WHITE PAPER

MAXIMIZE IT INVESTMENT WITH CLOUDREADY

SUMMARY

The digital landscape, market competition, and changing cloud computing models are forcing IT executives to rethink their strategy. Investments are being made in every corner of the infrastructure to manage applications, networks, and business services. However, this approach has left several monitoring tools obsolete, and as workloads are shifted from on-premises to a complex hybrid cloud environment, IT is losing control and visibility. A simpler and intelligent tool that integrates with existing systems and provides uninterrupted business service will boost investment in IT.

KEY INSIGHTS

- Monitor global infrastructure health and end-user digital experience consistently
- Unify existing toolset and achieve corporate resiliency through business service automation
- Integrate with ITSM and third-party application to streamline incident management
- Achieve enterprise objectives and value through an interlinked ecosystem of tools

exoprise

ADOPTION OF A UNIFIED IT MONITORING FRAMEWORK

Modern IT seeks ways to evolve by identifying new tools that will complement existing workflows and add functional value. This is not a rip-and-replace approach but rather an integrated way to build trust in the entire system. Major IT disruptions due to the rapid growth of cloud and hybrid computing models require data to be collected from multiple sources. Monitoring the effectiveness of SaaS services delivered though these emerging models is critical for optimal success and smoother business operations. Capturing real-time alarms from performance degrading systems in the entire infrastructure and sending notifications promptly to the service desk saves businesses a fortune.

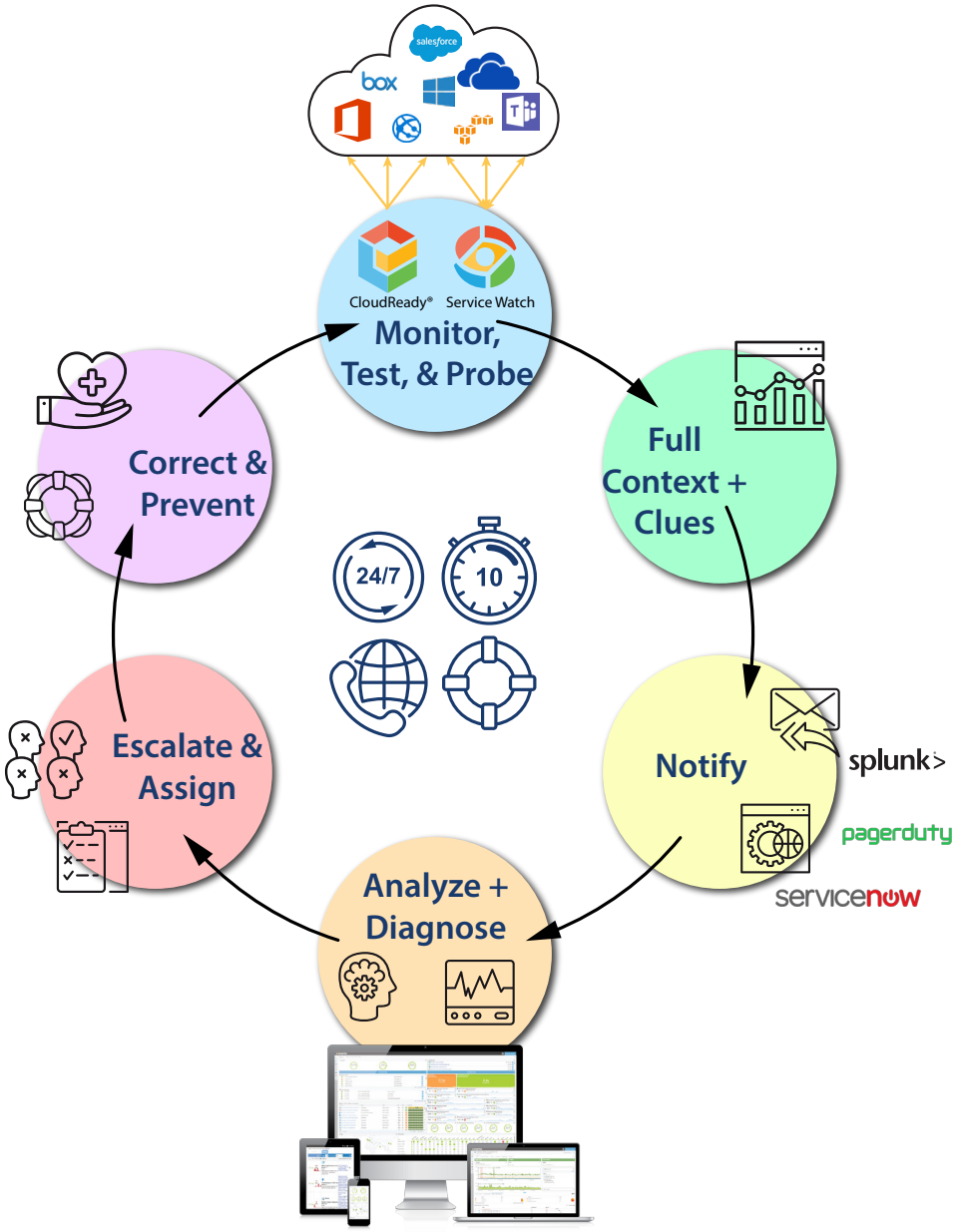


Figure 1. Incident Management With Exoprise CloudReady

In the current business environment, the demand for and adoption of new services by various in-house teams is increasing and IT is preparing for it more than ever. Recent data from Netskope Cloud Report 2019 shows that the **average company is using 1,295 cloud services** – a number that is growing year on year! In pursuit of monitoring all services and receiving instant notifications, the tools that IT executives propose and incorporate into their portfolio need be compatible. If implemented well, the new consolidated monitoring framework can deliver promising results. IT can improve administrative visibility of network and application performance and enhance the end-user experience. However, setting up a new monitoring tool requires time and no guarantee that it is compatible with today's hybrid cloud infrastructure. Therefore, ensure that your tool consolidation strategy allows for close and tight infrastructure integration in the long term.

Average company uses 1,2`95 cloud services and that number is growing each user.

2019 Netskope Cloud Report

CHALLENGES POSED BY EXISTING MONITORING PRACTICES

IT executives and managers often need to review their monitoring systems to justify their investment and ROI. The question that often gets asked is whether all the underlying low-level project metrics (audio and video quality, jitter, packet loss, round trip time, QoS, page layout, login, and connect time) are captured and if there is an optimal method for measuring end-user experience. Legacy monitoring systems are expensive to maintain and do not offer the convenience of scalability, reliability, or customization needed to meet the ever-changing needs of businesses.

- **Tool Incompatibility** – Before migrating the workload, it is better to evaluate all portfolio monitoring tools used by IT and see how they integrate with existing cloud solutions for data exchange. Tools developed today and, in the future, should easily integrate easily with cloud providers to allow for maximum flexibility and expandability.
- **Too Much Noise** – Monitoring tools can generate thousands of notifications each day that can amplify the noise and overwhelm IT teams. They may not have the resources and time to sift through alerts that may require immediate attention. Several problems like these become more acute when existing tools are departmental, and the complexity of modern data centers where computing, networking, and storage operations take place in separate silos.
- **Lack of Visibility** – Larger organizations have a heterogeneous environment with diverse applications, services, networks, containers, databases, virtual machines, DevOps, AIOps, hybrid cloud providers, and other myriad technologies. In addition, there is a need for monitoring security, identity, access control, user behavior, website reliability, devices, and log files. Once applications move to the cloud, it can obscure all endpoints in the service delivery chain, thus restricting visibility and control across the entire infrastructure.
- **Inability to Manage Incidents** – To accelerate troubleshooting and reduce MTTR, IT needs solutions that automate incident creation and populate details in the tickets. Business rules set in the ITSM can organize all incoming alarms based on their priority to give the system greater efficiency and reliability. However, existing monitoring tools are outdated and fail to capture all the alerts in

the first place. This can increase costs and overhead for any business if alarms go undetected.

- **Digital Transformation Roadblock** – Digital Transformation is the alignment of corporate culture to improve business processes by digitizing existing workflows and providing valuable services to customers. But achieving this goal and building a digital culture requires effort. The "Don't fix it if it isn't broken" mentality hinders the path to transformation and IT leaves behind monitoring tools that cease to add value after a certain period. According to Gartner research, organizational culture is the biggest drag on all digital transformation projects.
- **Automation Silos Slow IT** – As workloads shift from on-premises to the cloud, some tools can easily manage the centralization, orchestration, and automation of resources. Additional automated tools that help with CMDB population, network management, storage allocation, business intelligence, data analysis and so on all have a siloed purpose. This fragmented approach slows IT response time and increases complexity.

THE CLOUDREADY INTEGRATION APPROACH

Because of these limitations, companies need to find solutions that will make their migration and monitoring strategy work in the cloud. Exoprise CloudReady is a modern sophisticated tool that provides comprehensive coverage and end-to-end visibility of cloud applications such as Office 365, application and business services, and infrastructure components through synthetic and real user monitoring - all through a single SaaS platform.

CloudReady enables organizations with a unified automation framework that connects underlying infrastructure, shares data to maintain cross functionality, and drives business service value. IT teams can maximize their ITSM investments, simplify incident management and increase ROI by integrating with CloudReady. During an outage, CloudReady detects alerts quickly and sends notifications downstream to speed up the troubleshooting process, thus helping IT provide a greater customer experience.

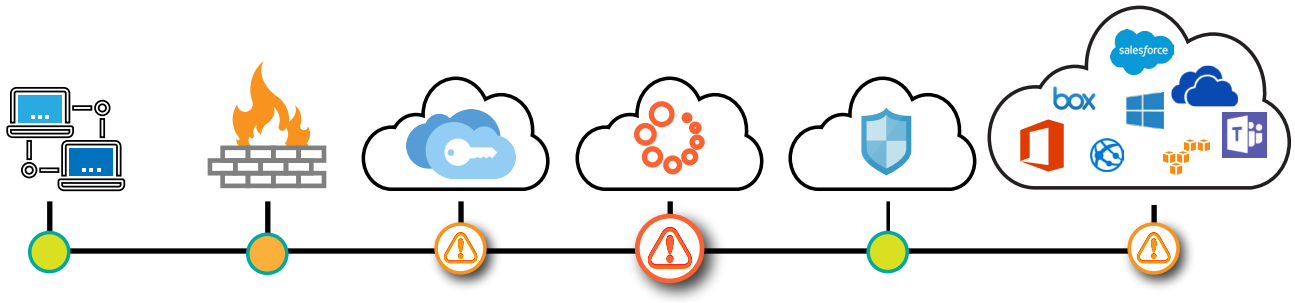


Figure 2. Business-critical Service Delivery Chain

Monitoring data from CloudReady supports existing IT processes and multiple operational workflows. By integrating data with other tools in an IT workflow, teams can easily get a complete overview of SaaS health and simplify data analysis. The

platform captures thousands of advanced metrics covering high-level actions such as the time it takes to send and receive an email, to low-level metrics such as Time-to-First-Byte (TTFB), Proxy Connect Time, AV Quality and DOM Loaded time.

4 WAYS TO SHARE CLOUDREADY ALARMS AND DIAGNOSTICS

1. Built-in Email and SMS Messages

   CloudReady offers email and SMS notifications by default which are included in the subscription price. They are also available for testing free of charge during the test phase. Once a sensor is created and deployed, alarms and thresholds are automatically configured for that sensor. For example, the most critical alarms are configured for a SharePoint sensor when you deploy SharePoint sensors in various locations. You can set new thresholds and adjust alarms according to sensitivity.

2. On-Premises Alarm Integration

   CloudReady has several ways to distribute alarms and alarm resolution to internal systems such as Splunk or Microsoft System Center Operations Manager (SCOM) for propagation and integration.

3. Private Sites

   Private sites are instances of a CloudReady agent running in a Windows Virtual Machine behind your firewall. Designate any private site to receive alarms for the CloudReady tenant. All relevant alarm data, with URLs and meta-data about the alarm and sensor, is written to an alarms.log file on the local system in JSON format. In addition, CloudReady alarm and resolution information in the Windows NT Event log can remain on a private site. In the event of an outage, prime site alarms can failover to other high availability sites.

   See Exoprise Online Help for a thorough example of Event Data and how to parse for integration: https://help.exoprise.com/kb/logging-nt-event-log-description/

Splunk Integration Example

Splunk can collect and index alarms from these logs to finally visualize them via charts and graphs and share with team members. When it comes to SCOM, CloudReady data can fed using the Operations Manager REST API. SCOM can collect this new data to create different types of charts and add to existing dashboards.

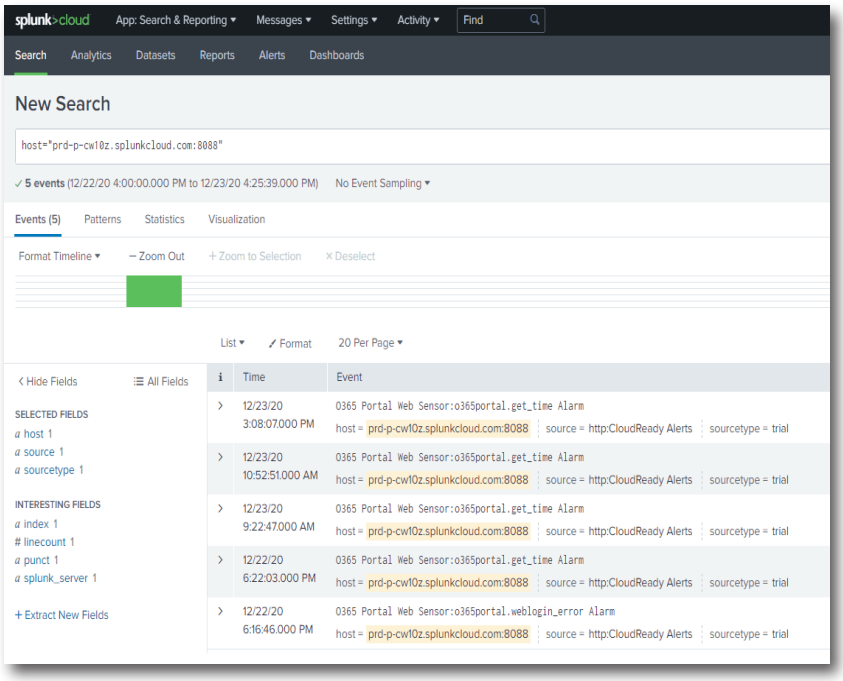
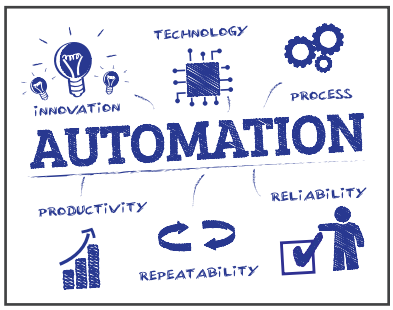


Figure 3. Splunk Example With Exoprise Alarm Integration

4. Hooks, Workflow, and Automation

CloudReady integrates with ITSM (ServiceNow and PagerDuty), AIOps/DevOps (Moogsoft), business communication (Slack), and SecOps (SumoLogic) tools to extend workflow automation in existing infrastructure. Downstream systems can capture alarms recorded by CloudReady and help IT gain unique insights into their environment.



Email Hooks

Although the built-in email messages may be sufficient, CloudReady also supports email hooks that allow for full customization of the template and formatting of the email message. Emails can be sent after the alarm is received, the alarm is resolved, or both. Email hooks are typically customized for automated email processing. IT operations professionals probably want the alarm plus specific information about its nature.

Web Hooks

Email hooks are a simple and effective way to notify people of alarms and issues but there are limitations on what you can do with the data and how you can insert it into an IT workflow. Applications with a defined API often allow you to certain JSON payload data to help IT with supplement information and decisions. A web hook sends an HTTPS post request to the tool you want or a RESTful URL of your choice with basic OAuth authorization.

Both email and web hooks allow property variables to determine what information is sent in the alarm and to recipients. Variables use the format $alarm.name$ to build a template.

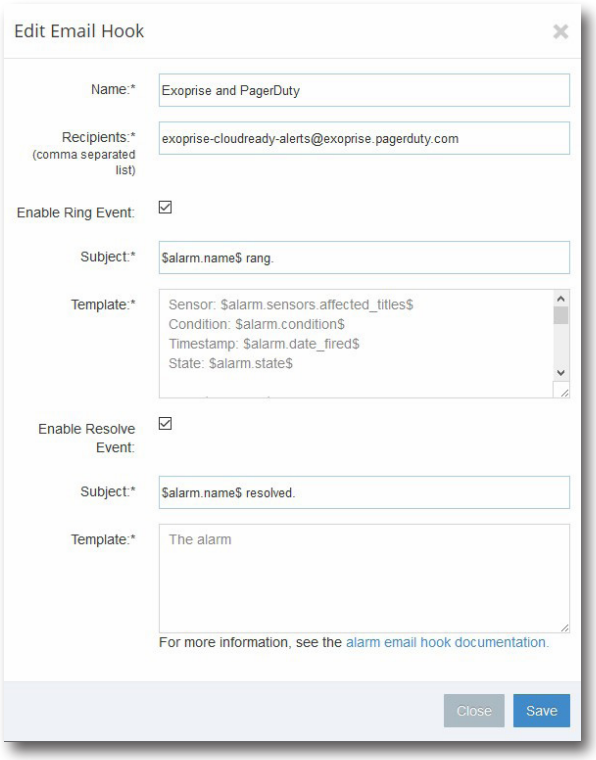


Figure 5. PagerDuty Integration Via Email Hook

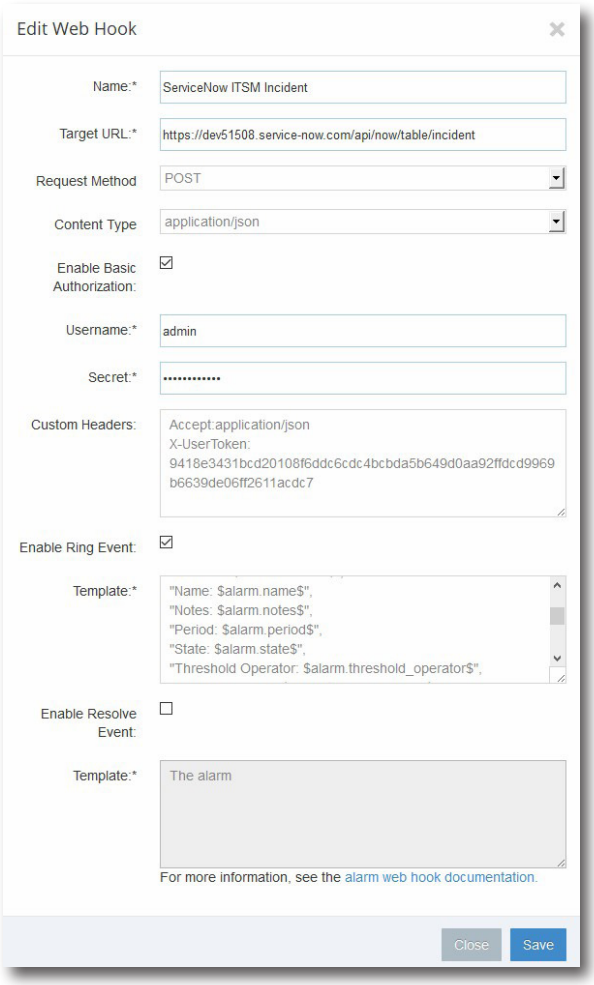


Figure 6. ServiceNow Webhook Example

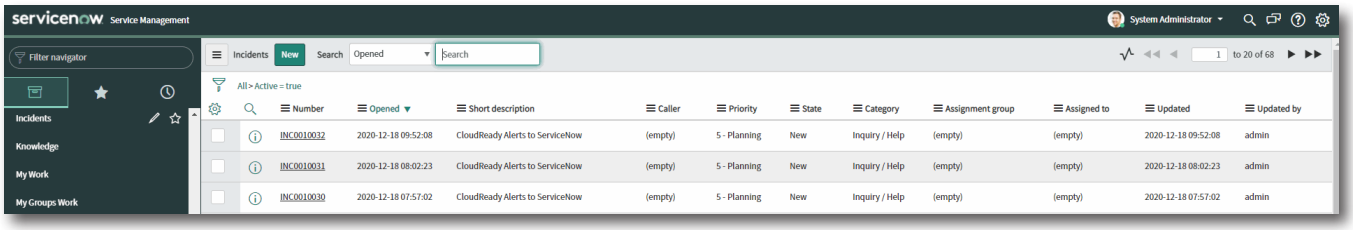


Figure 7. Example ServiceNow CloudReady Alarm Integration

5. Service API

   Connecting your CloudReady account directly to Office 365 via Microsoft's Service Communications API is easy. Like the Operations Manager REST API, the Office 365 Service Communications API is a REST service that lets you to develop solutions with any web language and hosting environment that supports HTTPS. You can access the Service Communications API, receive data, combine that data with CloudReady readings, and create custom graphics and dashboards that provide complete data on the state and trends of your enterprise-wide SaaS applications.

exoprise

260 Bear Hill Road
Suite 207
Waltham, MA 02451
1-855-EXO-PRISE
1-855-396-7747

www.exoprise.com
sales@exoprise.com

About Exoprise

Exoprise is the leader in Digital Experience Monitoring for SaaS, Cloud apps, and ALL of Microsoft 365. Our platform empowers businesses to see, diagnose, and optimize the applications and networks everyone relies on. We help organizations deliver optimal end-user experiences.