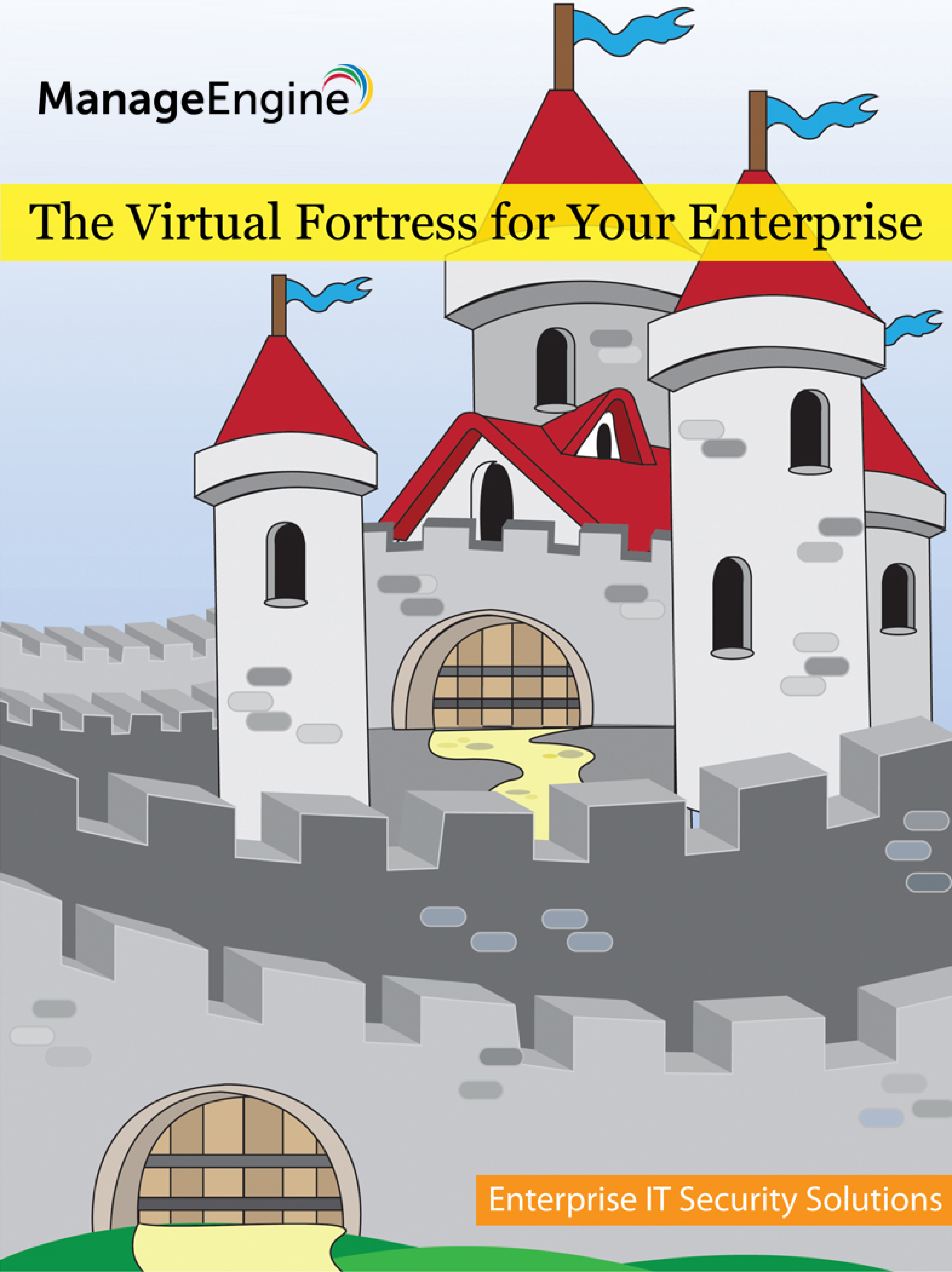
ManageEngine

The Virtual Fortress for Your Enterprise



Enterprise IT Security Solutions

ManageEngine – The Virtual Fortress for Your Enterprise!

Today's enterprises are facing unprecedented security threats. As organizations embrace new technologies, newer threats keep pace. Safeguarding the enterprise from evolving, sophisticated threats is the need of the hour.

When you dig deep into security incidents such as identity thefts, breaches, DoS attacks and others, you will find certain basic security measures carelessly handled. With today's social networks, bad news travels faster, lingers on to affect your business and haunt your brand name forever.

Combating the sophisticated cyber threats mandates a multi-pronged strategy - deploying security devices, enforcing security policies, controlling access to resources, monitoring events, analyzing logs, detecting vulnerabilities, managing patches, tracking changes, ensuring compliance, monitoring traffic and a host of other activities.

ManageEngine has a range of affordable Enterprise Security Management Software Solutions that help you build a secure fortress enabling you stay secure, ensure business continuity and enhance productivity.

A Strong Perimeter

Identify vulnerabilities & secure your boundary

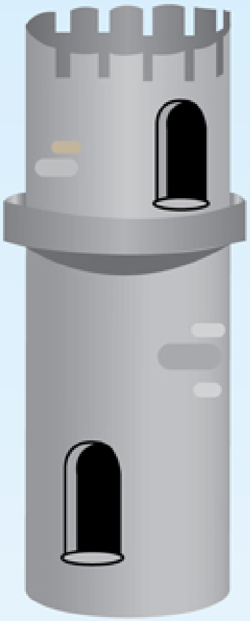
The first step in building a fortress is to secure your boundary, understand your vulnerabilities and initiate action for protection. For a strong perimeter in enterprises, you need to

- scan your network, create inventory of network assets
- identify network vulnerabilities & remediate them swiftly
- detect missing patches, hot-fixes & security updates on Windows and Linux and deploy them quickly
- manage changes to Windows files, folders and registry
- stay informed with audit reports on open ports, hardware and software

Security Managar Plus - Network Security Scanner & Patch Management www.securitymanagerplus.com

The Watch Towers

Monitor, analyze log data and alert on internal, external security threats



Watch Towers in the fortress help in observing the happenings around and protect from potential threats. In enterprises, keeping a watchful eye over the eventlog, application log and trails from perimeter security devices is essential to safeguard the organization from evolving internal and external threats and optimize performance. This mandates

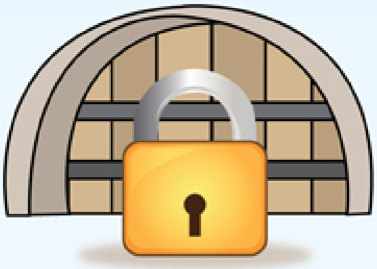
- automatically collecting, analyzing, reporting, alerting and archiving event log from distributed Windows hosts, Syslog from Unix hosts and devices & Application log from servers and databases
- monitoring, analyzing and reporting on logs from firewalls and other perimeter security devices
- troubleshooting network problems and optimizing bandwidth usage & performance
- complete visibility on internal & external security threats
- meeting regulatory audit and compliance requirements

Firewall Analyzer - Firewall Log Analysis www.fwanalyzer.com

Eventlog Analyzer - Syslog & Event Log Management www.eventloganalyzer.com

A Secret Chamber

Protect the keys to your kingdom



After building the fortress, the keys to your kingdom need to be protected. A strong perimeter just protects you from external attacks. But, to guard yourself from malicious insiders, you need a secure, centralized 'secret chamber' for safe upkeep of the keys and thereby control privileged access to a select few. In enterprises, you need to

- securely store, manage and control access to shared sensitive information such as passwords, documents and digital identities
- eliminate password fatigue and security lapses
- improve IT productivity many times by automating frequent password changes required in critical systems
- establish preventive & detective security controls through approval workflows & real-time alerts on password access
- meet security audits and regulatory compliances such as SOX, HIPAA and PCI

Password Manager Pro - Privileged Password Management www.passwordmanagerpro.com

The Citadel

Establish a centralized authority for network device configurations

In the fortress, citadel is the seat of the centralized authority and is the strongest component. In enterprises, network devices are the crucial components. Any unauthorized configuration change could wreak havoc on the network. To secure device configurations, you need to

- automate backup of configurations of switches, routers, firewalls & other devices
- track configuration changes in real-time & generate notifications
- prevent unauthorized configuration changes
- control access to configurations & enforce role-based restrictions for configuration upload
- check configurations for compliance to policies & standards
- get complete record of 'who', 'what' and 'when' of device configuration changes
- automate the entire life-cycle of device configuration tasks

DeviceExpert - Network Change & Configuration Management www.deviceexpert.com

The Operational Command Center

Constitute centralized control for servers & desktops

In the fortress, day-to-day operations are controlled from the command center. Likewise, in enterprises, servers and desktops constitute the nerve centre of routine operations. Securely managing them from a centralized location is a crucial task, which requires

- automating the desktop management routines of enterprises to standardize and secure their Windows network
- protecting desktops from wide range of threats
- quick troubleshooting of day-to-day issues
- generating comprehensive reports to audit IT assets

Desktop Central - Desktop and Server Management www.desktopcentral.com

Arm your Enterprise with ManageEngine Security Solutions;
Make IT Security your Priority!

- Network Security Management
- Network Security Audits
- User Account & Rights Management
- Security Information and Event Management
- Privileged Identity & Access Management
- Regulatory Compliance
- Internal Controls

ManageEngine

4900 Hopyard Rd., Suite 310, Pleasanton, CA 94588, USA
Phone: +1-925-924-9500 Fax: +1-925-924-9600
Email: sales@manageengine.com **Website: www.manageengine.com**