Any number of servers to scan, from one to hundreds of thousands

High frequency of checks, supported by horizontal scalability

Support for interaction between experts for speedy resolution of the detected problems

Easy integration with any existing monitoring systems deployed by the user

Continuous monitoring mode independent of the state of particular servers

Support for event escalation to comprehensive IT infrastructure monitoring systems

Flexible reaction to false positives, preventing an “avalanche” of alerts for events that were already verified

COMPLAUD helps you:

Detect software vulnerabilities

Verify compliance of configuration with security requirements

Implement custom checks on the existing platform based on client requirements

Create an inventory of software

Audit

Detection of software vulnerabilities

Compliance

Verification of software configuration security compliance

Inventory

Collection of information about the software that was installed on the monitored servers during a set time period. List of hardware and software, showing all changes in their state, similar to Audit and Compliance modes.

Management of false positives

Removal of an established false vulnerability from the audit results by permission of the security officer

Change tracking

Ticketing

Contact

Address:
127018, Russia, Moscow,
Polkovaya str., 3
Tel:
+7 (495) 009 87 87
+7 (800) 302 87 87
Email: info@rcntec.com

rcntec.com/en/complaud

COMPLAUD

An elastic distributed system for security status monitoring and IT infrastructure standards and settings compliance auditing

RCNTEC
Resilient Cloud and Network TEChnologies

COMPLAUD - monitoring information security, auditing standard compliance, tracking settings

COMPLAUD is:

Real-time information on compliance and vulnerabilities in your entire infrastructure

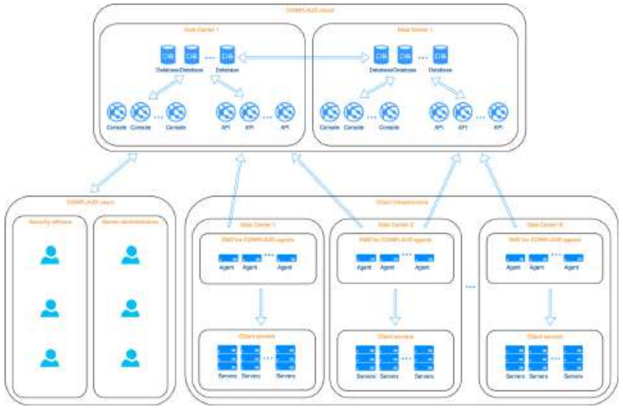
Assurance in passing any audit of security standards

No dependency on the “human factor” in providing information security

A unified console for information technology management and information security

Continuous auditing of all installed software

ARCHITECTURE DIAGRAM OF THE CLOUD



TECHNICAL FEATURES OF COMPLAUD

Horizontal scalability and resilience*

A comprehensive and fully documented API enables automated interaction with the system interface

Open source code for the agent and plugins ensures that the server audit process is transparent and customer-controlled

Use of the HTTPS protocol for agent-to-API interaction enables customization of agent code for a particular infrastructure or a particular customer

Escalation of the generated events through syslog and into the Slack corporate messenger helps ensure prompt reaction from information system administrators when a vulnerability or incompliance is detected

Integration with the Elasticsearch search engine enables storage and search of information covering all the detected vulnerabilities and cases of incompliance, as well as logs of system user actions

Web-based customization of compliance plugins enables flexible changes to the parameters that are monitored on the scanned hosts

Role-based access control helps organize interaction between security officers and information system administrators using Ticketing functionality

TECHNOLOGIES AND SOLUTIONS THAT ENABLE HORIZONTAL SCALABILITY AND RESILIENCE:

Cassandra, a decentralized NoSQL DBMS, ensures linear scalability and replication between any number of cluster nodes located across several data centers

Round-robin DNS enables load balancing between identical API nodes that process data sent from agents

Nginx, an asynchronous Web server, processes agent requests to the API. The amount and rate of requests can rise with practically no limits

FUNCTIONAL FEATURES

Constantly updated vulnerability audit based on over 14 thousand vendor security publications (Red Hat Enterprise Linux, CentOS, Ubuntu, Suse Linux Enterprise Server)

Security configuration compliance checking for Linux and MS Windows devices

Software inventory

SECURITY

Users and agents interact with the system using the encrypted HTTPS protocol

Confidential user data stored in the system is encrypted using the AES algorithm with a 256-bit key

MS Active Directory integration using the LDAP protocol ensures an approach to authentication and authorization procedures that is standard for corporate environments