LTS SECURE'S ZERO TRUST MODEL

Accelerate Security Transformation With **ZERO TRUST**

ENTERPRISE READY SECURITY

OVERVIEW

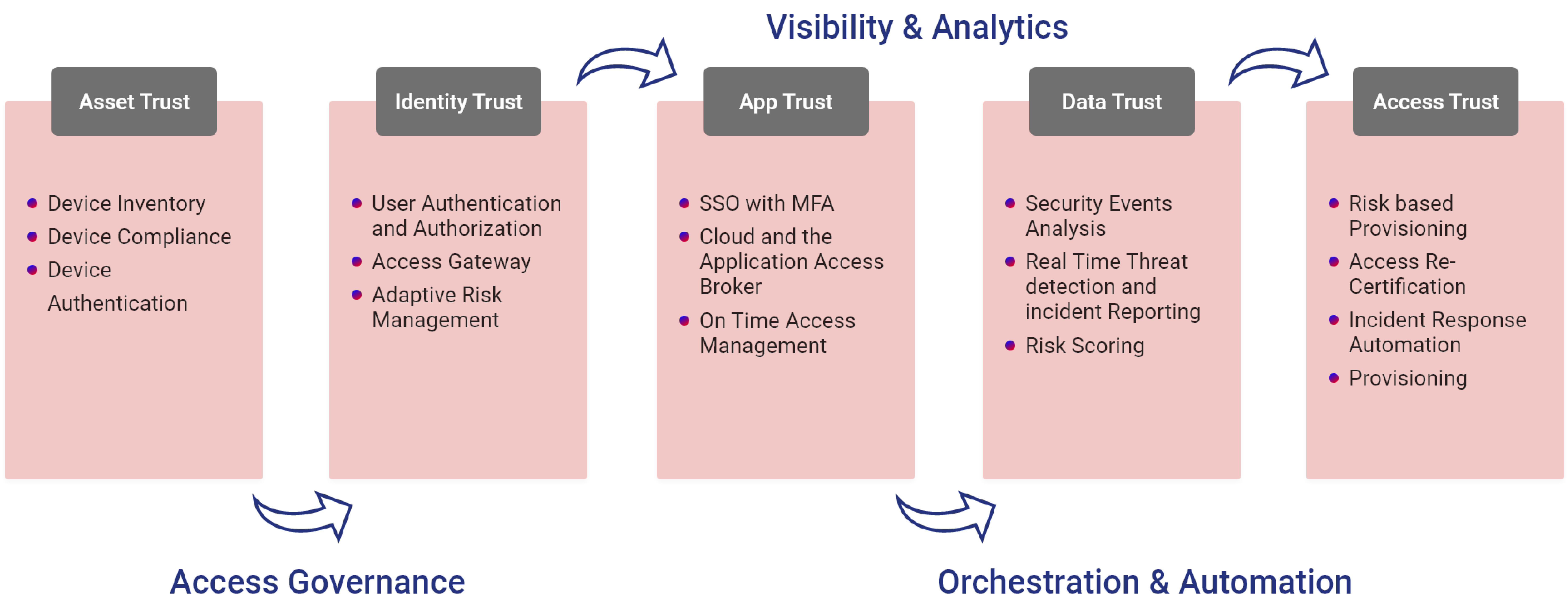
With remote users connecting via unmanaged devices to critical servers, sensitive data and business applications over the internet, organizations are in need of a new security model that is capable enough to adapt to the complexities brought on by the modern enterprise & remote workforce and is able to protect apps, data, users & devices.

LTS Secure's Zero Trust Model ensures that all of our users, regardless of their location, have to be authenticated, authorized, and continuously validated against defined security configuration before they are granted access to applications and data.

Businesses of all sizes are prone to cyber-attacks today; and the sophistication, undefined patterns and unpredictability only adds to the existing vulnerabilities. Experts have not been able to stick to one single technology or strategy to contain the menace of diverse and potent cyber threats.

Starkly different from the conventional enterprise security measures, the Zero Trust approach is context based. With a range of different technologies focussing on strengthening security from within, this approach safeguards your business with 'never trust, always verify' attitude.

The most common challenges faced by organizations that lead to security breaches risking valuable assets and sensitive data need to be prioritized.



Visibility & Analytics

Asset Trust

- Device Inventory
- Device Compliance
- Device Authentication

Identity Trust

- User Authentication and Authorization
- Access Gateway
- Adaptive Risk Management

App Trust

- SSO with MFA
- Cloud and the Application Access Broker
- On Time Access Management

Data Trust

- Security Events Analysis
- Real Time Threat detection and incident Reporting
- Risk Scoring

Access Trust

- Risk based Provisioning
- Access Re-Certification
- Incident Response Automation
- Provisioning

Access Governance

Orchestration & Automation

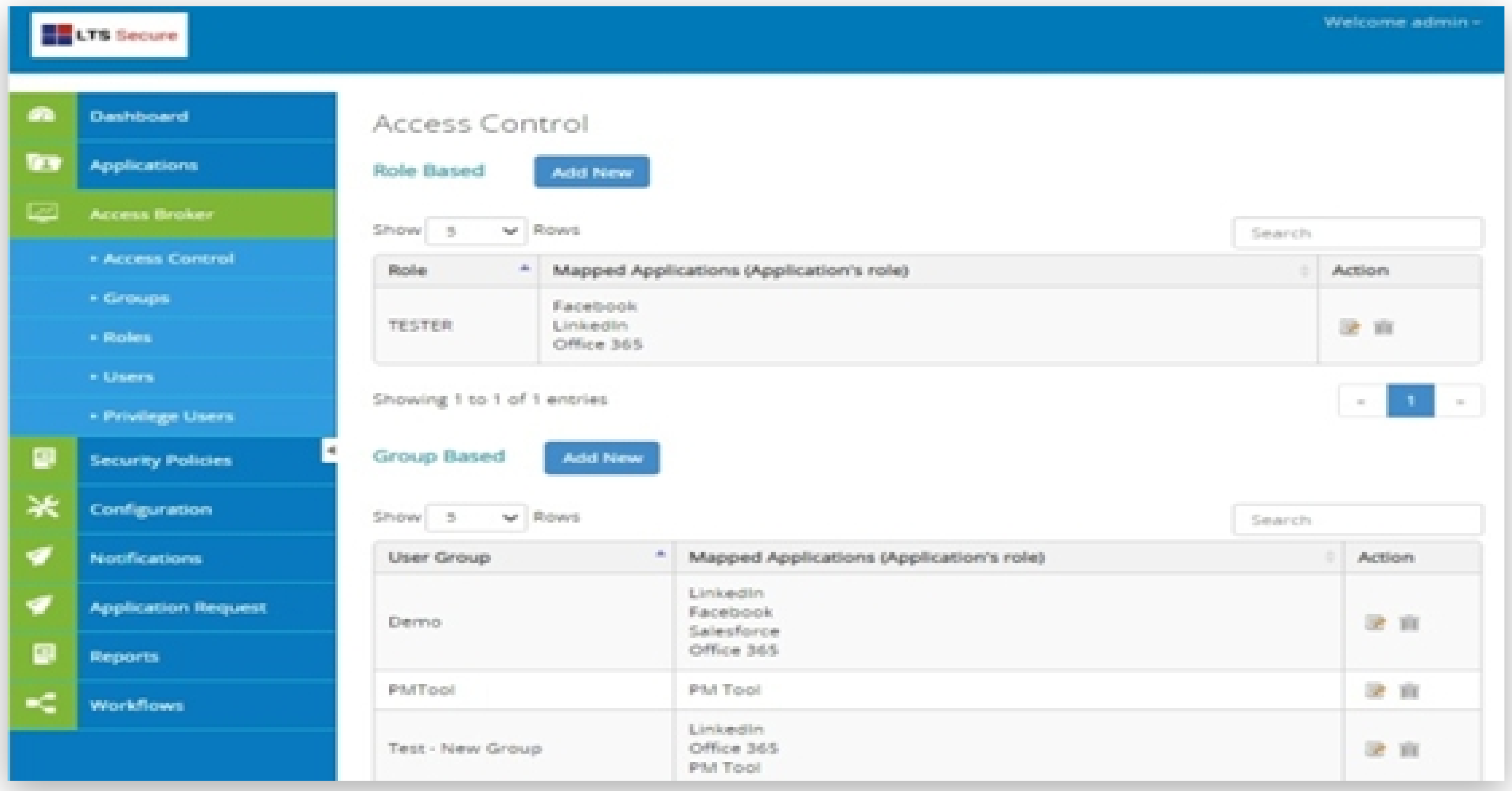
CRITICAL MODULES OF LTS SECURE ZERO TRUST MODEL

LTS Secure Zero Trust Security is a strategic combination. A high performance security structure carefully created by weaving in various independent solutions to safeguard and protect different aspects of enterprise network. Our Zero Trust Security strengthens security measures with a combination of:

IDENTITY MANAGEMENT (IDM) & ACCESS RECERTIFICATION

With Identity management, ensure a safe environment by identifying individuals in a system and controlling their access to resources and valuable assets. The most important aspect of a Zero Trust Security, IDM associates user rights and restrictions with established identity and entails comprehensive and secure management of identity life cycle of users, devices and applications with various features and modules.

With Access Recertification, control, manage and audit the security framework providing centralized visibility and compliance on roles and responsibility within the security architecture.



Access Control

Role Based

Role	Mapped Applications (Application's role)	Action
TESTER	Facebook Linkedin Office 365	

Showing 1 to 1 of 1 entries

Group Based

User Group	Mapped Applications (Application's role)	Action
Demo	Linkedin Facebook Salesforce Office 365	
PMTool	PM Tool	
Test - New Group	Linkedin Office 365 PM Tool	

Modules

- Role-based Provisioning
- REST API
- Flexible Data Model
- Password Management
- Identity Gateway
- Cloud SaaS Connectors
- Synchronization and Reconciliation
- User Activity Management
- Approvals by Email
- Logging, Auditing and Reporting
- Self Service and Profile Management
- User Provisioning and Deprovisioning
- Workflow Engine
- Open ICF Connector Framework

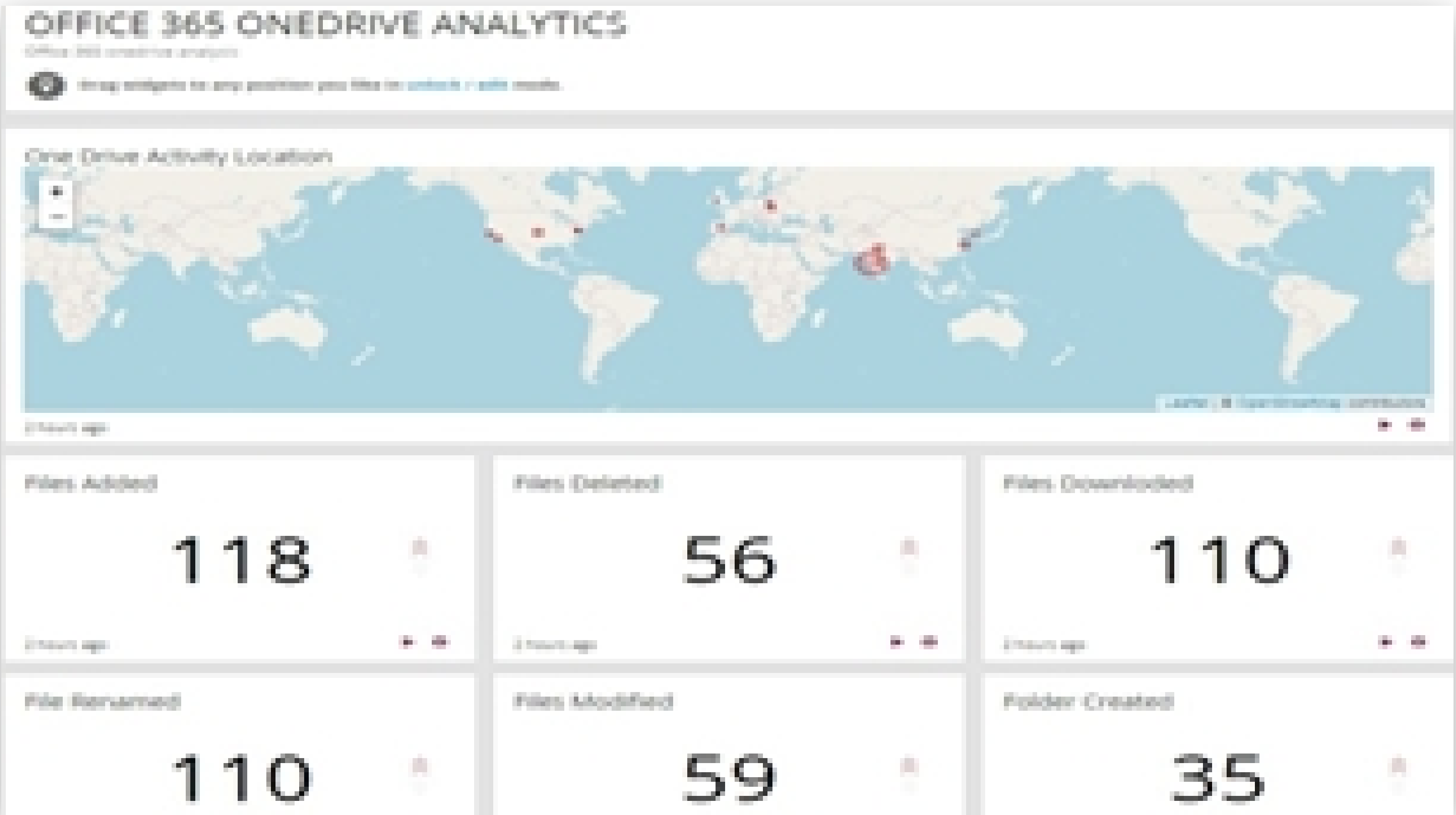
CRITICAL MODULES OF LTS SECURE ZERO TRUST MODEL

CLOUD ACCESS SECURITY BROKER (CASB)

Indispensable for cloud security, Cloud Access Security Broker acts as a unified security control by tracking security threats that might arise by accessing data and applications from the cloud. As a barrier between cloud providers and cloud service providers, CASB consolidates multiple types of security policy enforcement helping achieve Zero Trust Security by extending security policies beyond company infrastructure.

Modules

- Visibility
- Compliance
- Activity Monitoring & Analytics
- Early Threat Detection
- Cloud Threat & Risk Analytics
- Data Loss Prevention
- Prevent Data Exfiltration
- Reporting And Auditing



OFFICE 365 ONEDRIVE ANALYTICS

Office 365 onedrive analytics

Drag widgets to any position you like in unlock / edit mode.

One Drive Activity Location

2 hours ago

Files Added	Files Deleted	Files Downloaded
118	56	110
2 hours ago	2 hours ago	2 hours ago

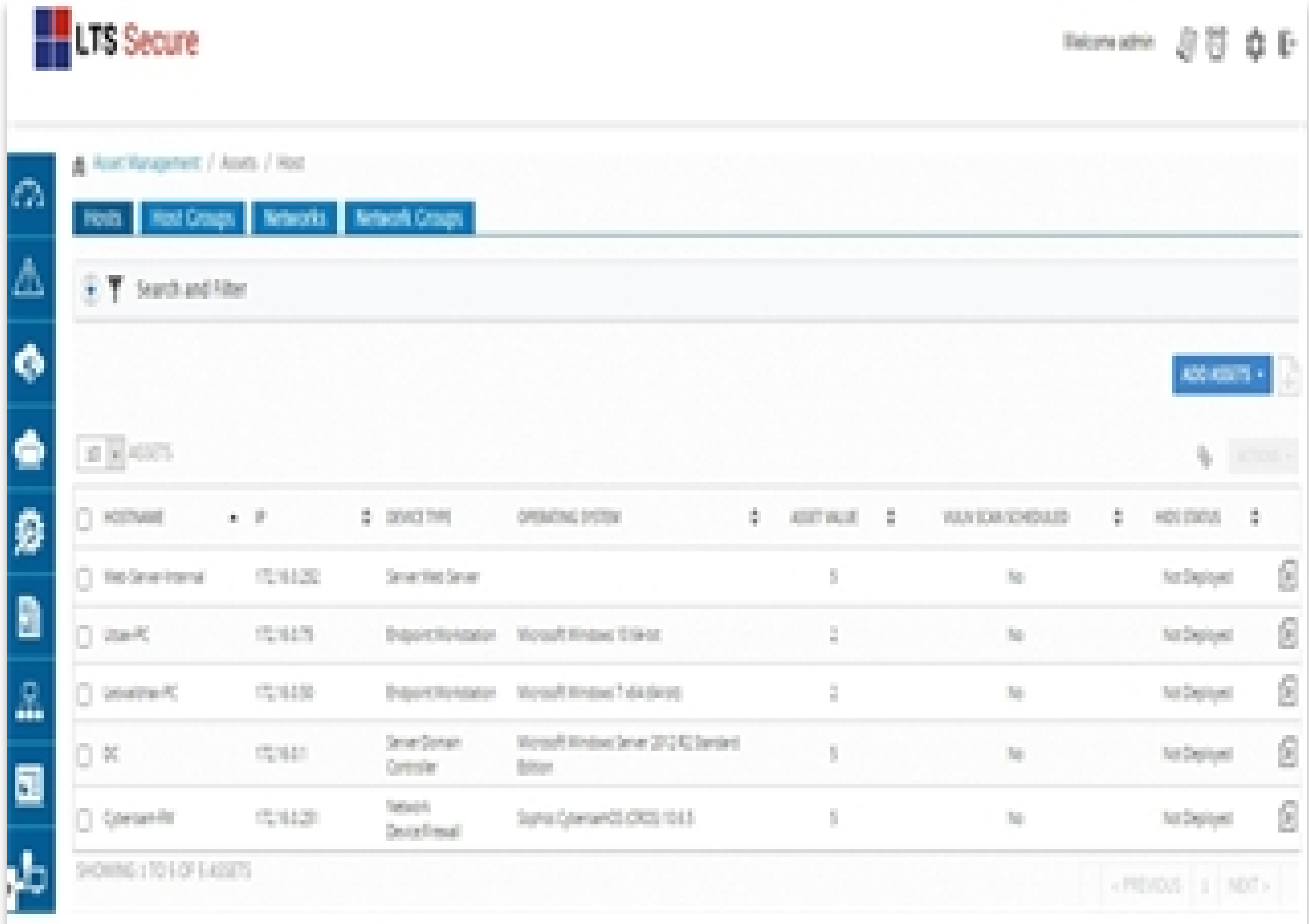
File Renamed	Files Modified	Folder Created
110	59	35

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Security information and event management (SIEM) continuously monitors all devices, servers, applications, users and infrastructure components for security threats protecting the IT assets and digital data of corporate organizations further helping achieve Zero Trust Security.

Modules

- Asset Discovery
- Vulnerability Assessment
- Security Analytics
- Event Correlation
- Intrusion Detection
- Threat Intelligence
- Compliance Reporting



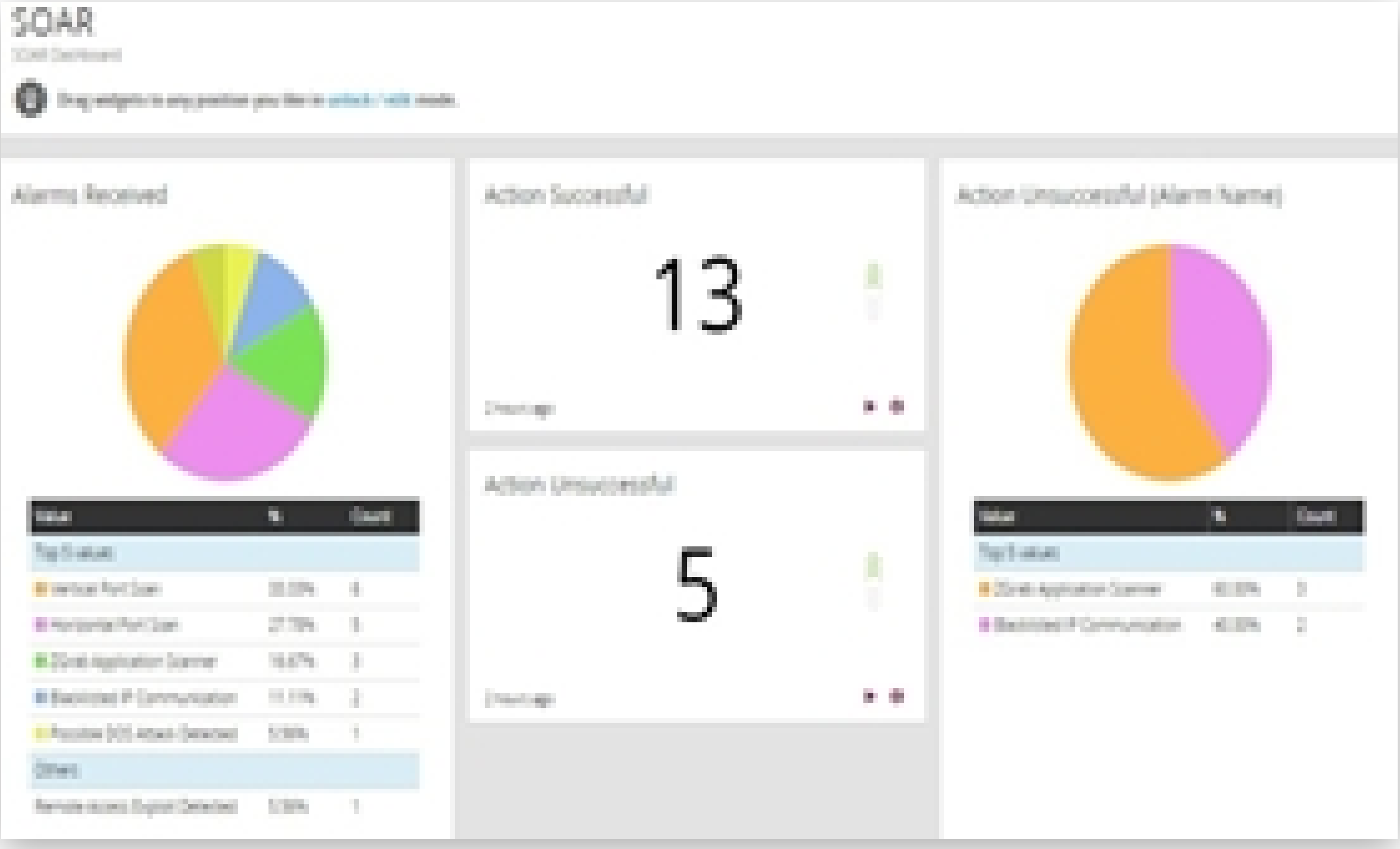
HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
Web-Server-Internal	172.16.0.[illegible]	Server/Web Server		5	No	Not Deployed
User-PC	172.16.0.[illegible]	Endpoint/Workstation	Microsoft Windows 10 [illegible]	2	No	Not Deployed
[illegible]-PC	172.16.0.[illegible]	Endpoint/Workstation	Microsoft Windows 7 x64 [illegible]	2	No	Not Deployed
DC	172.16.0.1	Server/Domain Controller	Microsoft Windows Server 2012 R2 Standard Edition	5	No	Not Deployed
Cyberoam-FW	172.16.0.[illegible]	Network Device/Firewall	Sophos CyberoamOS (CROS) 10.6.[illegible]	5	No	Not Deployed

SHOWING 1 TO 5 OF 5 ASSETS

CRITICAL MODULES OF LTS SECURE ZERO TRUST MODEL

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)

Security Orchestration, Automation and Response (SOAR) ensures efficient collection of data of various security threats from multiple sources and responds to these threats accordingly with or without human help. This comprehensive suite of security services adds immensely to Zero Trust security with various modules targeting specific issues.

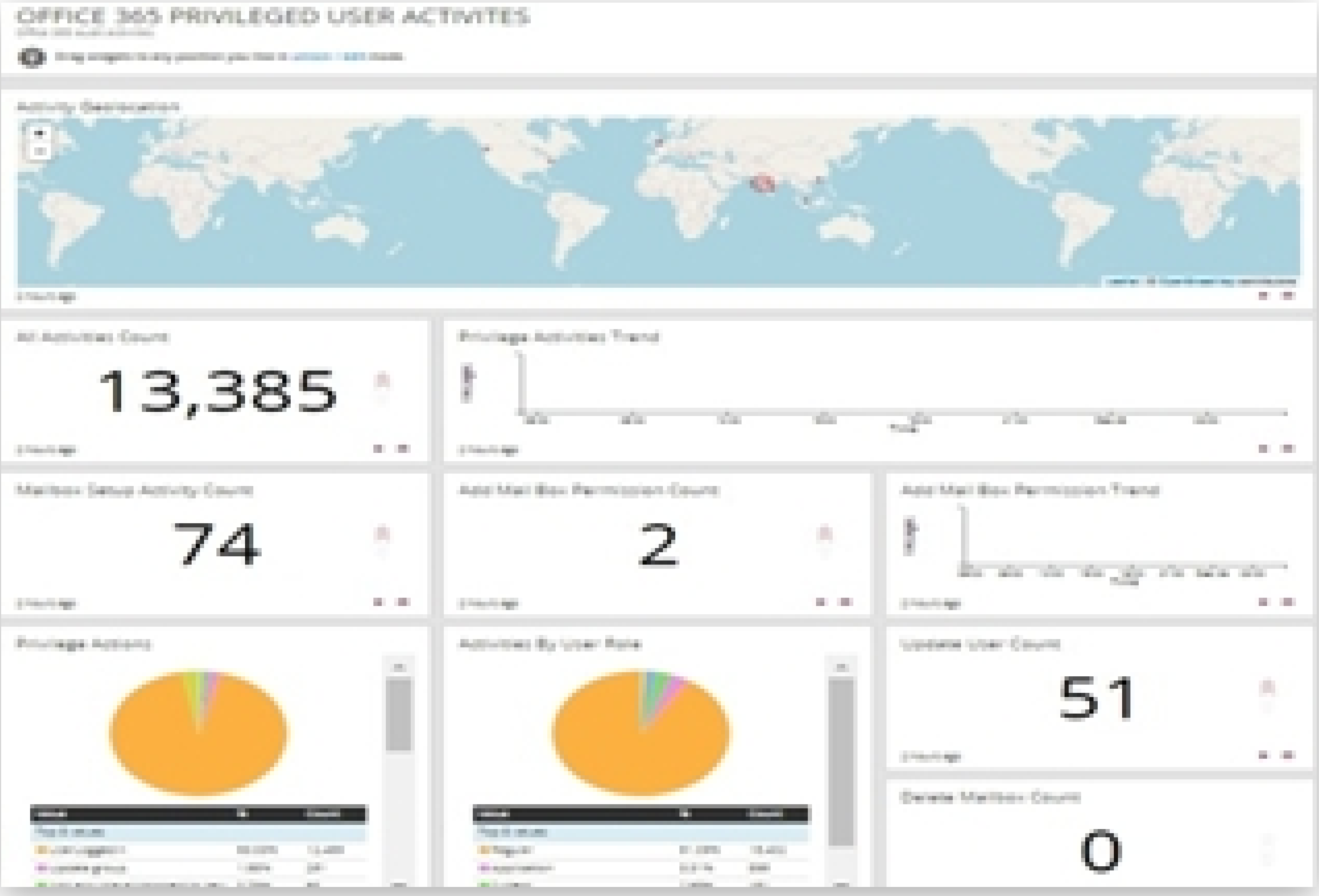

SOAR
SOAR Dashboard
Drag widgets to any position you like in unlock / edit mode.
Alarms Received
Value
%
Count
Top 5 values
Vertical Port Scan 33.33% 6
Horizontal Port Scan 27.78% 5
ZGrab Application Scanner 16.67% 3
Blacklisted IP Communication 11.11% 2
Possible DOS Attack Detected 5.56% 1
Others
Remote access Exploit Detected 5.56% 1
Action Successful
13
2 hours ago
Action Unsuccessful
5
2 hours ago
Action Unsuccessful (Alarm Name)
Value
%
Count
Top 5 values
ZGrab Application Scanner 60.00% 3
Blacklisted IP Communication 40.00% 2

Modules

- Security Orchestration
- Security Automation
- Automatic Response
- Incident Management
- Flexible Integrations
- Dashboards and Reports

USER ENTITY BEHAVIOR ANALYTICS (UEBA)

User entity behavior analytics (UEBA) solution makes use of machine learning and deep learning to model user and entity behavior to detect signs of abnormal and risky behavior occurring inside company environment.


OFFICE 365 PRIVILEGED USER ACTIVITES
Activity Geolocation
All Activities Count
13,385
Privilege Activities Trend
Mailbox Setup Activity Count
74
Add Mail Box Permission Count
2
Add Mail Box Permission Trend
Privilege Actions
Activities By User Role
Update User Count
51
Delete Mailbox Count
0

Modules

- Log Collection & Management
- Context & Enrichment
- Dashboarding
- Threat Detection & Investigation
- Incident Prioritization & Filtering

IMPLEMENTATION OF LTS SECURE ZERO TRUST MODEL

- **Identifying Critical Data**

  Initiate Zero Trust architecture by first locating sensitive business information and strategies and defining the area.

- **Limited Access**

  Exercising limited access ensures only right people have access to company assets after proper authentication and verification.

- **Preventative Measures**

  Enforcing Multi-factor Authentication to provide another layer of verification, implementing least privilege principle to ensure minimum amount of access to user and Micro-segmentation to prevent unauthorized lateral movement.

- **Threat Monitoring**

  Constantly monitoring all activity inside your environment including On-Premise & the Cloud.

- **Apply Analytics**

  Use security analytics to detect internal and external threats.

- **Base Lining**

  Compare current trends and activity with past baseline behavior to detect anomalies.

SUPPORTED ENVIRONMENTS

- Operating System
- VM's
- Database
- Networking Devices
- Security Solutions (NGFW, WAF, EPP, EDR, etc)
- Cloud

LTS SECURE'S ZERO TRUST MODEL DEPLOYMENT REQUIREMENTS (INCLUDING HARDWARE AS WELL AS SOFTWARE)

LTS Secure's Zero Trust Model has the following Hardware and Software requirements for deployment:

LTS SIEM Requirements

Recommended Hardware/Software		Server Quantity
Operating System	LTS Secure Operating System	1
Platform	VMware ESXi 5.5 and above/ Hyper-V	
Processor	12 Core VCPU	
Memory	16 GB	
Ethernet	1 GB X 2	
Hard Disk	500 GB(SAS)	
Installation Media	CD/DVD/USB	

- Require DNS Server to resolve other host names in the network
- Require host names to get access to server
- Static IP address to deploy SIEM Server
- Require a Netmask
- Require Gateway to route to other network

LTS Secure Logger Requirements

Recommended Hardware/Software		Server Quantity
Operating System	CentOS 7.5 minimal	1
Platform	VMware ESXi 5.5 and above/ Hyper-V	
Processor	8 Core VCPU	
Memory	16 GB	
HDD for OS	160 GB	
Live Data Storage	100 GB(Per day)* as per retention period	
Backup Storage	60 GB(Per day)* as per retention period	
Installation Media	CD/DVD/USB	

- Require DNS Server to resolve other host names in the network
- Require host names to get access to server
- Static IP address to deploy Logger
- Require a Netmask
- Require Gateway to route to other network

LTS Secure IDAM Requirements

Recommended Hardware/Software		Server Quantity
Operating System	CentOS 7 and JDK 8	1
Platform	VMware ESXi 5.5 and above/ Hyper-V	
Processor	8 Core VCPU	
Memory	16 GB	
HDD for OS	500 GB	
Installation Media	CD/DVD/USB	

- Require DNS Server to resolve other host names in the network
- Require host names to get access to server
- Static IP address to deploy Logger
- Require a Netmask
- Require Gateway to route to other network

LTS Secure Sensor Requirements

Recommended Hardware/Software		Server Quantity
Operating System	LTS Secure Operating System	1 for each location
Platform	VMware ESXi 5.5 and above/ Hyper-V	
Processor	8 Core VCPU	
Memory	8 GB	
Hard Disk	260 GB	
Installation Media	CD/DVD/USB	

- Require DNS Server to resolve other host names in the network
- Require host names to get access to server
- Static IP address to deploy Sensor
- Require a Netmask
- Require Gateway to route to other network

KEY BENEFITS WITH LTS SECURE'S ZERO TRUST MODEL

Uniform Security

Enforce your complete security mechanism across entire infrastructure.

Remote Access

Allow your employees to work more securely from anywhere.

Risk Mitigation

Reduce security gaps and lower the risk of lateral movement.

Secured Cloud Environment

Enforce stringent security controls to your cloud environment.

Increased Visibility

Centralized logging for inside to detect patterns of unusual/ suspicious behavior.

Minimize risk by discovering assets & better visibility.

Regain control in your cloud environment.

Security analytics, orchestration & automation helps secure your data.

Expedite your compliance audit initiative

LTS SECURE'S ZERO TRUST MODEL ENABLES YOUR ORGANIZATION WITH

- Integrated solution to boost the enterprise ability to do compliance auditing
- Centralized policy administration facilitates application-specific access with a streamlined, modest user experience.
- Data privacy and sovereignty with full encryption of user and application data.
- Scalable and cloud-native service with deployment flexibility and quick implementation for enhanced operational efficiency
- Enables Secure Access to Multi-Cloud and Data Center co-exists with and extends LTS Secure's Security Access portfolio for Hybrid IT
- Clear and quickest visibility and mitigation to malicious and anomalous activity
- Fast and flexible deployment across on-premises and multicloud resources

With LTS Secure's Zero Trust Model, Transform it into a Risk-Free and Trusted Corporate Environment.

TO REQUEST A LIVE DEMO OR FOR MORE INFORMATION ON LTS SECURE ZERO TRUST MODEL, PLEASE GET IN TOUCH WITH US:

✉ enquiry@ltssecure.com   www.ltssecure.com

About LTS Secure

LTS Secure is a global provider of Cyber security services with client spanning across industries. Offering security Suite to rationalize, prioritize & automate response to risks in your environment. LTS Secure provides comprehensive Cyber Security solutions with continuous monitoring at all layers of the IT stack including network packets, flows, OS activities, content, user behaviors and application transactions. Detect and Prevent Fraud, Data Leaks and Advanced Internal as well as External Attacks with advanced Security Orchestration, Automation and Response solutions.

LTS Secure