TekMonks

LOGINCAT

ZERO TRUST CYBERSECURITY

DATA SHEET

Zero Trust Based Cybersecurity

LoginCat, the world's first comprehensive Cyber Security suite and Artificial Intelligence (AI) driven, is a Zero Trust based platform for application security .

AI Based Security

More than just user ID and password authentication, AI is used to determine access to each specific application, system, or information.

Trust Based CyberSecurity

LoginCats AI engine evaluates a trust score for your identity based on behavior criteria such as your usual login timings, location, time, and even the way you enter the password.

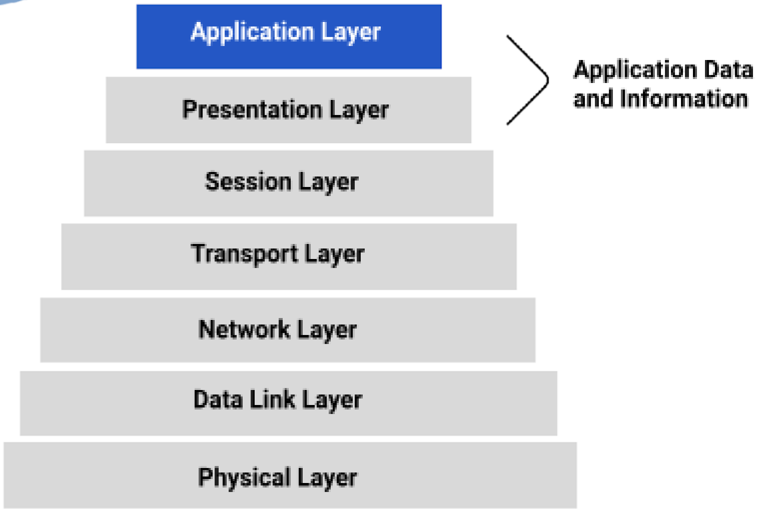
Restrict Access at the Network Layer

Restrict access at the physical network based on a user's trust scores not meeting the minimum requirements of the organization.

LoginCat secures existing and new applications by protecting against cyberattacks without risk from day zero. With no requirement to modify existing applications, LoginCat constantly provides updates to include the latest security and AI algorithms to protect against emerging threats.

- Zero Trust Multi-Factor Authentication (MFA)
- Cyber Trust Score Access
- Software Defined Perimeter (SDP) Protection
- Single Sign On (SSO)
- Password Management
- App Secure
- Security Operations Center (SOC)

LoginCat stops over 4 million cyberattacks per month for just one of our clients.



Application Layer

Presentation Layer

Session Layer

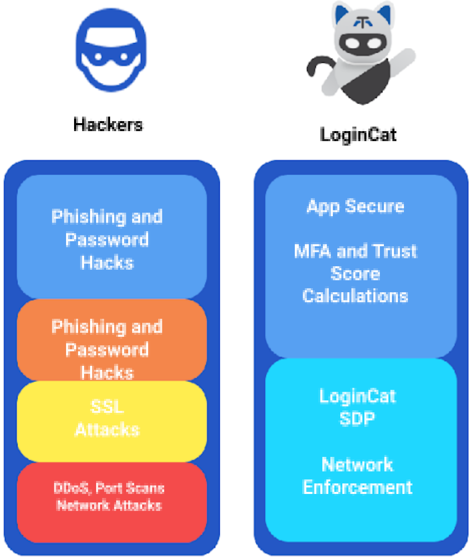
Transport Layer

Network Layer

Data Link Layer

Physical Layer

Application Data and Information



Hackers

Phishing and Password Hacks

Phishing and Password Hacks

SSL Attacks

DDoS, Port Scans Network Attacks

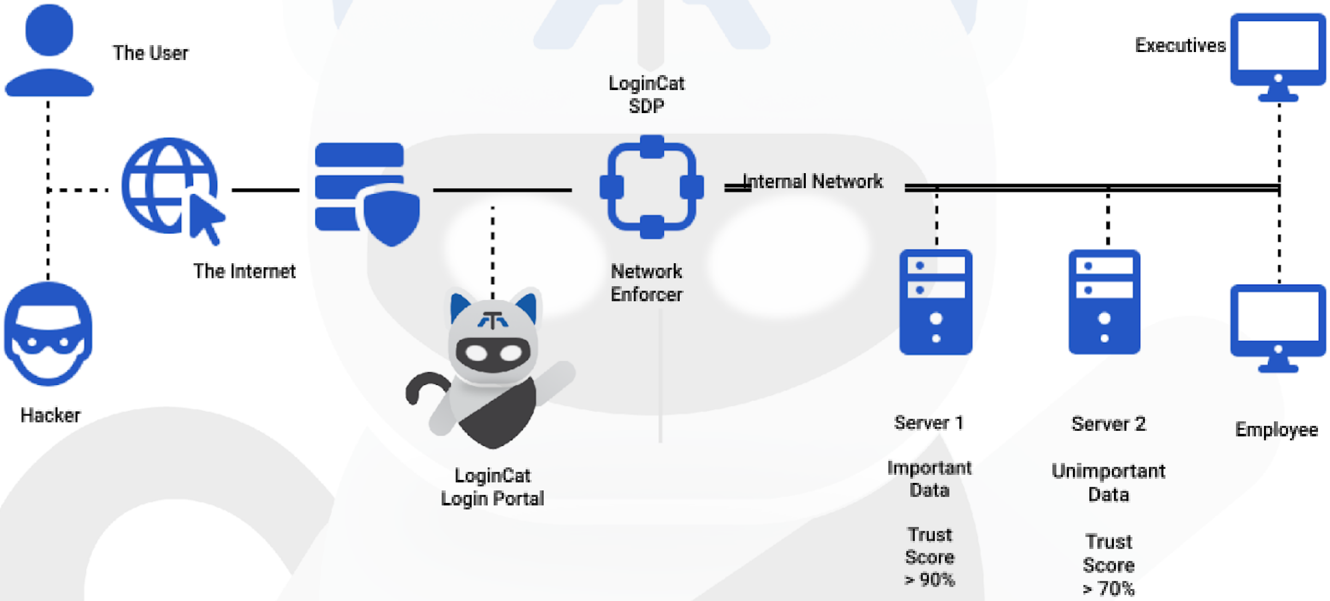
LoginCat

App Secure

MFA and Trust Score Calculations

LoginCat SDP

Network Enforcement



The User

Hacker

The Internet

LoginCat SDP

Network Enforcer

LoginCat Login Portal

Internal Network

Executives

Server 1

Important Data

Trust Score > 90%

Server 2

Unimportant Data

Trust Score > 70%

Employee

Features and Benefits

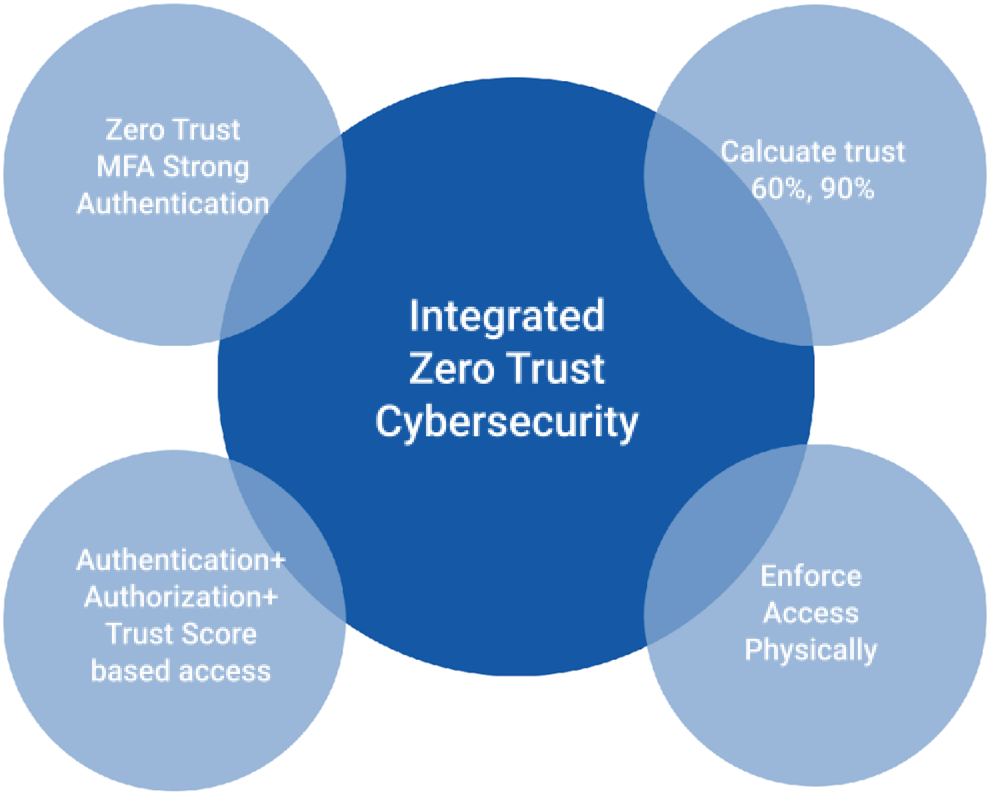
Zero Trust Multi Factor Authentication using AI

LoginCat supports several different factors for authentication including biometrics, one time passwords, passphrases, and questions.

MFA Login Portal LoginCat comes with its own MFA compliant, security hardened portal for login page implementation.

WebAuth, Biometric Password-less authentication support.

Pluggable 2FA Engine Supports OTP, T-OTP, Fingerprint, Face ID, and multiple other second factor authentication options.


Zero Trust MFA Strong Authentication
Calcuate trust 60%, 90%
Integrated Zero Trust Cybersecurity
Authentication+ Authorization+ Trust Score based access
Enforce Access Physically

Scenario: *Someone who is authorized to access highly confidential data is logged in successfully but detected to be in North Korea. Trust score is still very low even if requirements for authentication and authorization are met. Hence, access will still be denied.* ***(Zero Trust Model)***

Features and Benefits

Zero Trust Architecture

LoginCats AI engine evaluates a trust score for a user's identity based on criteria such as behavior, login timing, location, time and the way a password is entered prior to providing access to various servers and applications.

- Zero Trust requires organizations to not depend on traditional authentication. Users can be remote employees, partners, customers, contractors, and cyber-thieves attempting to access systems and sensitive data.
- LoginCat supports a Zero Trust Architecture. Requiring increased security over traditional authentication as users can be remote employees, partners, customers, contractors, cyber-thieves attempting to access systems and sensitive data.
- LoginCat matches a user's trust score to the minimum trust score for a particular application or system. If the trust level is not adequate, LoginCat will not provide access to those systems or applications.

Features and Benefits

A Unified Cyber Security Solution

LoginCat's SDP restricts access at the Network Layer based on the Cyber Trust Score to ensure only trusted access to an organization's network and systems

- Definition of password rules such as length, complexity, and how often passwords need to change.
- Configurable frequency of changing passwords whether it is weekly or 30 to 90 days
- Creating trust groups for users to only display and provide access to users approved for applications.
- Take over the responsibility for changing user passwords and not sharing with end users ensuring users can only securely access applications via the LoginCat user portal.

App Secure

Enables the addition of MFA support for legacy applications that only support single-factor authentication, enabling high-level security implementation.

- Robust verification of users identities coupled with sturdy security policies to keep financial data and online transactions secure.
- Protection of Authentication Factors.

Something	Details
You Know	**Password and Passphrase**
You Have	**SIM Card, Secure OTP, and Physical Matrix**
You Are	**Biometric**

At least two out of three factors must be present

Independence the authentication mechanisms used for MFA should be independent to one another. Such that access to one factor does not grant access to any other factor. Hence, it does not compromise the integrity of one the factors or confidentiality of any other factor.

Out of Band Authentication Out-of-band (OOB) refers to authentication processes where authentication methods are conveyed through different networks or channels.

Security Operations Center (SOC)

All events are logged, and alerts are raised. Events can be consolidated in an organization-wide monitoring solution. LoginCat's Security Operations Center (SOC) monitoring ensures the security of your connection, capable of the following:

- Alerts are raised upon unauthorized access. Administrators are made aware which user's laptop and/or phone is compromised.
- Alerts are also raised on Rogue IP - external hackers are identified and banned.
- All events are logged with the following user information:
  - User login
  - User accessing an application
  - User logout
  - User abusing authority
- All alerts are reliable and actionable not hundreds of alerts an hour like typical SIEMs

System Requirments

Specifications	
Supported OS	Linux, Redhat Enterprise and Ubuntu
Compliance	ISO 27001
System Requirements	4 cores and 12 GB RAM and 250 GB Disk
Product Model	SaaS Software
Installation Methodology	Delivered as Saas or Prebuilt VMs
Integration	Windows, Linux, Network via SNMP
Support	Click for Support Documentation

Produced/Printed in the UK 02/2023

PATENTS: US Patent Pending
IMPORTANT PRIVACY INFORMATION: If you would like to request access to or correction of your details, or if you would prefer you or your organization not to receive further information on Tekmonks products and services please contact us at: privacy@tekmonks.com

Tekmonks Ltd.

Kemp House, 152 City Road
London. EC1V 2NX. UK.