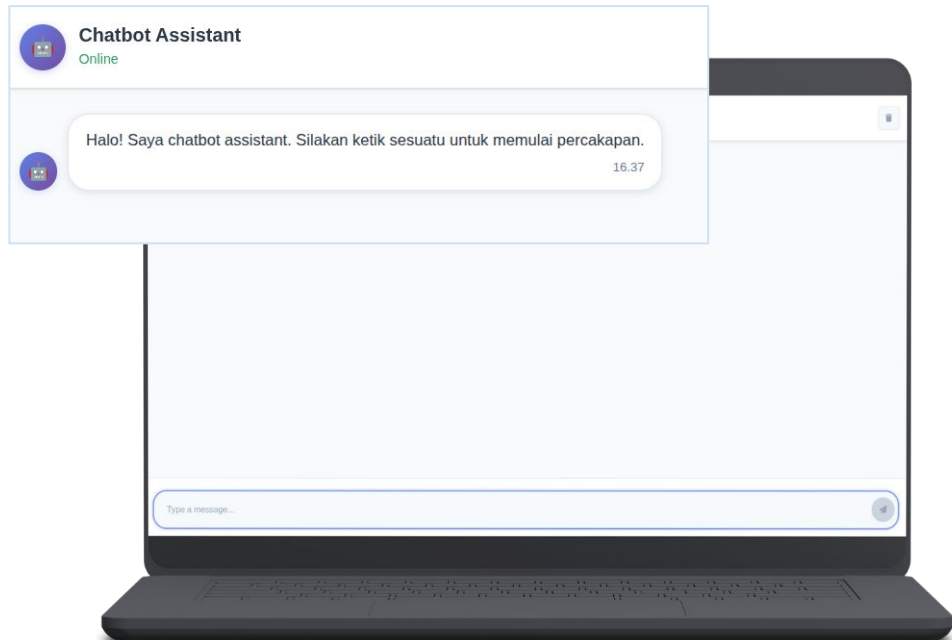
Enforce organizational policies with granular controls.

- **File Explorer Controls:** Manage folder options, drive access, context menus.
- **System Restrictions:** Control access to Control Panel, Task Manager, Registry Editor, Command Prompt, and Run dialog.
- **Security Policies:** Configure secure logon, account lockout policies, and legal notices.
- **Device Management:** Set USB device allowlists/blocklists and control peripheral access.
- **Network Policies:** Configure Wi-Fi settings with allowlists/blocklists.
- **Update Management:** Centrally manage Windows Update settings.
- **etc/many more**

AI Help Desk

Help users quickly find answers related to the Vanguard DM portal without requiring manual assistance.

- **Intelligently identifies** whether query requires documentation (e.g., how-to guides, configuration steps) or real-time system data (e.g., device lists, security status)
- **Delivers fast, accurate, and contextual relevant responses** to support independent problem solving
- **Future-ready:** will support direct actions via API integration—enabling the AI not only to answer questions but also to execute tasks when needed



Features Overview



 vostra.co.id

 [PT Vostra Internasional](#)

 [vostra_id](#)

Contact Us



sales@vostra.co.id

PT Vostra Internasional

Citra Gran Blok CW.07 No.18,
Jati Karya, Jati Sampurna, Kota Bekasi,
Jawa Barat, 17435