BULLWALL

BULLWALL VIRTUAL SERVER PROTECTION
FOR VMWARE

Protect Your Virtual Environment from Ransomware

PROTECT YOUR VMWARE VSPHERE AND ESXI PLATFORMS

Organizations face an increasing threat from ransomware attacks specifically targeting VMware vSphere and ESXi platforms, rendering their virtual environments inaccessible, taking down entire organizations.

BullWall Virtual Server Protection for VMware (VSP), secures virtual servers by preventing unauthorized access and encryption attempts from external sources on ESXi hosts on Red Hat Linux systems.

- Protects against access and encryption from the outside
- Easy to use MFA using Microsoft or Google authenticator
- Monitor running processes
- Detects critical file encryption & corruption of system files
- Automates response 24/7

BULLWALL VSP FOR VMWARE IS INSTALLED DIRECTLY ON ESXI HOSTS AND CONTINUOUSLY ENFORCES:

1. **Multi-Factor Authentication (MFA)** for SSH logins, allowing only authorized users access
2. **Monitoring of running processes** for malicious activity
3. **Monitoring of files, and storage—** including datastores, virtual disks, NFS storage, and internal storage

VSP EFFECTIVELY DETECTS AND MITIGATES RANSOMWARE THREATS IN REAL TIME

BULLWALL VIRTUAL SERVER PROTECTION FOR VMWARE WILL:

PROTECT AGAINST ACCESS AND ENCRYPTION FROM THE OUTSIDE.

MFA protection for ESXi hosts connecting via SSH

Prevents exploitation of admin privileges on critical infrastructure

Additional Critical Security

Essential security features of MFA and OLTP for SSH access on VMware for Red Hat and Linux platforms

Monitor Files on Datastores & Virtual Disks

Detects and stops critical file encryption and corruption of VMware system files and images

ENTRAP INTRUDERS ATTEMPTING TO REMOTELY GAIN ACCESS TO SERVERS.

Intruder Entrapment

Exposes and traps invisible intruders on the network while alerting IT teams

Discover Malicious Running Processes

Detects and stops malicious running processes suspected of the encryption and corruption of VMware system files and images

Prevent Data Exfiltration

Blocks lateral movement and disrupts command-and-control activity on critical infrastructure

DETECT AND PREVENT MALWARE DEPLOYMENT ON SERVERS.

Advanced Monitoring and Threat Prevention

Blocks unauthorized server access and prevents malware deployment

Reduce Recovery Efforts

Automates response and recovery, minimizing damage and enhancing resilience

Enhance Audit Reporting

Simplifies compliance with automation and clear, traceable records

LEVERAGE 24/7 REMEDIATION OF EARLY INDICATORS OF COMPROMISE.

Protect 24/7 365 Days/Year

Ensures continuous, automated ransomware prevention and automated response

Contain Breaches Immediately

Instantly isolates threats, preventing further damage

Integrate with Security Operations Seamlessly

Facilitates effective incident management with comprehensive platform integration

MAINTAIN COMPLIANCE WITH CYBER INSURANCE POLICIES.

Reduce Cyber Insurance Costs

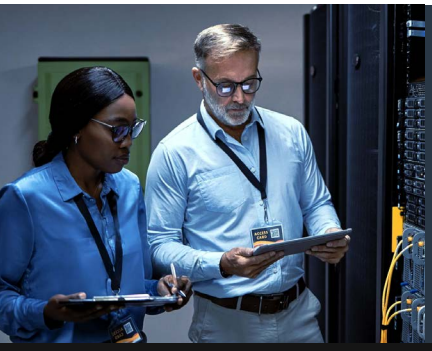
Lower premiums by demonstrating reduced ransomware impact

Ensure Comprehensive Insurance Compliance

Aligns with insurance requirements for server access to support claim eligibility

Maintain Immutable Records of Server Access

Keeps detailed access logs for compliance and analysis



ON AVERAGE, THE RANSOM FOR AN ATTACK DELIVERED VIA VMWARE ESXI SERVERS IN 2024 WAS $5 MILLION...

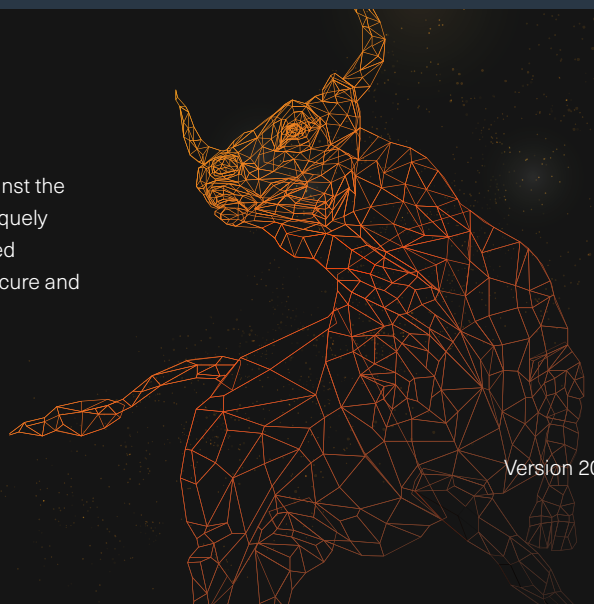
ONLY BULLWALL VIRTUAL SERVER PROTECTION CAN STOP IT

ABOUT BULLWALL

BullWall is the pioneer in ransomware resilience, providing robust defenses against the relentless threat of ransomware. Our focus on the latest ransomware tactics uniquely addresses critical gaps left by other security solutions. By delivering server-based protection without an endpoint agent, BullWall keeps critical IT infrastructure secure and operational during the core stages of an attack – before, during and after.

Learn more at www.bullwall.com.

BULLWALL



Version 2025.03