XcellSecure

Splunk-as-a-Service

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered By:

splunk>

BUILD FOR A DATA-DRIVEN FUTURE | BRING DATA TO EVERY QUESTION, DECISION & ACTION.

Splunk Cloud | Splunk ITSI | Splunk Insights for AWS | Splunk for IoT | VictorOps | Splunk Enterprise Security | Splunk Phantom | Splunk UBA

sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud +91-22-67111555

XcellSecure

Why Choose Splunk

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

XcellHost Support
24x7 Delightfull Support

Reasons To Choose Splunk Services

- Act Faster
- Accelerate Innovation
- Amplify your data's impact
- Scale without the stress
- Professional services
- Support and Training
- Engaged community of passionate experts
- Vibrant ecosystem of partners and developers
- Smart insights driven by AI & ML
- Reduced Operating Costs
- Modernize on a single data platform
- Cutting edge mobile & augmented reality technology.

Splunk Certifications

- splunk> ACCREDITED ES IMPLEMENTATION
- splunk> ACCREDITED SALES ENGINEER III
- splunk> ACCREDITED CORE IMPLEMENTATION
- splunk> ACCREDITED IMPLEMENTATION FUNDAMENTALS
- splunk> ENTERPRISE CERTIFIED ADMIN
- splunk> ENTERPRISE CERTIFIED ARCHITECT
- splunk> CORE CERTIFIED POWER USER
- splunk> CERTIFIED DEVELOPER

XcellSecure

Splunk IT Service Intelligence

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: splunk>

Predict & prevent with one unified monitoring experience.

Get started faster with purpose-built pre-packaged modules, apps and add-ons for ITSI.

Features

- Troubleshooting and Monitoring
- AIOps Platform
- 360-degree Insights
- Future Degradation
- Access, Server, InfoSec logs
- Wrangle large amount of data in real time
- Anomaly Detection

Key Benefits

- Transform Operations
- Get ahead of outages
- Reduce MTTI & MTTR
- Increase mean time between failures (MTBF)
- Decrease mean time to detect (MTTD) through prediction
- Visualize & Cross Correlate
- Deploy at scale — and in days not months

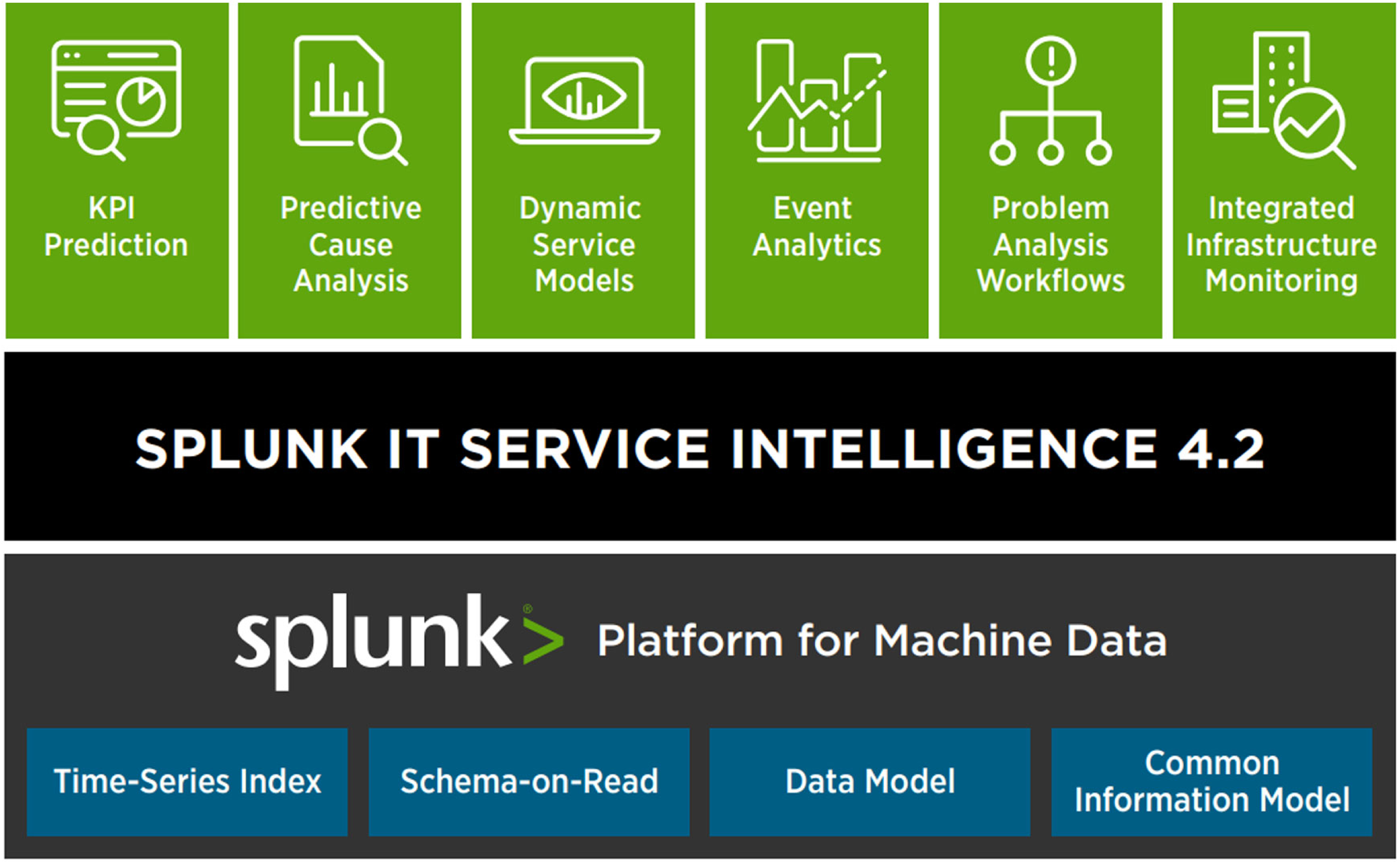
Learn More https://www.xcellhost.cloud/splunkitsi

XcellSecure | Splunk IT Service Intelligence

Key Capabilities

- Shift to Predictive IT
- Deep Dive to Find Your Problems Fast
- Weather the Event Storm
- Enjoy a Full-Stack Monitoring Suite
- Initiate remediation & Automate incident workflows.

Refrence Architecture



KPI Prediction

Predictive Cause Analysis

Dynamic Service Models

Event Analytics

Problem Analysis Workflows

Integrated Infrastructure Monitoring

SPLUNK IT SERVICE INTELLIGENCE 4.2

splunk> Platform for Machine Data

Time-Series Index

Schema-on-Read

Data Model

Common Information Model

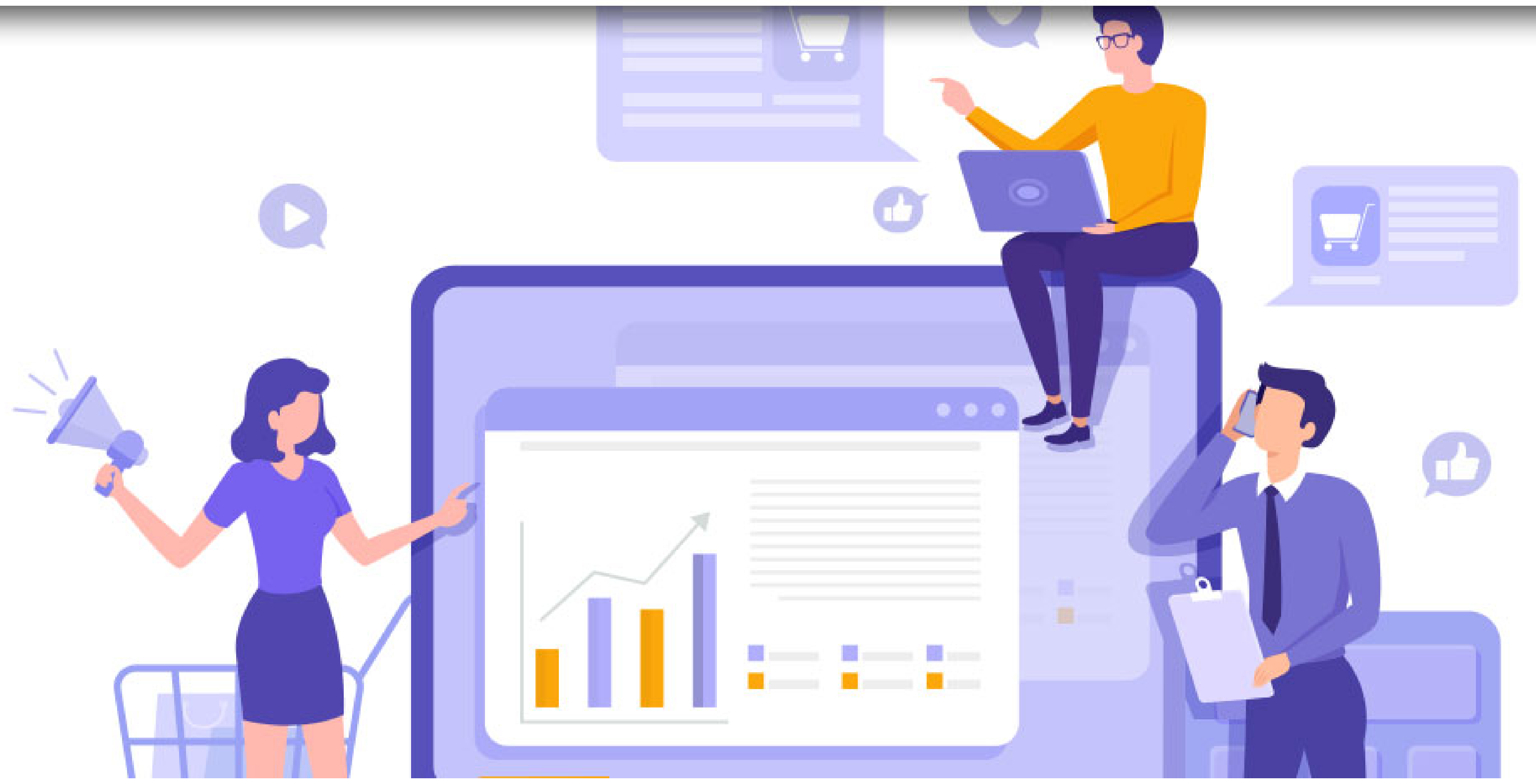
XcellSecure

Splunk Insights for AWS Cloud Monitoring

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: splunk> aws



Analytics and visibility for your AWS workloads.

See what's happening in your Amazon Web Services (AWS) deployments with end-to-end security, operational & cost-management insights.

Features

- Central Logging & Monitoring Security Posture
- Troubleshooting & AIOps Platform
- Physical Security
- Data Encryption
- Authentication and Access Management
- Threat Detection
- Data Integrity

Key Benefits

- Enhance Security
- Help ensure Adherence
- Leverage Machine Learning
- Effectively manage AWS costs
- Operational Insights
- real-time awareness of performance
- Migrate Successfully & adherence to security and compliance

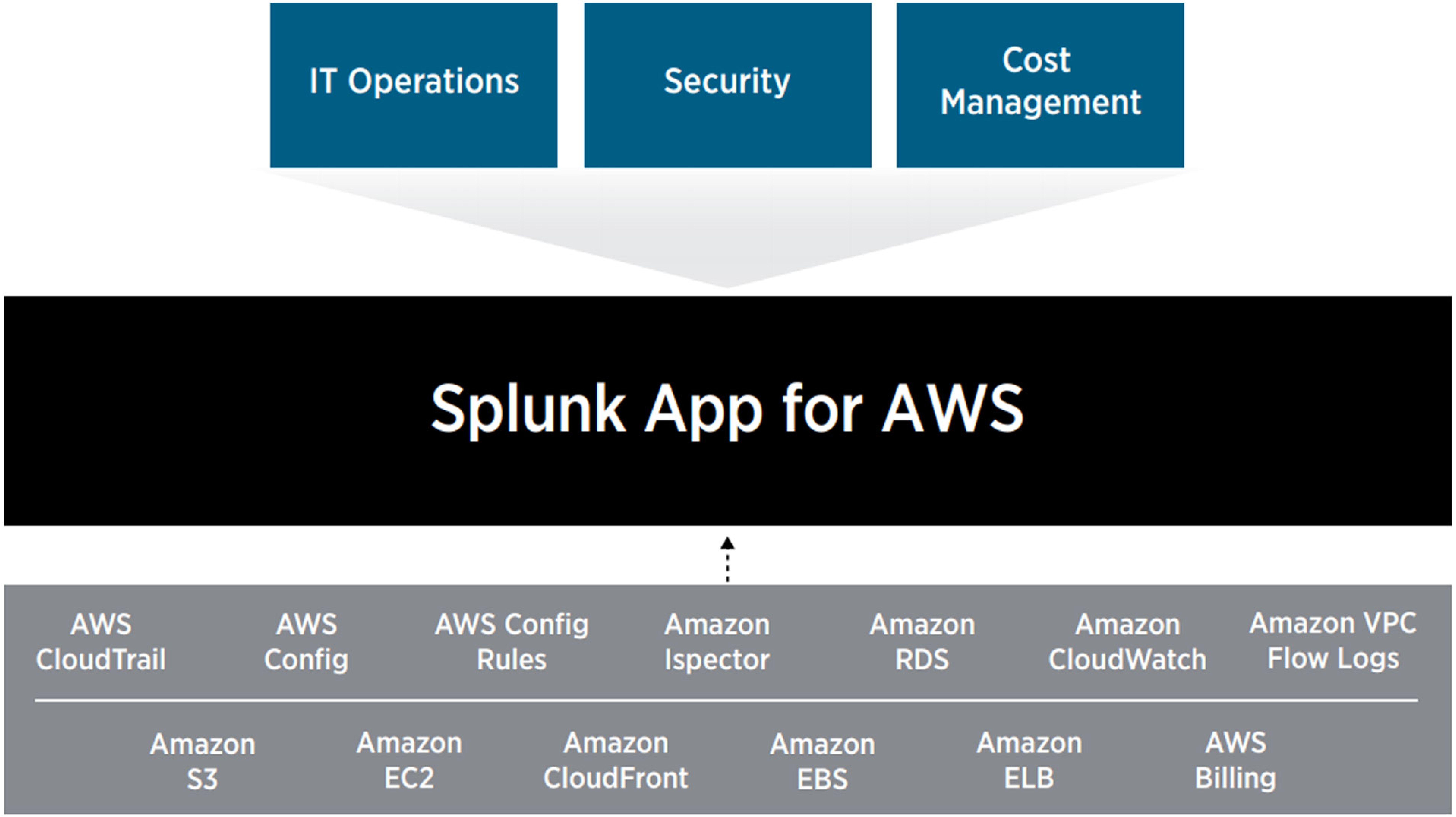
Learn More https://www.xcellhost.cloud/splunkinsight

XcellSecure | Splunk Insights for AWS Cloud Monitoring

Key Capabilities

- Comprehensive Security dashboards
- Visualize your AWS resources
- Billing Management
- Cost Management
- Usage Monitoring

Refrence Architecture



IT Operations

Security

Cost Management

Splunk App for AWS

AWS CloudTrail

AWS Config

AWS Config Rules

Amazon Ispector

Amazon RDS

Amazon CloudWatch

Amazon VPC Flow Logs

Amazon S3

Amazon EC2

Amazon CloudFront

Amazon EBS

Amazon ELB

AWS Billing

XcellSecure

Splunk® App for Infrastructure

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: splunk>

Unify and correlate logs and metrics in one solution.

Comprehensive infrastructure monitoring, alerting & investigation

Features

- Infrastructure Monitoring
- Streamlined Workflows & Advanced Alerting
- Pre-built and custom visualizations performance
- Infrastructure Data with Service Context
- Alerting & Investigation
- Grouping & filtering entities.
- Unified metrics and logs

Key Benefits

- Simplify and modernize
- Get full visibility
- Speed up investigations
- Get to root Cause Faster
- Improve productivity
- Cross-tier correlations
- streamlined troubleshooting workflows

Learn More https://www.xcellhost.cloud/splunkapp

sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud +91-22-67111555

XcellSecure | Splunk® App for Infrastructure

Key Capabilities

Monitoring metrics That matter

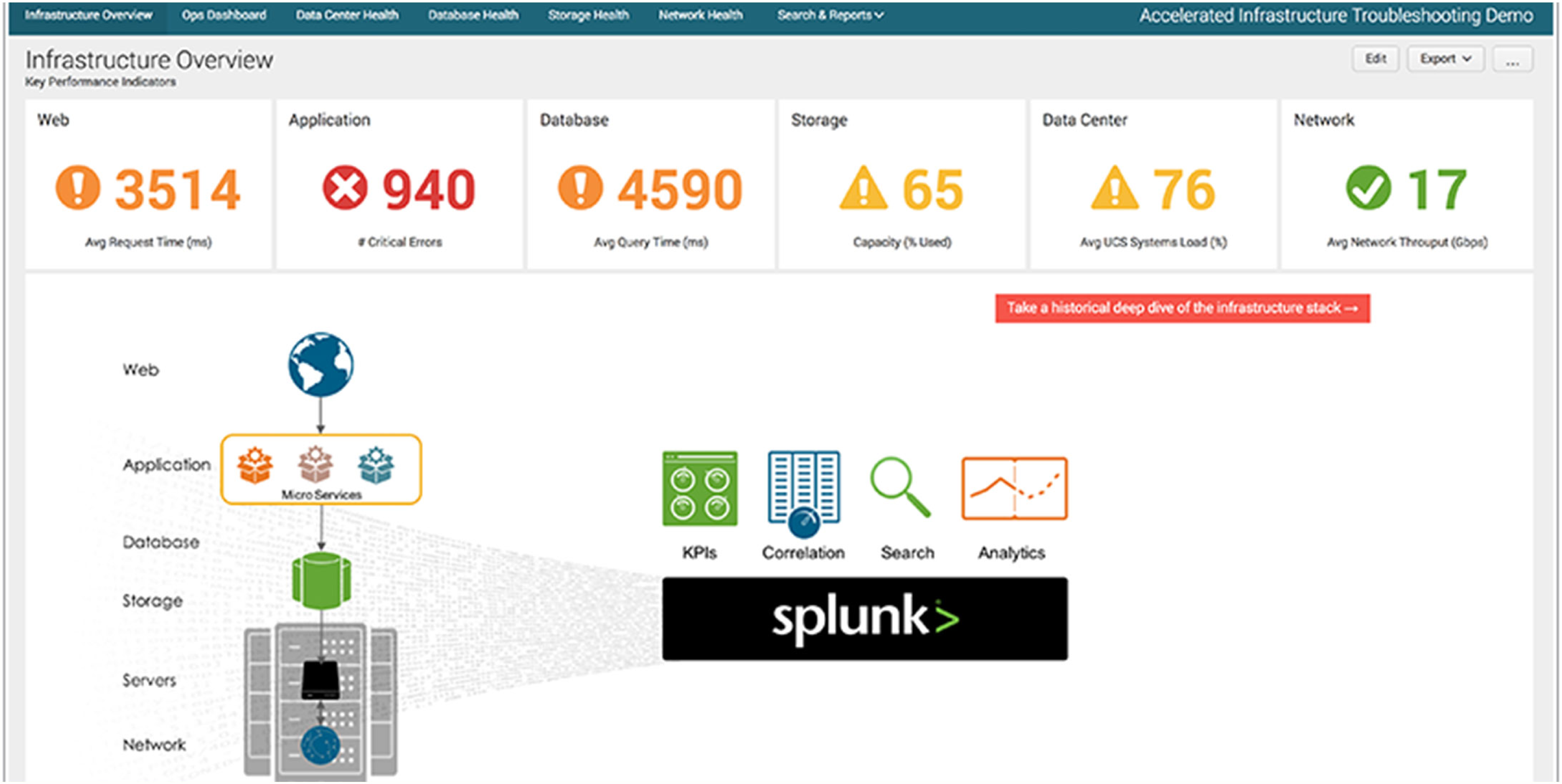
Advanced alerting for faster triage

Visualizations for real time monitoring

Correlations pinpoint performance trends

Enrich infrastructure data with service context

Dashboard



Infrastructure Overview

Key Performance Indicators

Web	Application	Database	Storage	Data Center	Network
3514	940	4590	65	76	17
Avg Request Time (ms)	# Critical Errors	Avg Query Time (ms)	Capacity (% Used)	Avg UCS Systems Load (%)	Avg Network Throuput (Gbps)

Take a historical deep dive of the infrastructure stack →

XcellSecure

VictorOps

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
splunk> VictorOps

VictorOps Make On-Call Suck Less.

On-Call Management + Automated Escalations + Centralized System Information

Features

- ChatOps & Reporting
- Mobile & Noise Suppression
- Delivery Insights & Live Call Routing
- API & Webhooks.
- Runbooks & Graphs

Life Cycle

- Detection
- Response
- Remediation
- Analysis
- Readiness

Key Benefits

- System,Application Performance Monitors
- MTTA/ MTTR
- Post-Incident Review
- Empower DevOps Teams
- Improve the On-Call Experience
- Faster Incident Response & Incident Frequency
- Expert Support 24X7

Learn More https://www.xcellhost.cloud/victorOps

sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud +91-22-67111555

Key Capabilities

On-Call Scheduling
Made Simple

Rapid Incident
Response

Incident
Analysis

Real-Time Visibility Helps
Improve Application Delivery

Incident
Reporting

Featured Integrations

Amazon CloudWatch
Cloud Monitoring

Grafana
Analytics

Nagios / Nagios XI
System Monitoring

New Relic
APM

Prometheus
Time Series

SignalFX
Cloud Monitoring

Slack
Collaboration

Splunk
Analytics

Splunk Insights for Infrastructure
Analytics

Splunk ITSI
Analytics

Splunk Phantom
Security

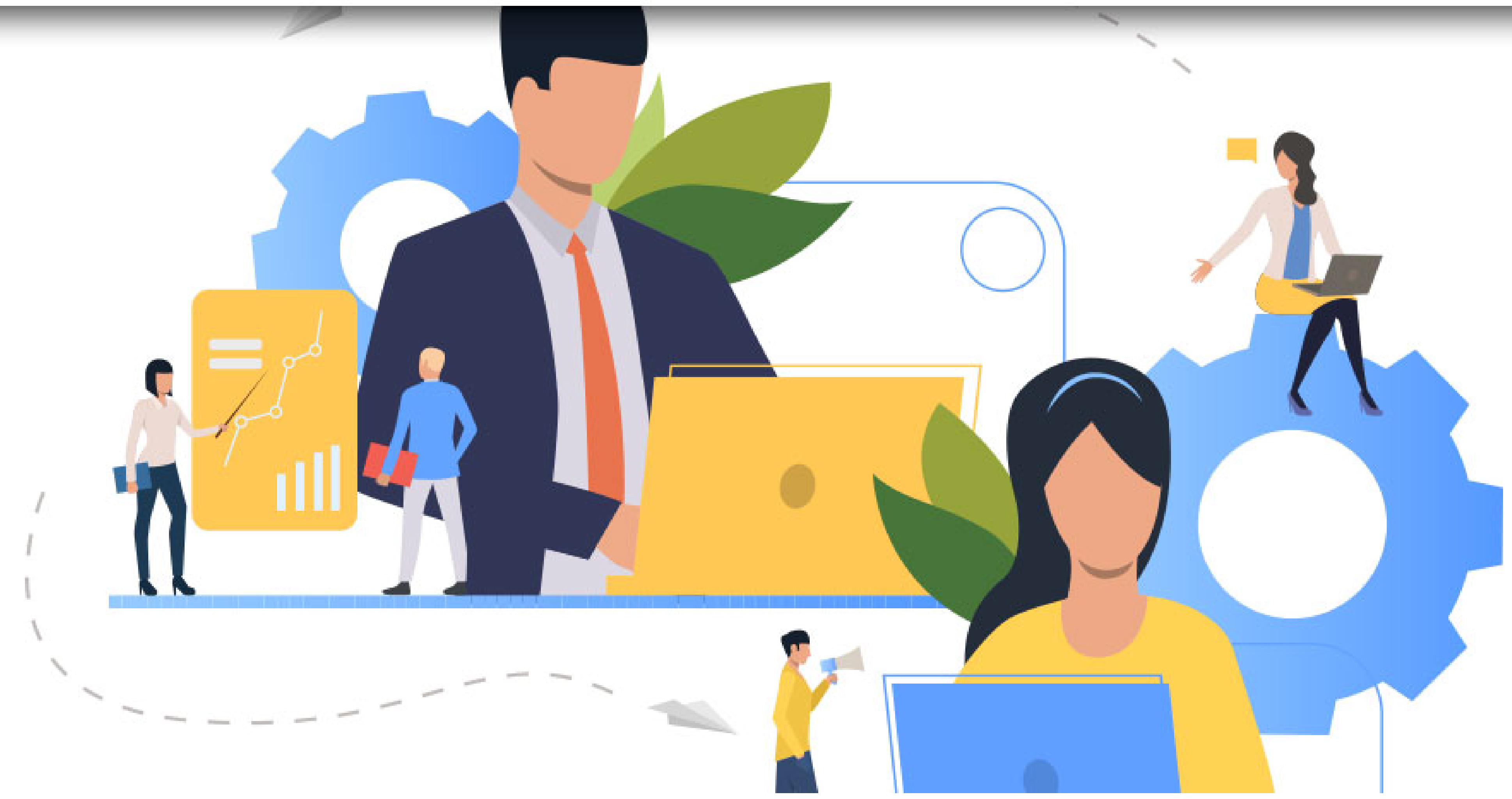
VictorOps to ServiceNow
Service Desk

XcellSecure

Splunk® Enterprise Security (SIEM)

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: splunk>



Drop your breaches with an analytics -driven SIEM solution

Analytics-driven security and continuous monitoring for modern threats

Features

- Incident Review and Classification
- Investigator Journal & Investigation Timeline
- Advanced Threat Investigation
- Protocol Intelligence
- Threat Intelligence Framework
- Identity and Asset Framework
- Risk-Based Analysis

Key Benefits

- Optimize security operations
- Improve security posture
- Enhance investigation capabilities
- Make better informed decisions
- Flexibility to customize
- Manage Alerts
- Expert Suppport 247X7

Learn More https://www.xcellhost.cloud/splunksiem

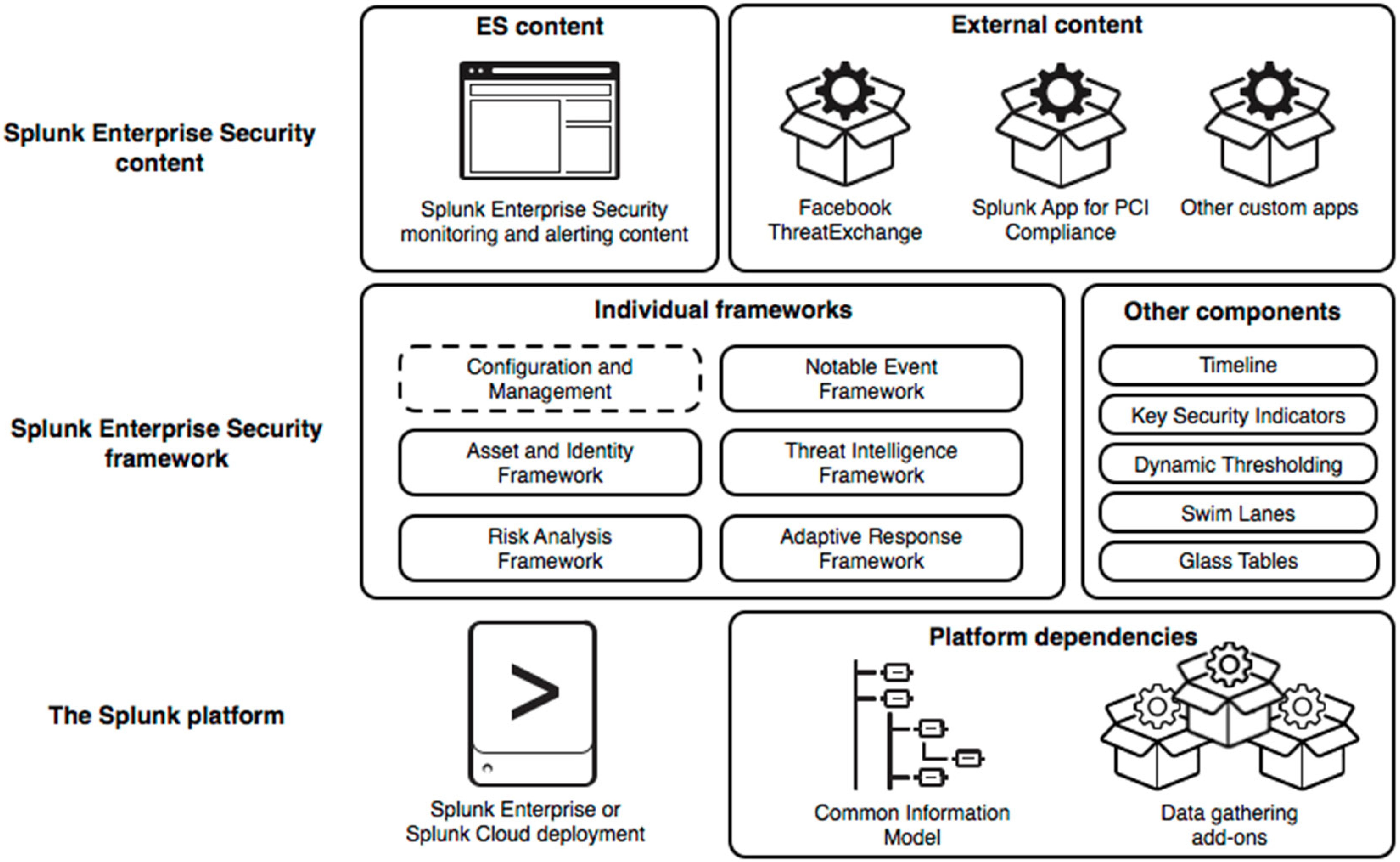
sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud +91-22-67111555

XcellSecure | Splunk Enterprise Security (SIEM)

Key Capabilities

- Improve Security Operations
- Investigative Tools to Respond Fast
- Automate and Respond
- Incident Review and Classification
- Big Data Platform for Security Intelligence

Splunk Enterprise Security Integrations



Splunk Enterprise Security content

ES content

Splunk Enterprise Security monitoring and alerting content

External content

Facebook ThreatExchange

Splunk App for PCI Compliance

Other custom apps

Splunk Enterprise Security framework

Individual frameworks

Configuration and Management

Notable Event Framework

Asset and Identity Framework

Threat Intelligence Framework

Risk Analysis Framework

Adaptive Response Framework

Other components

Timeline

Key Security Indicators

Dynamic Thresholding

Swim Lanes

Glass Tables

The Splunk platform

Splunk Enterprise or Splunk Cloud deployment

Platform dependencies

Common Information Model

Data gathering add-ons

XcellSecure

SPLUNK® Phantom (SOAR)

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: splunk> phantom

Maximize your SOC efficiency with SOAR capabilities

Supercharge your security operations with Splunk Phantom security automation

Features

- Automate Security Actions using Phantom Playbooks
- Flexible Integrations
- Process Workflows
- Incident Management
- Threat Intelligence
- Collaborate, Respond & Manage Phantom Mission Control
- Orchestrate Security Infrastructure Using Phantom Apps

Key Benefits

- Close your security skills gap
- Act as a force multiplier
- Supercharge your SOC
- Overall mean time to resolve (MTTR)
- Incident Response
- Reduce the amount of uninvestigated & unresolved alerts
- Automate time-consuming investigations & remediate

Learn More https://www.xcellhost.cloud/splunkphantom

sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud +91-22-67111555

XcellSecure | Splunk Phantom (SOAR)

Use Case

Endpoint Quarantine

Suspend Users

Collect Machine Data

Suspend Network Access

Kill Processes

Current Security Operation Process

Observe
Point Products
Orient
Analytics
Decision Making
Acting
FIREWALL
IDS / IPS
ENDPOINT
WAF
ADVANCED MALWARE
FORENSICS
MALWARE DETONATION
SIEM
THREAT INTEL PLATFORM
HADOOP
GRC
TIER 1
TIER 2
TIER 3
FIREWALL
IDS / IPS
ENDPOINT
WAF
ADVANCED MALWARE
FORENSICS
MALWARE DETONATION
AUTOMATED
MANUAL (TODAY)

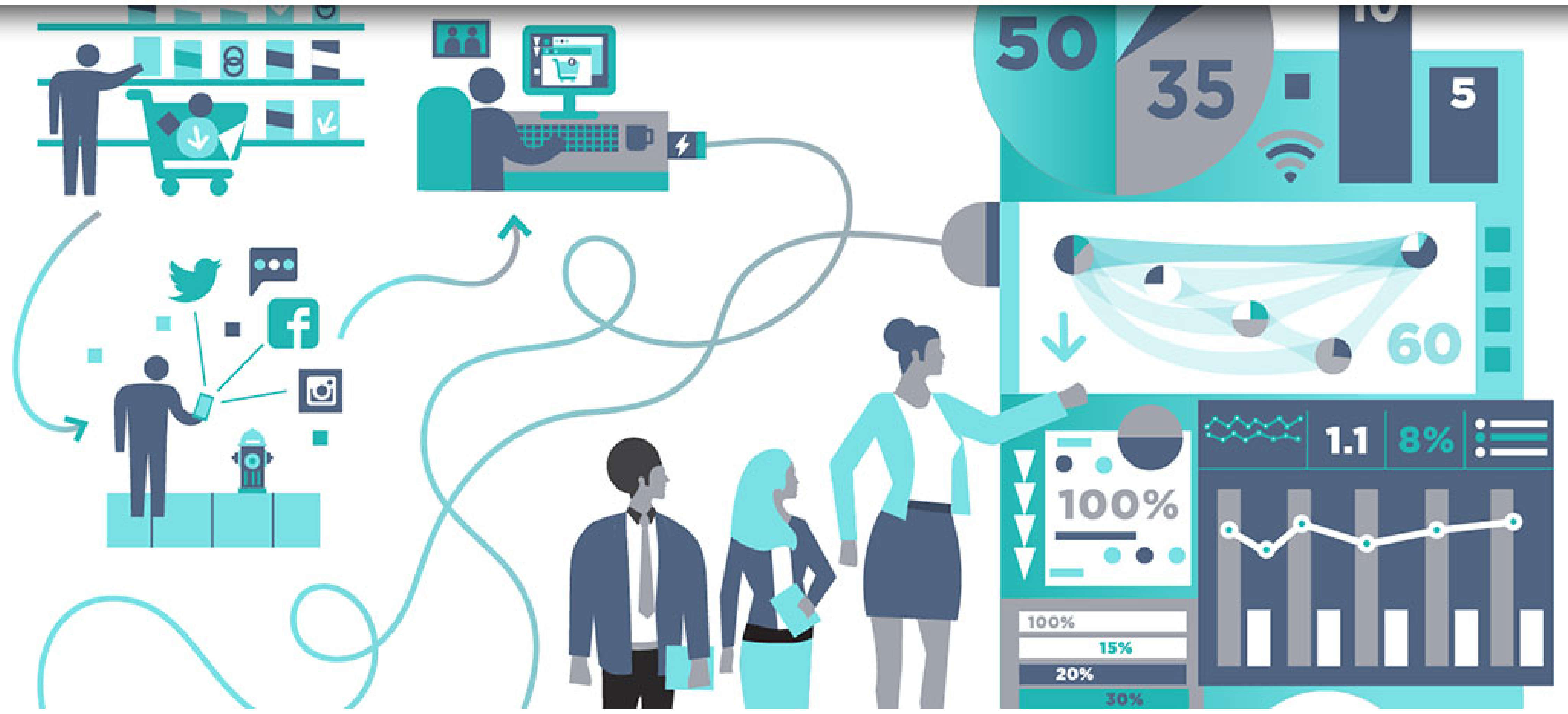
XcellSecure

SPLUNK® User Behavior Analytics (UBA)

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: splunk> | Caspida



Detect unknown threats & anomalous behavior using machine learning

Securing against unknown threats through user and entity behavior analytics

Key Benefits

- Enhance Visibility
- Enhance Detection
- Improve Detection
- Increase security analyst effectiveness
- Easy to use for SOC analysts
- Easy to use incident for responders
- Easy to use for SIEM administrators

Use Case

- Detect compromised accounts
- Detect compromised endpoints.
- Detect data exfiltration.
- Provide context and information for investigations.
- Detect insider abuse, including privileged account abuse.

Learn More https://www.xcellhost.cloud/splunkuba

Use Content Enchancement

- Account Takeover
- Suspicious Behavior
- Lateral Movement
- Cloud Storage
- Data Exfiltration

How Does Splunk UBA Work

NETWORK LOGS

IDENTITY LOGS

ENDPOINT LOGS

SERVER LOGS

APPLICATION LOGS

MACHINE LEARNING

SUSPICIOUS DATA MOVEMENT

UNUSUAL MACHINE ACCESS

FLIGHT RISK USER

UNUSUAL NETWORK ACTIVITY

MACHINE GENERATED BEACON

45+ ANOMALY CLASSIFICATIONS

MACHINE LEARNING

LATERAL MOVEMENT

SUSPICIOUS BEHAVIOR

COMPROMISED ACCOUNT

DATA EXFILTRATION

MALWARE ACTIVITY

20+ THREAT CLASSIFICATIONS

XcellSecure

Splunk for Industrial IoT

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:

splunk>

New insights from sensors, devices & industrial control systems

Generate real-time & predictive insights from your industrial operational data

Features

- Real-Time Monitoring
- Advanced Analytics
- Actionable Intelligence
- Mitigate Failure with built in AI/ML
- Analytics-Driven Security
- Live Alerts & Dashboards
- Powerfull Data Enrichment

Key Benefits

- Gain real-time insight
- Collect, manage and analyze
- Complement & integrate
- Optimate Integrator for PI System to Splunk
- Secure OT Operations
- Kepware Industrial Data Forwarder for Splunk
- HTTP Event Collector (HEC) and Modular Inputs

Learn More https://www.xcellhost.cloud/splunkIOT

✉ sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud ☎ +91-22-67111555

Why Splunk for Industrial Data and the IoT?

- Monitoring and Diagnostics
- Security, Safety
- Compliance
- Predictive Maintenance
- Asset Performance Management

How Connecting Splunk to Industrial Data and the IoT Works

IT Analyst

Security Analyst

Business Analyst

Process Engineer

Search

Alert

Visualize

Predict

Develop

splunk>

kepware

Devices

Networks

Geo-location

Servers

Applications

Virtual Index

OSIsoft

Hadoop Clusters

Amazon EMR on S3

Data Warehouses and Relational Databases

DB Connect

Structured Data

CRM

ERP

CMMS

EAM

MES

Finance

amazon web services
S3
APP

XcellSecure

SignalFx

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
splunk> SignalFx

The only real-time monitoring & observability platform for cloud infrastructure & microservices.

The Only Platform with Streaming Analytics and NoSample™ Tail-Based Distributed Tracing

Solutions

- Infrastructure Monitoring
- Application Monitoring
- Container Monitoring
- Serverless Monitoring
- CI/CD Monitoring
- Cloud Migration
- Cloud Cost Optimizer

Key Benefits

- Better Customer Experience
- Higher Developer Productivity
- Proactive Actionable Alerts
- Centralized Control
- Full Stack Metrics & Distributed Tracing
- Fullstack Correlation
- Uncover deeper insights & easily recognize patterns

Learn More https://www.xcellhost.cloud/signalfx

XcellSecure | SignalFX

Key Capabilities

Instant Visualization	Minimize Noise With Templated Intelligence Alerts.	Directed Troubleshooting	Observability as an Enterprise Service	Asset Performance Management

SignalFX Process

DIRECTED TROUBLESHOOTING
APPLICATIONS
CLOUD INFRASTRUCTURE
TRACES
METRICS
EVENTS
STREAMING
STREAMING
SignalFx
CLOUD MONITORING POWERED BY STREAMING ANALYTICS
Debugging
Root Cause Analysis
Service Mapping
MONITORING AS A SERVICE
Alerting
High Cardinality Analytics
High-Res Visualization
DIGITAL BUSINESS MONITORING
APPLICATION MONITORING
INFRASTRUCTURE MONITORING
REAL-TIME PROBLEM DETECTION

XcellSecure

Business Flow

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
splunk>

Gain insights into your business processes

Explore and visualize business processes for increased transparency

Solutions

- End-to-end process discovery through event stiching
- Rapid process analysis with simple exploration interface
- Investigative drill-down with filtering
- Side-by-side A/B comparison of process flows
- Investigate potential root causes of problems

Key Benefits

- Comprehensive Discovery
- Faster Problem Detection
- Improve Performance
- Centralized Control

Key Capabalities

- Discover Your Business Processes
- Explore Process Variances
- Identify Root Causes

Learn More https://www.xcellhost.cloud/businessflow

sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud +91-22-67111555

XcellSecure

Splunk Cloud

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by: splunk>

Upgrade to the most flexible, secure & cost-effective data platform service

Turn data into answers with Splunk deployed and managed securely, reliably and scalably as a service

Features

- Dashboards and Visualizations
- Monitoring and Alerting
- Support and Services
- Apps , Add-ons & Metrics
- Machine Learning Toolkit (MLTK)
- Scale and Manageability
- Performance & Integrations

Key Benefits

- Fast Time to Value
- Infrastructure Requirements
- Maximize Resources
- Reporting
- Using All Your Data
- Minimal delay and change management
- Experience Integrated ML Analytics

Learn More https://www.xcellhost.cloud/splunkcloud

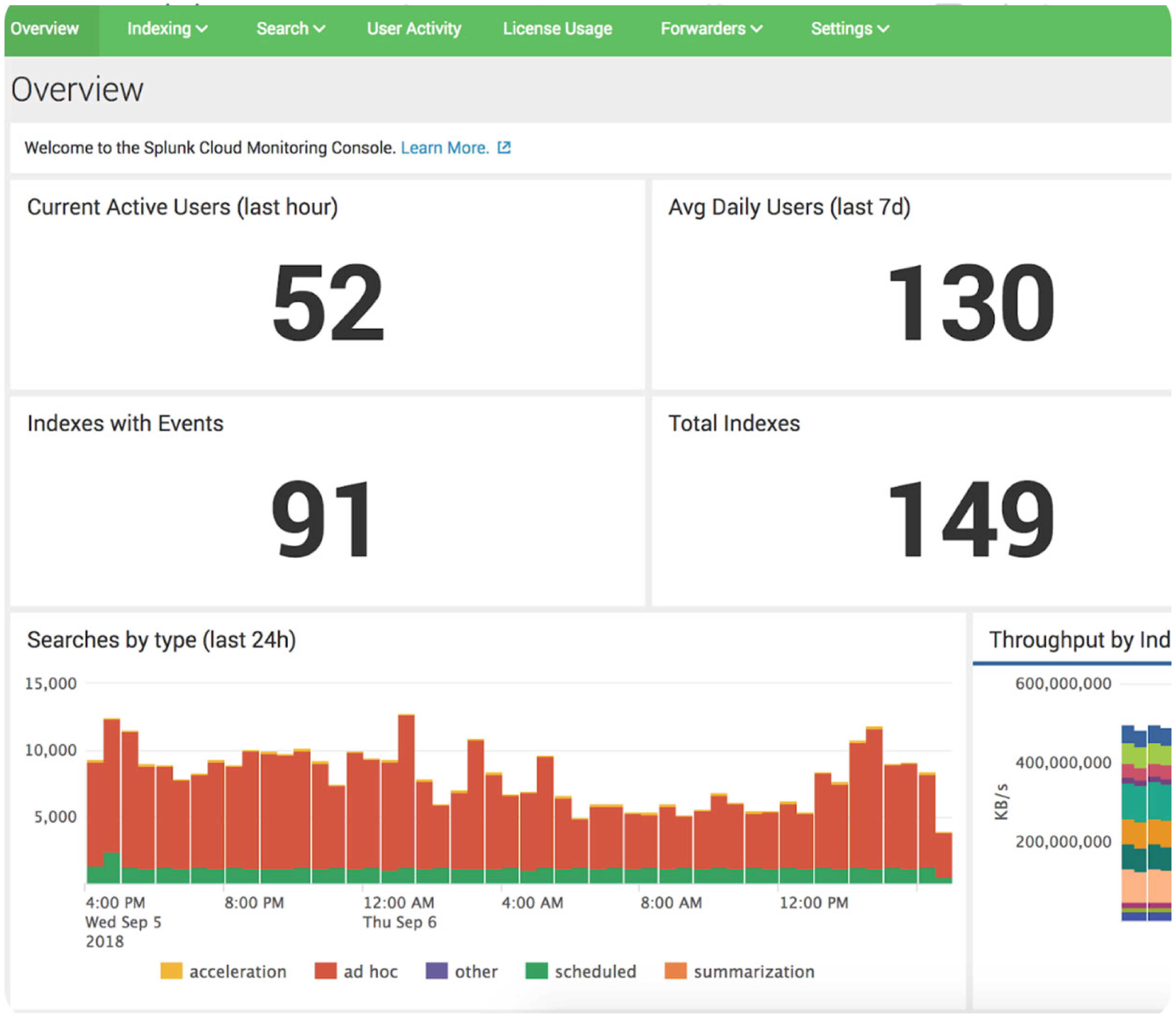
sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud +91-22-67111555

XcellSecure | Splunk Cloud

Key Capabilities

- Splunk Enterprise As a Service
- We'll Do the Heavy Lifting
- AI & ML For Prediction & Self-Healing
- Alerts You Can Count On
- Best-in-class encryption

Dashboard



Overview

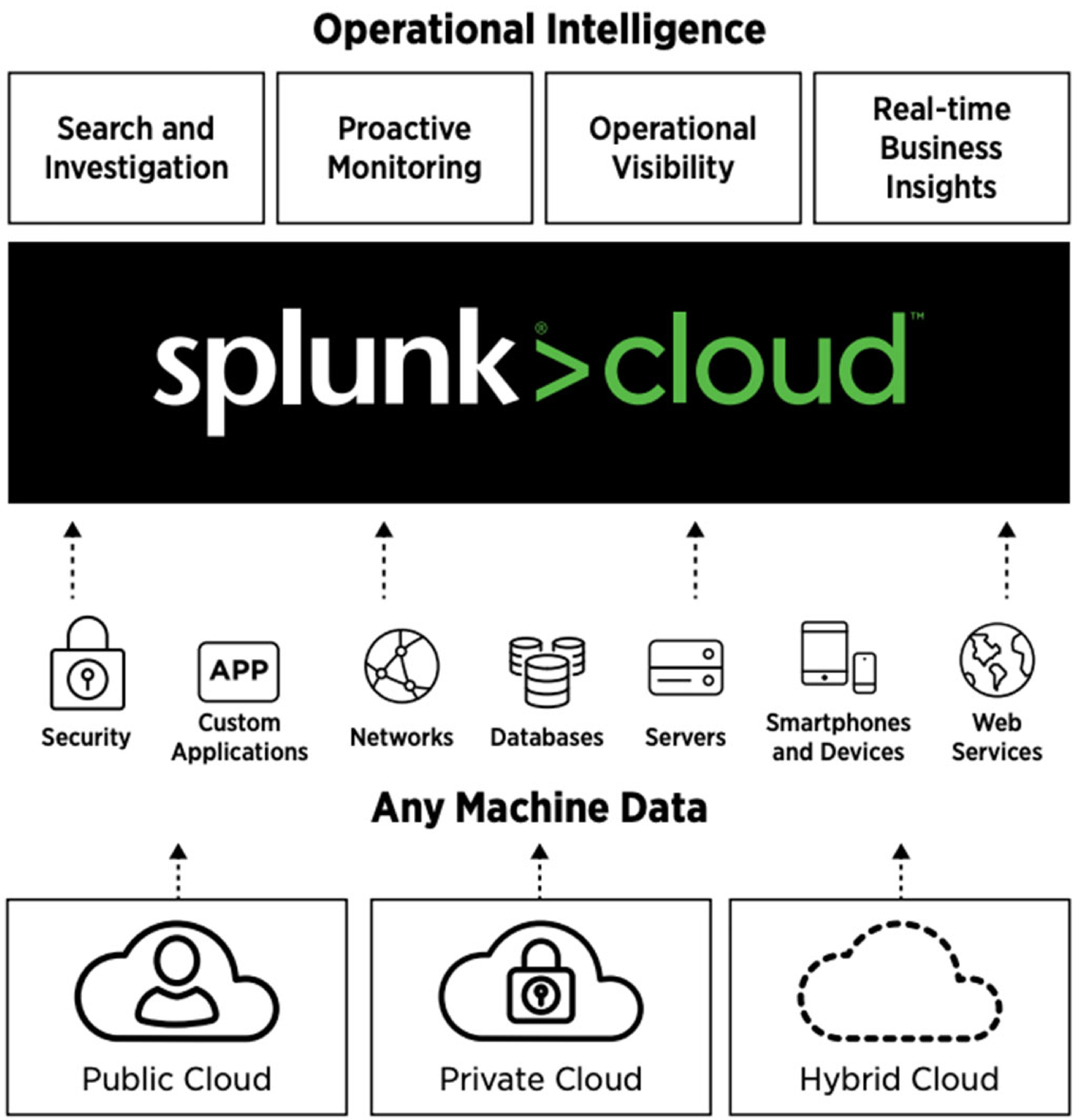
Welcome to the Splunk Cloud Monitoring Console. Learn More.

Current Active Users (last hour) 52	Avg Daily Users (last 7d) 130
Indexes with Events 91	Total Indexes 149

Searches by type (last 24h)

Throughput by Ind

Gain Operational Intelligence



XcellSecure

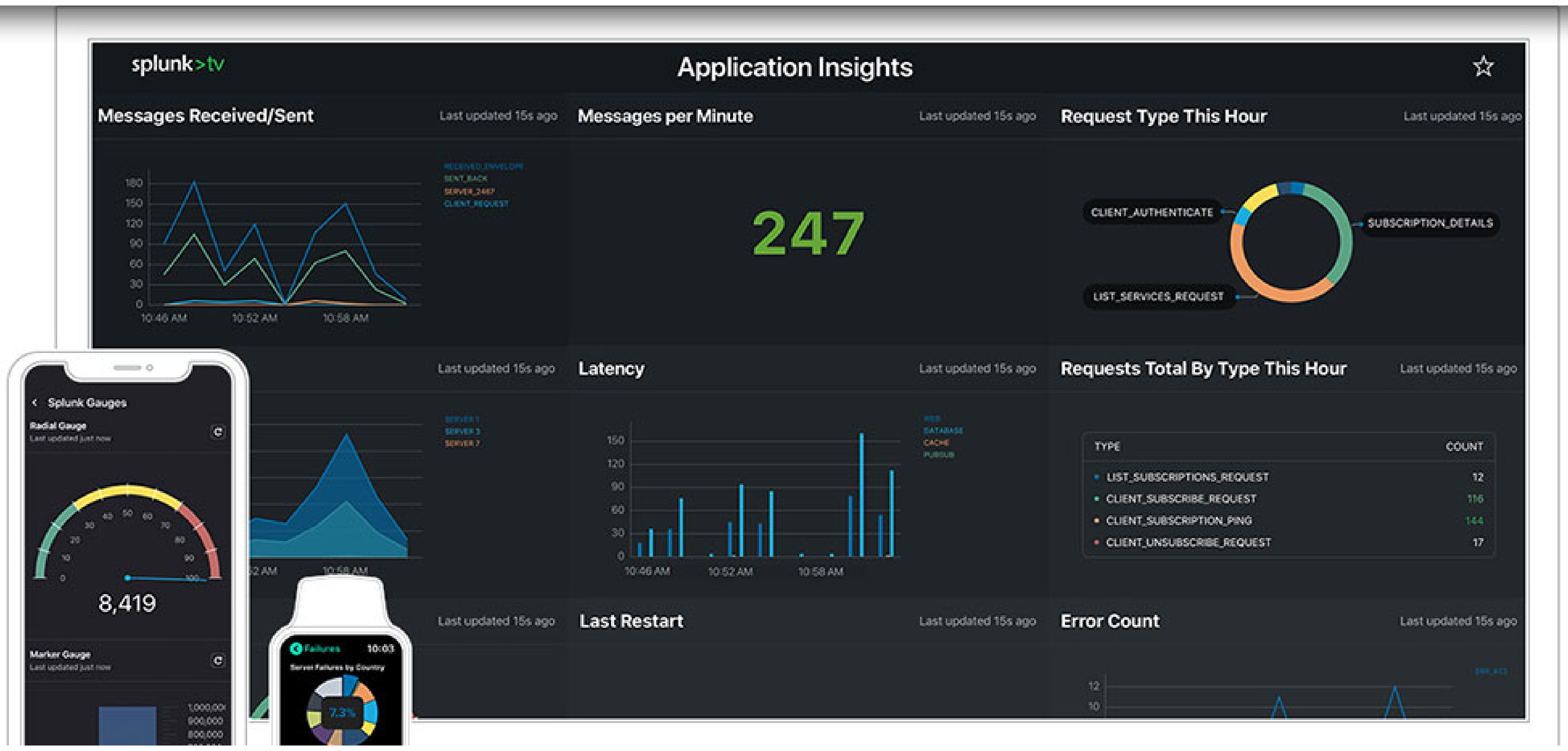
Splunk Enterprise

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:

splunk>



TYPE	COUNT
LIST_SUBSCRIPTIONS_REQUEST	12
CLIENT_SUBSCRIBE_REQUEST	116
CLIENT_SUBSCRIPTION_PING	144
CLIENT_UNSUBSCRIBE_REQUEST	17

The data platform empowering more users, everywhere

Harness the untapped value of your machine data to optimize your organization and deliver an unrivaled customer experience

Features

- Connected Experiences
- Dashboards and Visualizations
- Monitoring and Alerting
- Apps , Add-ons & Metrics
- Machine Learning Toolkit (MLTK)
- Scale and Manageability
- Performance & Integrations

Key Benefits

- Real-Time Visibility
- Data Source Agnostic
- AI & Machine Learning
- Reporting
- Support and Services

Key Capabilities

- Empower Your Users Everywhere
- Get Answers Faster with Metrics
- Experience Integrated ML Analytics

Learn More https://www.xcellhost.cloud/splunkenterprise

sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud 24 +91-22-67111555

XcellSecure

Splunk Platform Comparison

Secure Cloud Services for your online business since 1999.
.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered by:
splunk>

Features	Splunk Free	Splunk Enterprise	Splunk Cloud
Maximum Daily Indexing Volume	500MB	Unlimited	Unlimited
Maximum Users	1	Unlimited	Unlimited
Universal Data Collection/ Indexing	☑	☑	☑
Metrics Store	☑	☑	☑
Data Collection Add-Ons	☑	☑	☑
Monitoring and Alerting		☑	☑
Dashboards and Reports	☑	☑	☑
Search and Analysis	☑	☑	☑
Event Annotation	☑	☑	☑
Automatic Data Enrichment	☑	☑	☑
Anomaly Detection	☑	☑	☑
Tables, Data Models and Pivot	☑	☑	☑
Splunkbase Apps	☑	☑	☑
Splunk Premium Solutions		☑	☑
High Availability		☑	☑
Disaster Recovery		☑	☑
Clustering		☑	☑
Distributed Search		☑	☑
Performance Acceleration		☑	☑
Access Control		Granular and Customizable	Granular and Customizable
Single Sign-On/LDAP		☑	☑
Developer Environment		Full access to APIs and SDKs	Full access to APIs and SDKs
Dynamic Data			
Support	Community	Standard or Premium	Standard or Premium

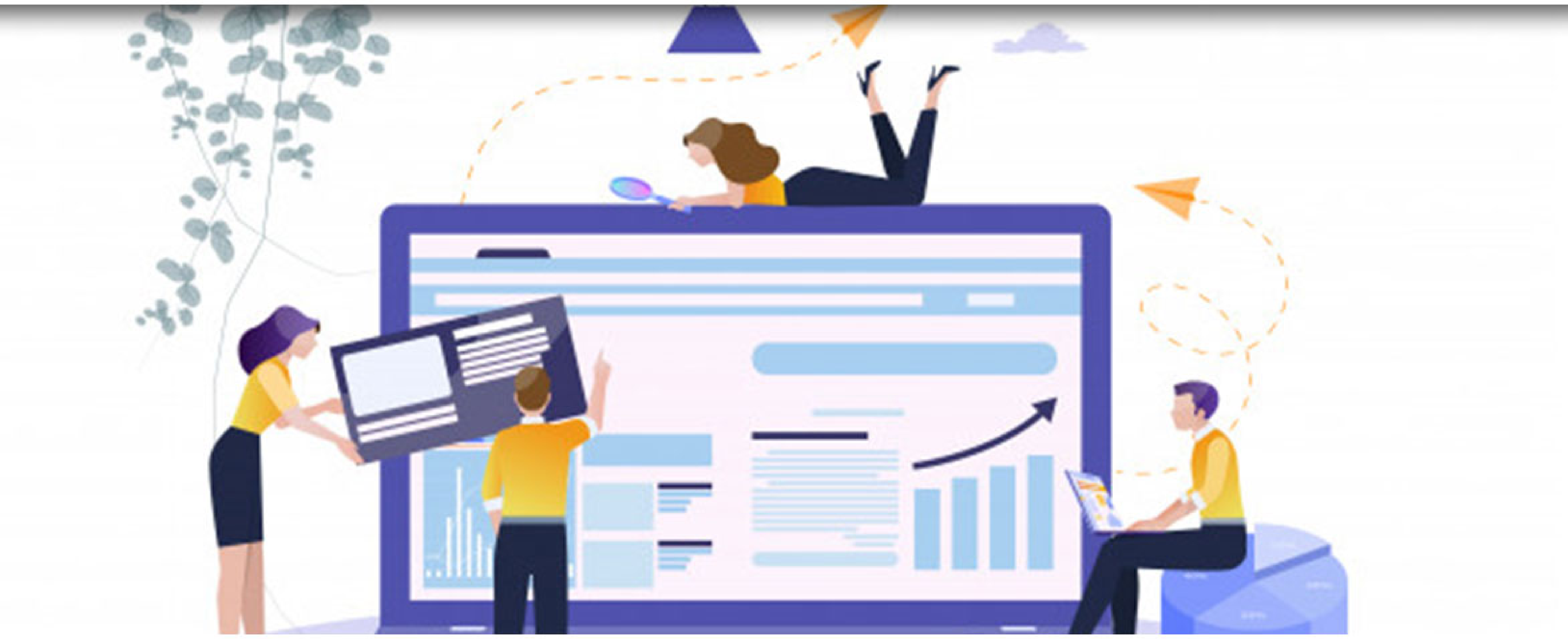
XcellManage

Managed Splunk Services

Secure Cloud Services for your online business since 1999.

.Reliable .Secure .Speed .Scalable .Manageable .Compliant

Powered By: splunk>



Managing & Developing Apps for Large-Scale Splunk Deployment

- Are you maximizing your Splunk investment?
- Are you getting real-time insights from Splunk ES?
- Are you finding it difficult to hire Splunk talent?

How XcellHost Can Help

- Security Automation with adaptive response
- Use case library to catch credible threats
- Assess, Architect, and Deploy
- Strengthen investigations
- Data onboarding, deploying apps
- Build custom dashboards with rich UI
- Improve Security

Benefits

- Performance & Health Monitoring & Response
- Management Of Forwarder Log Collectors
- SPLUNK Administration & Maintenance
- 24/7 SOC Monitoring & Alerting
- Migration Services
- Health check of Splunk clusters

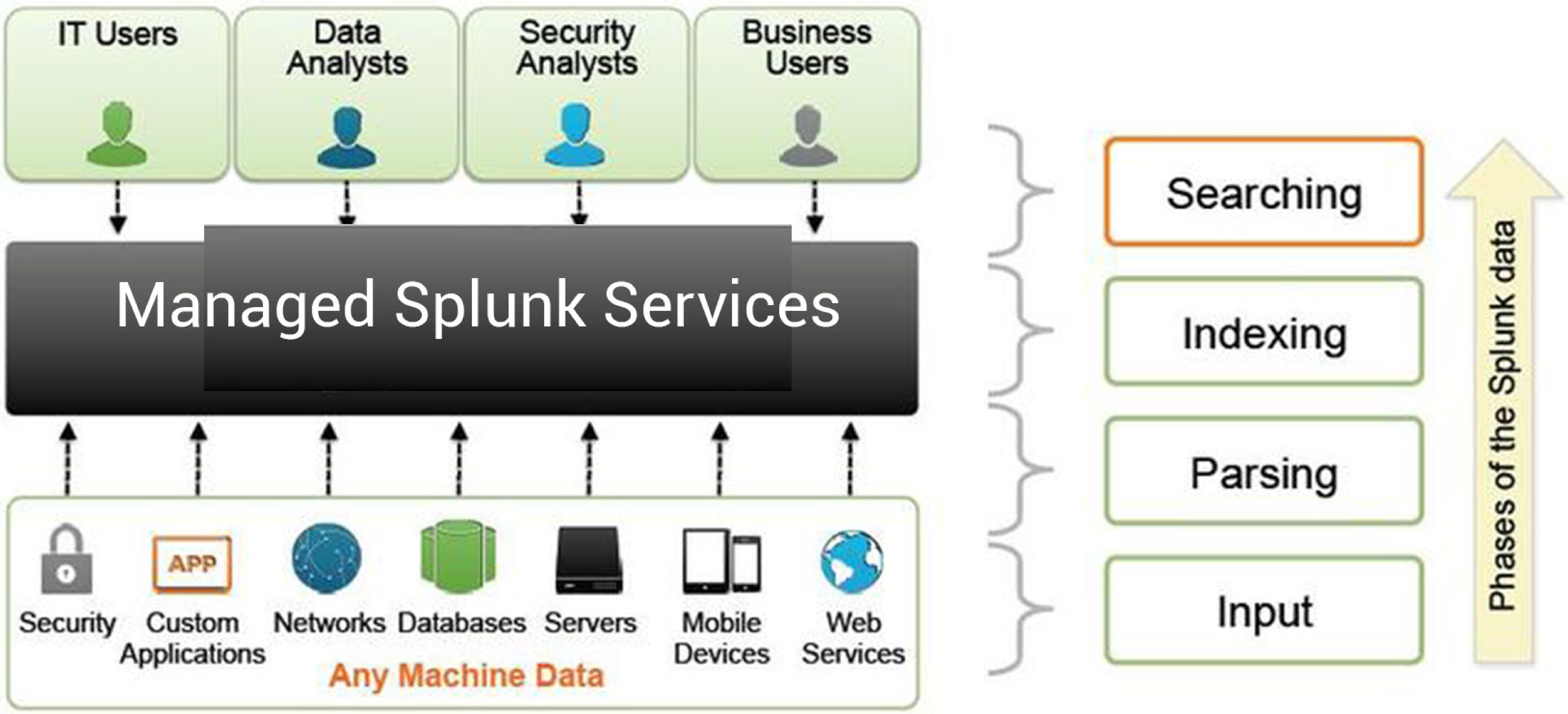
Learn More https://www.xcellhost.cloud/managedsplunk

sales@xcellhost.cloud www.xcellhost.cloud @xcellcloud +91-22-67111555

Unified Splunk Managed Services

Get More Out of Your Splunk

Managing Splunk For Enterprises To Get Real-Time Operational Intelligence Has Never Been Easier



IT Users

Data Analysts

Security Analysts

Business Users

Managed Splunk Services

Security

Custom Applications

Networks

Databases

Servers

Mobile Devices

Web Services

Any Machine Data

Searching

Indexing

Parsing

Input

Phases of the Splunk data

60%	Reduction in Admin costs
31%	Reduction in Splunk TCO
2	Average # of Days for Ticket Closure
20%	Reduction in Incoming Tickets

Expert Support All Day, Every Day

- 24/7 Live Chat
- Active Community
- Troubleshooting
- Up-To-Date Applications
- Strong Knowledge Base

Global Reach - Personal Touch

ISO/IEC 27001 Information Security Management

ISO/IEC 20000-1 Information Technology Service Management

ISO 9001 Quality Management

ISO 22301 Business Continuity Management

- INDIA
- DUBAI
- SINGAPORE

209, Laxmi Plaza, Bldg. No. 9
Laxmi Industrial Estate,
Andheri (W), Mumbai - 400053
MAHARASHTRA, INDIA

✉ sales@xcellhost.cloud

www.xcellhost.cloud

@xcellcloud

☎ +91-22-67111555