



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

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 through 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.

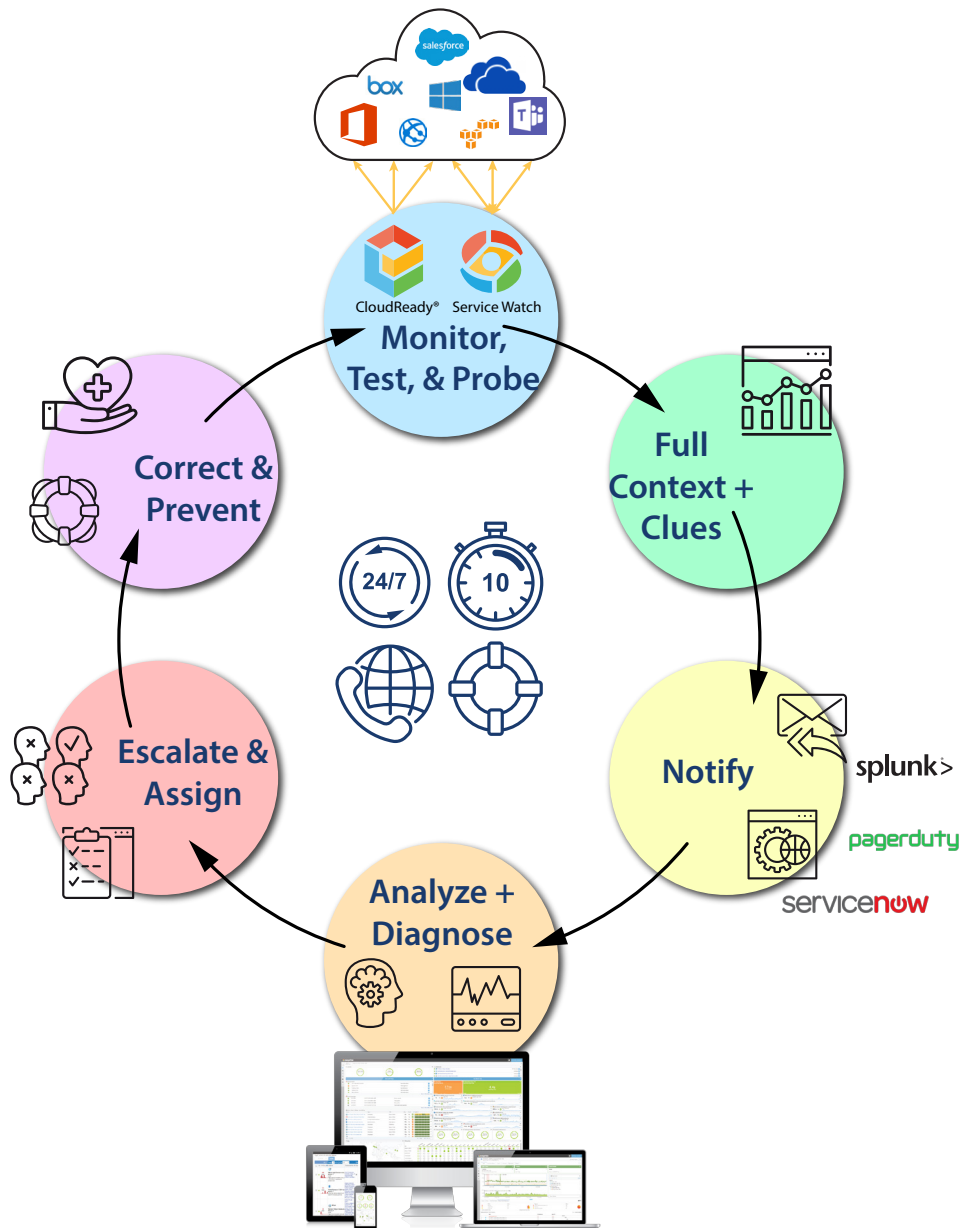


Figure 1. Incident Management With Exoprise CloudReady

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.

*Average company uses
1295 cloud services
and that number is
growing each year.*

[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 (e.g. A/V quality, jitter, packet loss, QoS, 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.
- **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.
- **Lack of Visibility** – Larger organizations have diverse applications, services, and networks. 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. 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** – The “Don’t fix it if it isn’t broken” mentality hinders digital transformations 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 EXOPRISE 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.

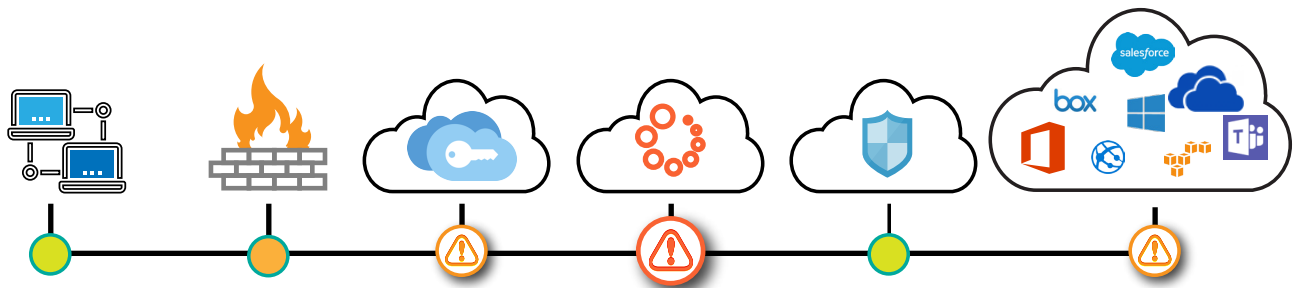


Figure 2. Business-critical Service Delivery Chain

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 Exoprise platform captures thousands of advanced metrics such as Time-to-First-Byte (TTFB), Proxy Connect Time, AV Quality and DOM Loaded time to assist in root cause analysis across disparate systems.

83% of respondents consider API integration a critical part of their business strategy, driven by digital transformation initiatives and cloud adoption

5 WAYS TO SHARE EXOPRISE ALARMS AND DIAGNOSTICS

1. Built-in Email and SMS Messages

Exoprise 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 SharePoint monitoring when you deploy SharePoint sensors in various locations. You can set new thresholds and adjust alarms according to sensitivity.

[Cloud Elements - State of API Integration Report \(400 integration professionals and IT executives\)](#)

2. On-Premises Alarm Integration

Exoprise has several ways to distribute alarms and resolutions 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 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](https://help.exoprise.com/kb/logging-nt-event-log-description/) for a thorough example of Event Data and how to parse for integration: <https://help.exoprise.com/kb/logging-nt-event-log-description/>

Microsoft SCOM 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, Exoprise data can be fed to SCOM using the Operations Manager REST API. SCOM can collect this new data to create different types of charts and add to existing dashboards.

Splunk Integration Example

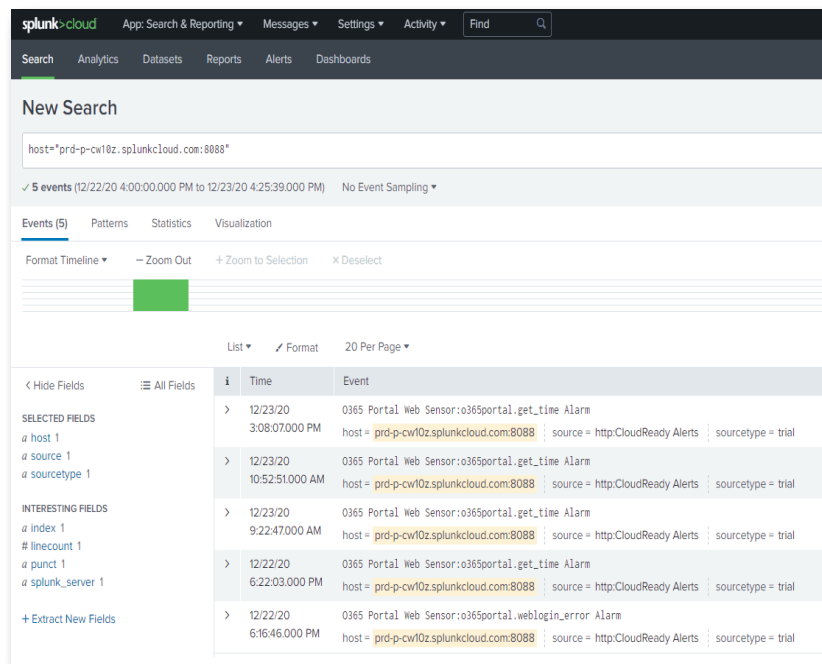


Figure 3. Splunk Example With Exoprise Alarm Integration

With Exoprise, Integration to our existing ITSM tools was incredibly easy. We use splunk extensively, and we hooked up Exoprise in 2 clicks. Now the ops team receives alerts whenever our SaaS services are having issues in the same way they do for everything else. That delivers Instant value with zero learning curve.

*Services Manager,
End User Services
Global Confectionary
Manufacturer*

4. Hooks, Workflow, and Automation

Exoprise can integrate with most notification and aggregate services. Any system that supports webhook or email notification such as 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 Exoprise 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 message. Email hooks are typically customized for automated email processing.

Web Hooks

Applications with a defined API often allow JSON or other data payloads to help IT with supplemental information and decisions. A web hook utilizes HTTPS post requests to any tool or RESTful URLs with any kind of authorizations.

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.

Edit Email Hook

Name: Exoprise and PagerDuty

Recipients: exoprise-cloudready-alerts@exoprise.pagerduty.com

Enable Ring Event: ☒

Subject: \$alarm.name\$ rang.

Template: Sensor: \$alarm.sensors.affected_titles\$, Condition: \$alarm.condition\$, Timestamp: \$alarm.date_fired\$, State: \$alarm.state\$

Enable Resolve Event: ☒

Subject: \$alarm.name\$ resolved.

Template: The alarm

For more information, see the [alarm email hook documentation](#).

Close Save

Figure 5. PagerDuty Integration Via Email Hook

Edit Web Hook

Name: TeamsHook - Exchange, SharePoint Outages

Target URL: https://xoprise.webhook.office.com/webhookb2/f1054a8a-3cd5-4b0e...

Request Method: POST

Content Type: application/json

Custom Headers: Customer-Header: Value

Enable Basic Authorization: ☐

Enable Ring Event: ☒

Message Body: { "title": "Alarm Fired", "text": "\$alarm.name\$", "sections": [] }

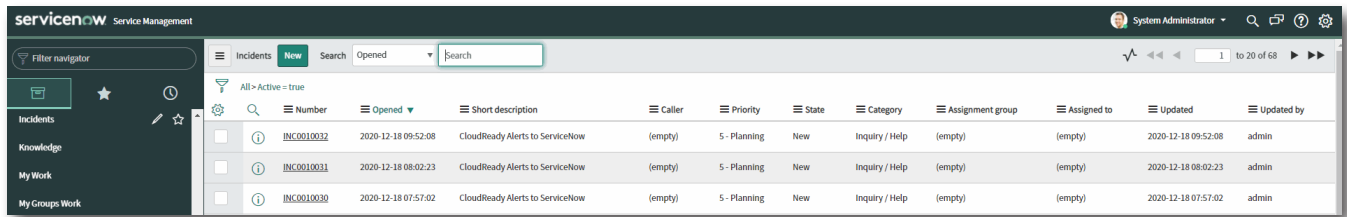
Enable Resolve Event: ☒

Message Body: { "text": " Name: \$alarm.name\$, Date Resolved: \$alarm.date_resolved\$, Aggregate: \$alarm.aggregate\$, Condition: \$alarm.condition\$ }

For more information, see the [alarm web hook documentation](#).

Close Save

Figure 6. Microsoft Teams Webhook Example



The screenshot shows the ServiceNow 'Incidents' list. The table contains three incidents, all with the category 'CloudReady Alerts to ServiceNow' and priority '5 - Planning'. The incidents are created by 'admin' on 2020-12-18.

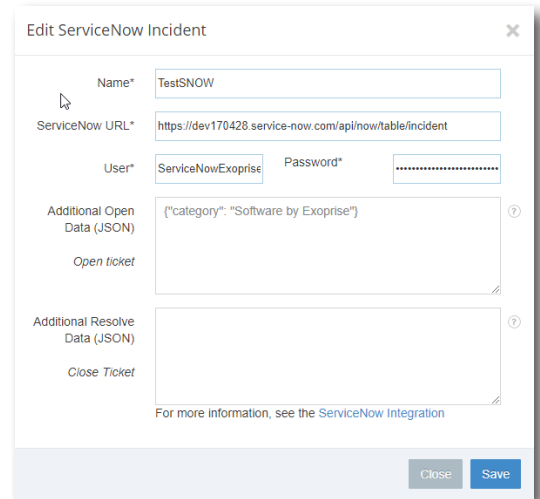
Incident Number	Opened	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated	Updated by
INC0010012	2020-12-18 09:52:08	CloudReady Alerts to ServiceNow	(empty)	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2020-12-18 09:52:08	admin
INC0010011	2020-12-18 08:02:23	CloudReady Alerts to ServiceNow	(empty)	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2020-12-18 08:02:23	admin
INC0010030	2020-12-18 07:57:02	CloudReady Alerts to ServiceNow	(empty)	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2020-12-18 07:57:02	admin

Figure 7. Example ServiceNow Alarm Integration

5. ServiceNow Incident, Ticket Automation with Exoprise

Exoprise recently enhanced its integration with ServiceNow enabling customers to automatically open and resolve incidents within the ServiceNow console. This was a frequently requested feature and gives IT teams unprecedented insight into network degradations and outages for every user and location. Collaborate with network and support teams via ServiceNow tickets and Exoprise to quickly resolve issues and get the business back online no matter where employees work.

Here is an example screenshot from the Exoprise ServiceNow Incident creation call. All that's required is your ServiceNow tenant URL and an account with access to create and resolve incidents. Exoprise automatically populates required fields with the right information to give personnel actionable insight into the context for an outage or problem.



The screenshot shows the 'Edit ServiceNow Incident' form. The 'Name' field is populated with 'TestSNOW'. The 'ServiceNow URL' field contains the API endpoint. The 'User' field is 'ServiceNowExoprise' and the 'Password' field is masked. The 'Additional Open Data (JSON)' field contains the JSON object: {"category": "Software by Exoprise"}. The 'Open ticket' button is visible. The 'Additional Resolve Data (JSON)' field is empty, and the 'Close Ticket' button is visible. A link to 'ServiceNow Integration' is provided at the bottom.

Figure 7. ServiceNow Incident Creation

INTEGRATION MATTERS

Enterprises are growing and maturing. And with more maturity comes the usage of sophisticated technology that businesses adopt over time. Several monitoring tools available today in IT are pure play either meant for incident management, AIOps, business communications, SMS alerting or log monitoring. No one tool does everything and most organizations use them just to complete the monitoring picture. Furthermore, these tools are meant for different teams and which ultimately creates silos. The rapid shift in SaaS application delivery from on-premises to the cloud has added more complexity to the overall monitoring strategy. New areas beyond the reach and control of IT have emerged that continue to be difficult and challenging to monitor.

Against this backdrop, companies need to rethink their IT game plan to derive more value from existing infrastructure. Effective and reliable monitoring solutions that increase internal efficiency and drive business growth are becoming a necessity. Investment in a SaaS monitoring tool that provides deep end-to-end visibility, easy integration with tools such as ServiceNow and sends instant notifications to anyone in the event of outages is required. Exoprise is just that solution.



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.