everbridge®

WHITE PAPER

Stop Alert Floods & Get Work Done

A SELF-SERVICE APPROACH TO EVENT SUPPRESSION

xmatters
AN EVERBRIDGE COMPANY

HOW TO READ THIS WHITE PAPER

We wrote this paper to address the effect that event storms can have on IT departments. We asked Charles Araujo, Principal Analyst at Intellyx, to objectively establish the current state of alert storms and how IT organizations are struggling to work through incidents in the face of overwhelming alert volumes. We also wanted to explain how xMatters addresses this pain now, and how it will improve in the future. xMatters Signal Intelligence correlates alerts and suppresses up to 90% of duplicate notifications so IT teams can do their jobs without constant interference.

In short, read the first half of this paper for an explanation of alert floods and event storms. Read the second half to learn xMatters' unique approach to blocking redundant alerts so IT teams can focus on fixing issues fast.

The Storm Before the Storm

Why Alert Suppression is Now Critical

Every IT operations team is familiar with the flood of alerts that a single issue can cause in today's highly integrated technology stacks.

The industry refers to this phenomenon as an alert storm, and it's starting to become a significant problem for IT organizations.

Alert storms act as a sort of Denial of Service (DOS) attack on an IT operations team. As the alerts come pouring in, they overwhelm a team's ability to sort through them and find the real issues amid the flood of duplicate entries and false positives.

Alert storms are most likely to occur during a significant operational impact, which inevitably also involves a large number of responders. As alerts and notifications fly, the alert storm makes it harder for the IT organization to sort out what is happening and respond — at precisely the moment that such a response is business-critical.

While alert storms are not new, the growing complexity of the IT stack is causing them to grow in both frequency and intensity. At the same time, the nature of operational support is transforming as organizations adopt agile, DevOps, and other more iterative development and deployment approaches. These two trends are creating the perfect storm in which alert storms now threaten the operational viability of the IT organization.

A Tapestry of Technology

Part of the reason that alert storms are becoming more problematic is that the technology stack has grown increasingly complex over the years.

More troublesome than this raw complexity, however, is that as issues cascade through this interconnected network of applications, different systems often manifest issues in unpredictable ways. This unpredictability causes systems to generate false positive alerts — often leading operations teams on the proverbial wild goose hunt.

The great irony is that the very alert management solutions that IT put in place to help ensure that they could monitor and manage these increasingly complex environments and optimize operational performance are now working against them. These resulting storms are making it nearly impossible for IT to manage through all the static.

Agile and DevOps Change the Rules

At the same time that the complexity of the stack was growing, another trend was taking root within IT organizations that would further amplify the impact of alert storms: the adoption of iterative development and deployment approaches.

These iterative approaches include things like agile development, the DevOps movement, and the use of continuous integration/continuous delivery methods. Before their adoption, there was a fairly clear demarcation between development and operations teams — development developed and operations operated.

In this previous era, therefore, when an alert storm emerged, its impact was mostly limited to the operations team — and they could just hunker down and weather the storm. In the era of agile and DevOps, things are not so simple.

Today's iterative development approaches have all but eliminated the line between dev and ops. As organizations begin to deploy code continuously, the line between when an application is 'in development' and when it is 'in operation' has become fuzzy. As a result, operations is now everyone's job. This new reality means that everyone is on the notification list when things go wrong.

A Rising Tide Sinks All Boats

The fact that an application is now simultaneously in development and in operation means that the impact of an alert storm is exponentially greater.

Now when alert storms strike, they no longer impact just the operations team. As these events occur, the alerts not only cascade and multiply across systems — resulting in alert storms — but those alert storms now cascade across operational systems and impact the work of nearly everyone in IT.

Developers, who were once blithely unaware that an alert storm was happening, now find themselves inundated with alerts and notifications. And, as organizations have sought to embed these types of notifications and alerts into the native development workflow, alert storms have now become disruptive to the development process and are on the verge of becoming debilitating.

Like a rapidly rising tide, these floods of alerts, and the notifications they create, wreak havoc across the whole of IT and, left unchecked, will undermine IT's ability to scale and adapt for the future.

The Intellyx Take

Alert Suppression Everywhere

For enterprise leaders, the situation has reached a critical state. The good news is that the solution is clear: organizations must suppress irrelevant alerts. Of course, that simple solution is not quite as easy as it sounds.

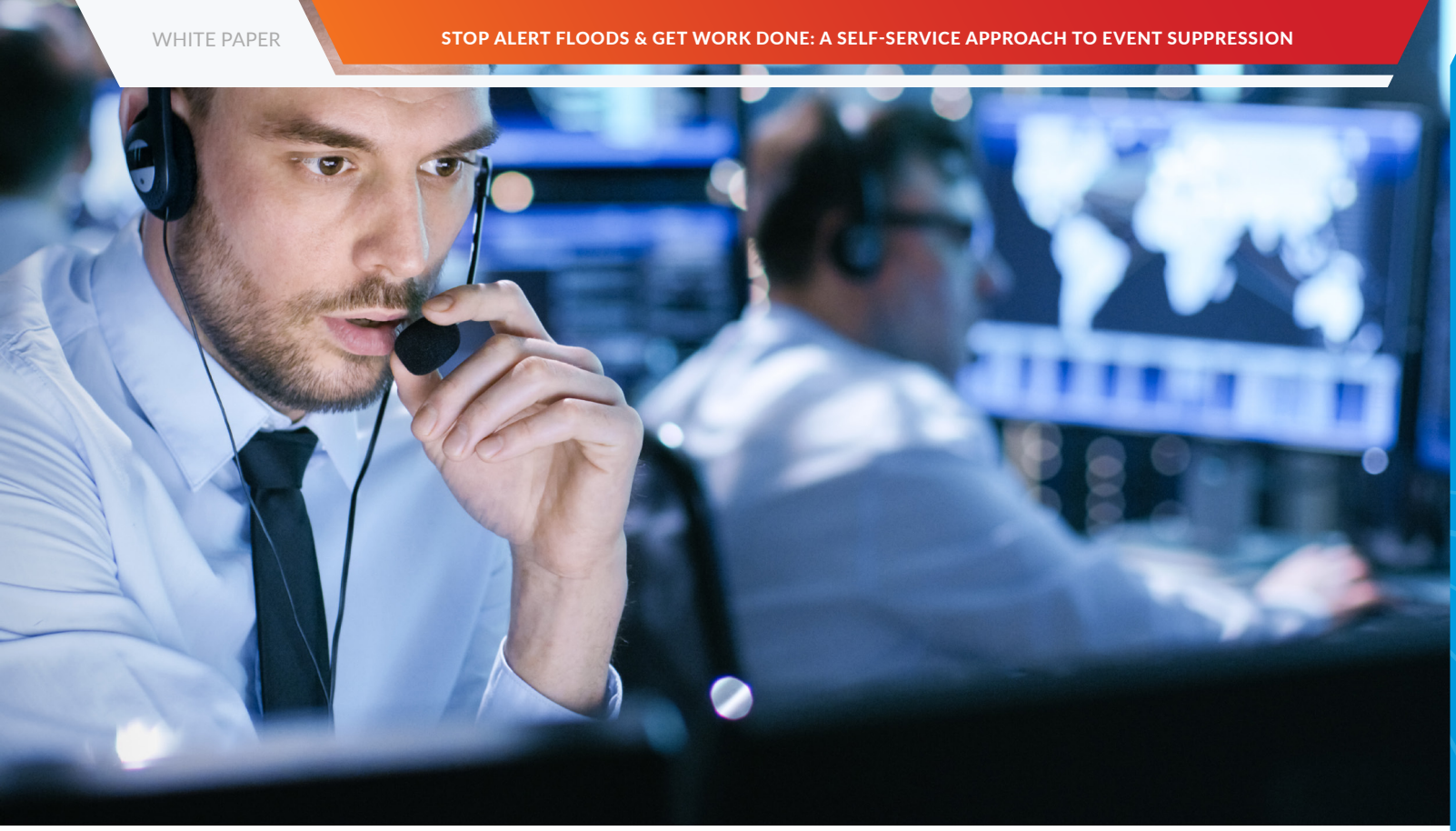
The reality is that most enterprises have numerous operational platforms that both create and consume alerts — and that's not likely to change any time soon. Even for those organizations that have invested in a tool that was explicitly designed to manage alert storms, the reality is that it is the rare (non-existent, really) organization that has been able to successfully consolidate everything into one place.

Enterprise reality is much messier. As a result, every system that is used to capture alerts, issue notifications, or kick-off operational automation must now incorporate a degree of alert suppression in the solution.

Depending on the situation, suppression may come from machine learning algorithms, rules-based engines, or any other number of approaches. What is vital, however, is that alert suppression must now be an essential element of every operational management tool — and organizations must employ it everywhere if they want to have any hope of surviving this perfect storm.

ABOUT THE AUTHOR

Charles Araujo is an industry analyst, internationally recognized authority on the Digital Enterprise and author of The Quantum Age of IT: Why Everything You Know About IT is About to Change. He is a Principal Analyst with Intellyx, the first and only industry analyst firm focused on agile digital transformation. He has authored three books and published over 100 articles. He is a regular contributor to CIO.com and has been quoted or published in Time, InformationWeek, CIO Insight, NetworkWorld, CIO & Leader, IT Business Edge, TechRepublic, Computerworld, USA Today, and Forbes.



The xMatters Way

Event Suppression Leads to Better Results

When an IT event occurs, notifications from a single integration can create a flood that overwhelms users. When you limit notifications, you build a cascading series of good results for your organization.

The main benefit being that IT incident resolution teams can respond earlier. Earlier responses prevent major incidents. Teams use the extra time to mitigate events more effectively. IT organizations use the extra time to turn their attention from firefighting to innovating, building new features, and making customers happy.

xMatters already has two ways to limit over-notification that can prevent your teams from working issues effectively.

Notification flood control prevents over-notification from the same integration during an event.

Subscription de-duplication dynamically sends you the best content based on your role in the communication process and suppresses any duplicate subscription notifications.

Introducing Intelligent Event Management

With intelligent event management, xMatters introduces event flood control. Event flood control correlates alerts from an event and suppresses them when the volume of similar events exceeds the default threshold.

When an event occurs, if you're on call or have a subscription to the alert source, you receive an alert. It may be a text, a push notification, a phone call, or any combination. Each time an integration – say between monitoring and the service desk or between the service desk and a ChatOps tool – is activated, another alert goes off.

As groups triage an event to determine the cause and how to fix it, and produce regular updates, it's easy to see how the combination of all these notifications can blow up your phone pretty fast. xMatters counts notifications across events and within events.

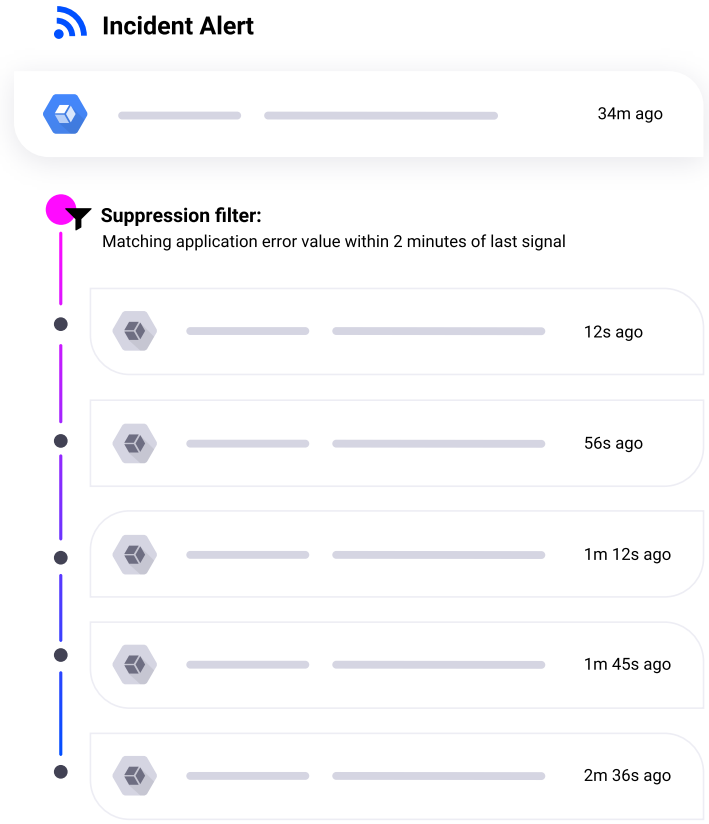
You get one alert. You get another. You get a third. If the fourth alert comes in within a minute, xMatters correlates it with the other three and informs you that you have an alert storm or an event flood. It suppresses subsequent alerts from the same integrations until the storm has passed.

How It Works

Based on actual customer event flood data, the xMatters default Event Rate Filter for inbound integrations is 4 events per minute for events from the same integration to the same targeted recipients. This provides effective protection against sudden surges of duplicate alerts from events while allowing real event traffic to proceed as normal. The suppression remains in effect until the incoming rate of event requests drops below 4 per minute again.

When the volume of alerts triggers flood control, the targeted recipients receive a single notification from xMatters instead of a flood of event notifications, and periodic updates while the flood is ongoing.

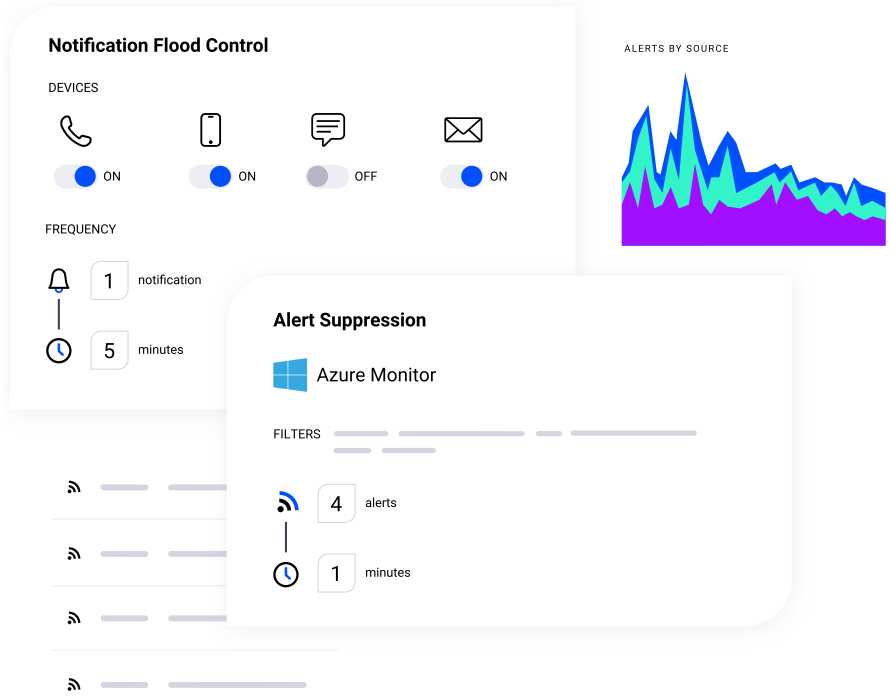
When a flood is detected, the initial notification explains that there is an alert storm, shows that alerts are being suppressed for an event, and describes the process going forward.



As long as the flood continues to meet the conditions of the Event Rate Filter, xMatters will send an updated version of this notification every 15 minutes, or for every 1,000 suppressed events, whichever occurs first.

Event flood control has been found to reduce events **90%** or more at Fortune **500** customers.

We've also updated our Recent Events report to see the details of the flood.



Once suppression kicks in, any additional requests that meet the conditions of the Event Rate Filter are suppressed beneath the event that triggered the filter. A suppression icon indicates that suppression has occurred for this event, and the stacked icon with a running badge count indicates the number of suppressed requests. Click the stacked icon to see more information in the Suppression report.

Usually, stakeholders who are not directly involved in resolving an incident still want to know when event floods are happening in your system. If this is you, you can create a subscription to get notified when a flood occurs and is ongoing. You can even subscribe to communication plans and integrations, and select the device types that you'd like to receive notifications on.

xMatters integrates with hundreds of third-party applications, including major AIOps players like Moogsoft and Big Panda, to pinpoint issues, automatically engage the right team members to drive resolution, and help customers identify issues and block redundant noise. xMatters has found that event flood control reduces events by 90% or more at Fortune 500 customers.

Details in the Suppression Report

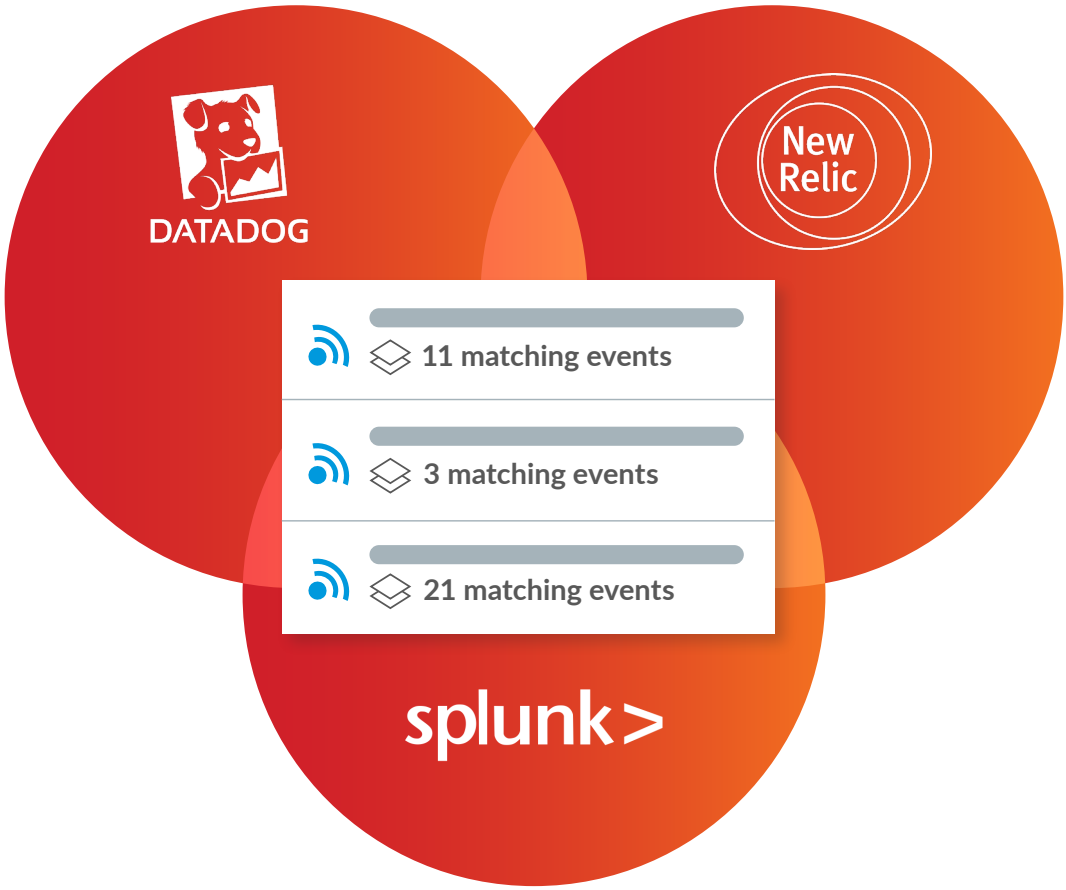
The event report includes a Suppression tab that provides detailed information about the requests that were correlated with it. This Suppression report includes the date and time of the:

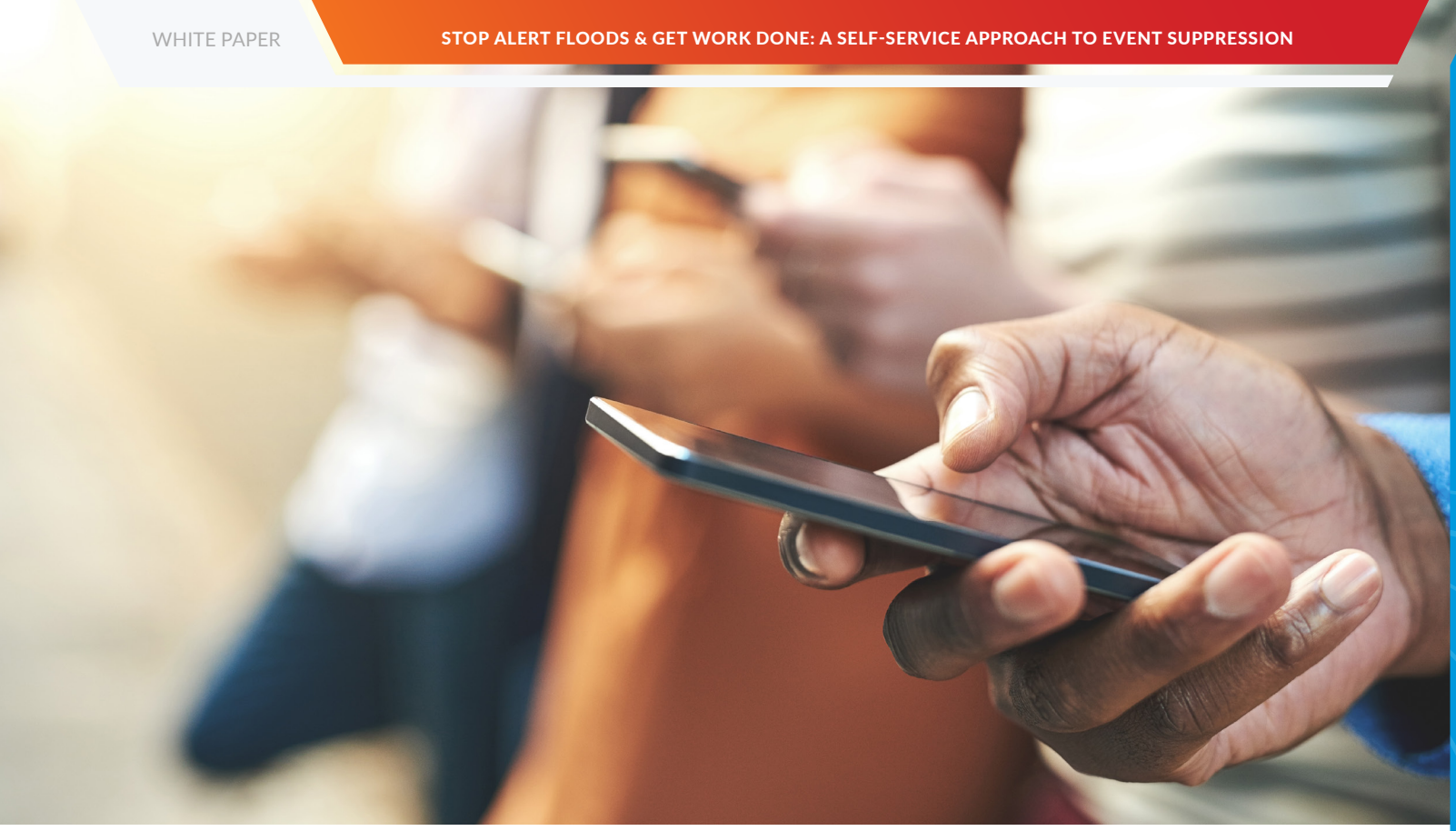
+ First suppressed event (when the flood was detected)
+ Most recently suppressed request

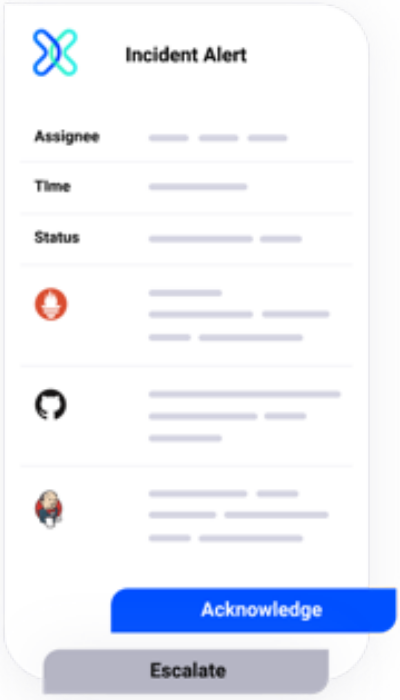
For each request it gives the following:

+ When the request was suppressed
+ The name of the flood control filter that applied to the request
+ The values of the event properties that match the filter (in the sample shown below, “Integration” and “Targeted Recipients”)
+ The priority of the request
+ The initiator of the request
+ A column for each event property and its value

Use the xMatters REST API to retrieve data about events with a “SUPPRESSED” status.







Event Flood Control in the Real World

Beta tests have put event flood control to the test, and the effects are dramatic. Review the results from two actual trial use cases.

In the first customer example, an integration targeted the same group 1,492 times in 1 hour 19 minutes. The default filters reduced the number of events to just 34. In other words, from 19 events per minute to one event every 2.3 minutes.

In the second customer example, the flood of alerts creates a 4.7-hour wait time for new notifications. That is potentially a catastrophic result. With event flood control, the number of events is reduced to produce no wait time at all.

Without Flood Control	With Flood Control
Example 1	
1,492 Alerts to the Same Group	**34** Events to the Same Group
4,412 Total Events	**1,037** Total Events
3.5 Hours Delay	**No Queue** or Delay
Example 2	
4,232 Alerts to the Same Group	**282** Events to the Same Group
5,835 Total Events	**828** Total Events
4.7 Hours Delay	**No Queue** or Delay

Sneak Peak

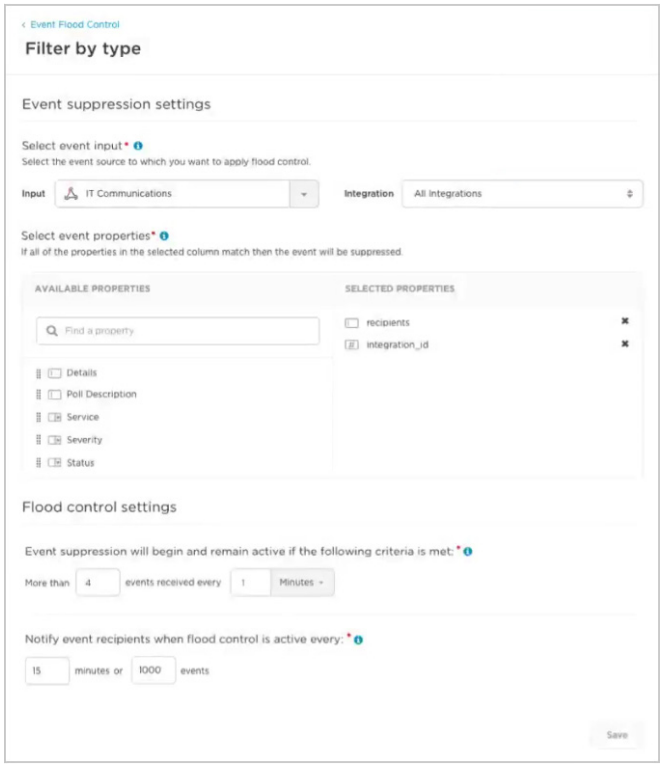
Customized Event Flood Control Settings

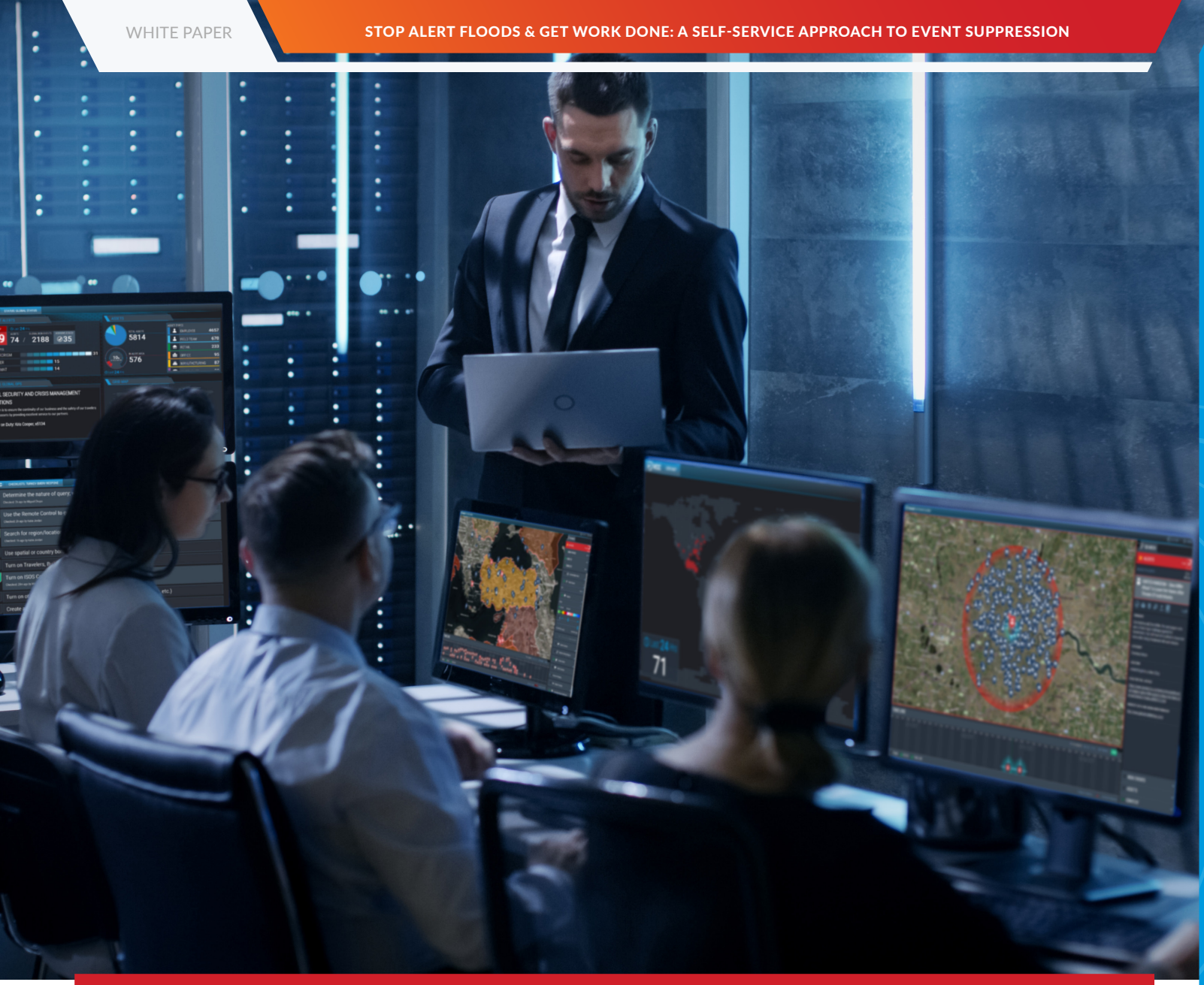
If default predefined filters don't meet your needs, help is on the way. In March 2019, xMatters introduced custom self-service filters.

Maybe you'd like to do more granular filtering and suppression, such as by alert type (e.g., network issues) or sub-subsystem (e.g., be able to differentiate between the Nagios and Zenoss alerts that are being fed into your Moogsoft monitoring system). Or perhaps you'd like to define different flood threshold parameters, such as >10 'high' priority events every 3 minutes from a specific communication plan (a communication plan is an integration flow).

You'll be happy to know that xMatters delivers customizable event flood control settings that allow you to define your own flood control rules. You will be able to determine:

- Which communication plan or integration you want the filter to apply to
- Which event properties you'd like to compare to determine if it's a duplicate event
- The rate you consider a flood, which is a rolling window of the number of events per time period (current default is 4 in a minute)
- How often to remind recipients that an event flood is occurring (current default is every 15 minutes)





Conclusion

Tool proliferation has become a double-edged sword for the agile enterprise. As DevOps teams increase their adoption of useful apps to accelerate software development and delivery, this added complexity can exacerbate the challenges of incident management. Teams may be overwhelmed by hundreds of digital events within minutes of an issue, preventing them from focusing exclusively on resolution.

xMatters Signal Intelligence blocks redundant alerts so teams can focus on fixing issues fast. By intelligently correlating events, xMatters successfully reduces noise surrounding major incidents and proactive response toolchains by 90% or more. That's a lot of noise, interruptions, and distractions that teams no longer have to deal with.

Don't get caught in the storm. Sign up for a free instance to try xMatters today or book a demo to learn more.

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order to Keep People Safe and Businesses Running™. During public safety threats such as active shooter situations, terrorist attacks or severe weather conditions, as well as critical business events including IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, over 5,400 global customers rely on the Company's Critical Event Management Platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes through the secure delivery to over 100 different communication devices, and track progress on executing response plans. Everbridge serves 8 of the 10 largest U.S. cities, 9 of the 10 largest U.S.-based investment banks, 47 of the 50 busiest North American airports, 9 of the 10 largest global consulting firms, 8 of the 10 largest global automakers, 9 of the 10 largest U.S.-based health care providers, and 7 of the 10 largest technology companies in the world. Everbridge is based in Boston with additional offices in 20 cities around the globe. For more information visit www.everbridge.com

About xMatters

xMatters an Everbridge company is a service reliability platform that helps DevOps, SREs, and operations teams automate workflows, ensure infrastructure and applications are always working, and rapidly deliver products at scale. Our code-free workflow builder, adaptive approach to incident management, and real-time performance analytics all support a single goal: the happiness of your customers.

VISIT WWW.EVERBRIDGE.COM
CALL +1-818-230-9700