White Paper
eCube_LTCG Dynamic Security Tools

Introduction

In the wake of major security breaches that have occurred to major retailers and online companies, cyber security has become a big priority for IT organizations across the world. Most organizations are challenged to maintain compliance and dependable cybersecurity posture to reduce the risks of breaches and security issues within their enterprise systems and cloud based services. In this paper we will examine the existing security system's focus areas and propose a solution to make it better.

Background

Companies have historically addressed five main areas when establishing a secure network for internal use. The addition of internet access has greatly increased the ability of unauthorized people to gain access and compromise a company's security. The addition of Cloud applications has further increased that potential threat. To combat the threats they face, security analysts focus on the key areas of protection for security:

1. Identification – providing a method to identify valid users is growing more sophisticated these days.
2. Authentication – preventing unauthorized access of secured systems by non-authorized personnel.
3. Integrity – ensuring your software systems, data and infrastructures maintain their integrity and don't get modified, replaced by a Trojan horse or destroyed by intruders.
4. Encryption – most secure systems use encryption for network traffic and file storage protection.
5. Detection – the best security systems can detect intrusions into a secure system and notify the security administrator.
6. Authorization/Permissions – timely management of security permissions is the best way to protect systems, prevent data breaches and protect sensitive data from employees or other authorized personnel.

7. Backup/Recovery – restoration of compromised systems requires mandatory and timely backups of software configurations and data.

Addressing these issues requires companies to adopt strict security guidelines for administrative and end-user company computer usage and protection of data. While these areas are constantly changing in scope and the technology to address each aspect, they remain as the foundation most companies use for their security model. Company policies and procedures are usually developed to address the response and standards that will be applied to each. Typically these procedures require employees to read, conform and acknowledge them on a periodic basis.

The Problem

Most companies have existing security software and policies to ensure protection from attack, but sometimes these policies rely on manual intervention and they don't get timely updates and changes to the trusted employee accounts are not made or new additions to the enterprise don't get sufficient security protection. The lack of awareness of security issues and timely security updates increases your risk of a data breach or being hacked. New threats appear all the time and threaten the network with infection of viruses or bots, so you need a pro-active approach.

Dynamic and automatic cybersecurity management tools are key to attaining risk management goals as it provides policy and compliance context, and mines the enterprise systems for vulnerability information, remediation opportunities, configuration details, and ultimately, a comprehensive view of the enterprise risk.

Working diligently to secure their environments, Information Technology teams and cybersecurity professionals must be equipped with technology that allows them to identify, monitor and manage their true level of security posture and related risks.

White Paper

eCube_LTCG Dynamic Security Tools

The Solution

To ensure that security protections remain intact and new threats are dealt with as they appear, an infrastructure to monitor the security systems in place is necessary. An assessment of your existing security system is required to establish your current security level, identify all of the weaknesses in your secure system and respond with an appropriate infrastructure plan. Once this infrastructure is in place, you will need an automated system to monitor, respond to threats and maintain it.

eCube_LTCG Dynamic Security Tools uses distributed agents and centralized management services to automatically scan, document, report and monitor all the enterprise services, devices, connections and configurations.

The aggregation and centralization of system knowledge data over time, enables these Dynamic Security Tools to access security risks and produce remediation recommendations. These recommendations are cross referenced to the configurable enterprise preferences and requirements for industry security frameworks and related security controls (NIST, ISO, PCI-DSS, OWASP, etc.)

Risk Assessment

Dynamic Security Tools need to assess security risks across the enterprise on a periodic basis and classify the threat level so that responses can me made appropriately. These responses may be daily or hourly and for high risk security exposure, alerts may be necessary.

Identify security issues

A good security tool must be able to identify all security threats and assign the right threat level to each, which corresponds to the level of focus that will be used to address each issue. Responses to security threats will used to address future security risks and produce remediation recommendations.

White Paper

eCube_LTCG Dynamic Security Tools

Remediation

Dynamic Security Tools can use database driven security responses and invoke remediation responses based on the classification of the threat. These recommendations are based on the customer’s system configuration profile for security frameworks for the 7 key areas of protection (Identification, Authentication, Integrity, Encryption, Detection, Authorization/Permissions and Backup/Recovery)

White Paper

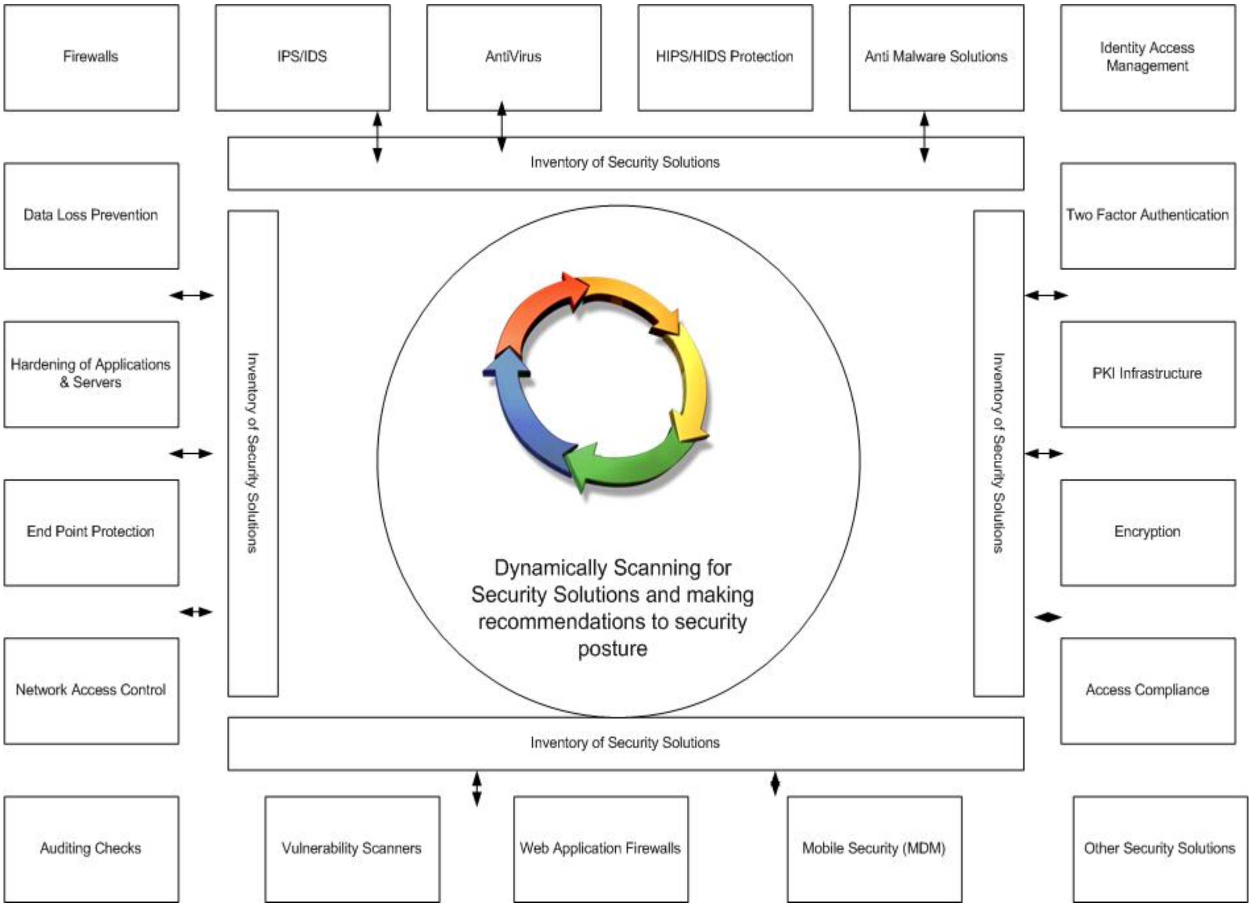
eCube_LTCG Dynamic Security Tools

Solution Overview

A dynamic security system must have at its heart a Hybrid Infrastructure Platform to ensure security is enforced across the hybrid environment. This means that the solution must be highly portable and distributed to be effective.

Design

The design and structure of the eCube_LTCG Dynamic Security Tools are shown in the diagram below:


Firewalls
IPS/IDS
AntiVirus
HIPS/HIDS Protection
Anti Malware Solutions
Identity Access Management
Inventory of Security Solutions
Data Loss Prevention
Two Factor Authentication
Hardening of Applications & Servers
PKI Infrastructure
Inventory of Security Solutions
Inventory of Security Solutions
End Point Protection
Encryption
Dynamically Scanning for Security Solutions and making recommendations to security posture
Network Access Control
Access Compliance
Inventory of Security Solutions
Auditing Checks
Vulnerability Scanners
Web Application Firewalls
Mobile Security (MDM)
Other Security Solutions