BlackBerry
Intelligent Security. Everywhere.

White Paper

Responding Smarter, Faster and Better

BlackBerry Alert

How critical event management enhances cyber incident recovery

The Move is on to Centralized, End-to-end Solutions

The demands on security leaders are the most intense they've been in recent history. Increasingly intricate systems, the accelerating shift to the cloud, the shift to remote work, and more sophisticated external threats have created the perfect storm.

Responding effectively to major incidents now requires more than human expertise, diligence, and manual processes. When systems are compromised or shut down and vital business data is unavailable, every second lost can have costly and far-reaching effects.

Beyond rare global emergencies like the COVID-19 pandemic – which sparked a 35% rise in cyber attack volume, according to Microsoft – security leaders constantly confront severe incidents:[1]

- Cybersecurity threats are relentless, evolving, and inevitable – even for the most skilled and experienced security teams
- Other frequent disruptions include outages, critical vulnerabilities, software updates and new releases, and human error

The traditional, compartmentalized incident response approach used in most security operations isn't working anymore. Many organizations are using security information and event management (SIEM) solutions, often in combination with other tools that offer incident management.

With multiple systems from multiple vendors in place and little to no integration, communication silos and inefficiencies are inevitable. It's no wonder companies are struggling to respond effectively to major security incidents.

What is a critical event?

In cybersecurity, a *critical event* is a major incident that's disruptive enough to pose a meaningful risk or threat to your organization and its assets, including:

- IT assets
- Personal/company data
- Supply chain
- Machinery and equipment
- Buildings, facilities, branches, retail stores
- Product inventory
- People (employees, partners, customers)
- Brand/reputation
- Customer loyalty/relationships

4 Reasons Current Cyber Incident Response Tools aren't up to the Challenge

Traditional cyber incident response tools and processes have multiple limitations, including:

1. Poor collaboration	Security teams tend to be dispersed and even global, which complicates incident response. Then there are the relevant teams outside of security (senior leaders, developers, and external partners and customers) that struggle to stay in the loop.
2. A "noisy" alerting environment	Security teams can easily be overwhelmed by a regular barrage of blanket alerts. If alert fatigue sets in, crucial messages may be ignored.
3. Inefficient manual methods	Manual processes, workflows, and escalation are time- and labor-intensive. They can also inhibit data collection and tracking.
4. Inaccurate or incomplete contact information	Incomplete, outdated contact information for internal and external stakeholders is a common flaw in cyber incident alerting systems. Even if it's correct, it can be hard to access.

1.Microsoft

Critical Event Management for Cyber Incident Response

Security leaders are leaving behind disjointed incident response approaches. They're looking for one-stop, end-to-end solutions that provide:

- Access to real-time, aggregated threat data to reduce Mean Time to Detect (MTTD)
- Tools with rapid, automated communication and collaboration to reduce Mean Time to Repair (MTTR)
- The ability to maintain a full audit trail for future process improvements and accountability
- Vendors with broad expertise and capabilities that can consolidate technology beyond incident response (connecting cybersecurity consulting, AI-based endpoint protection, and more)
- An intuitive user experience for operators and end-users

Instead of adding an extra layer of complexity with a separate tool, the right critical event management (CEM) platform can unify and augment your existing incident response tools with the latest technology.

According to Gartner, two of the top recent security trends are centralizing data from multiple security products to improve threat detection and response, and automating repetitive security processes to increase accuracy and productivity. An advanced CEM solution does both, enabling faster, more informed incident response with:[2]

- Situational monitoring of business systems
- Early threat detection
- Automated incident response
- Simplified, real-time targeted or mass notifications
- Enhanced post-incident analysis

A cutting-edge CEM platform is designed to align with today's realities, including a dispersed, mobile workforce, more frequent and severe cybersecurity incidents, and the explosion of available data.

2.Gartner report

6 Benefits of Shifting to CEM

CEM allows security teams to collaborate quickly and easily with stakeholders inside and outside the organization – from initiating real-time chats on a central platform to sharing encrypted information.

Beyond faster, simpler communication, the most effective CEM platforms unify and streamline the management of cyber incidents with key capabilities like these:

1. Centralized and coordinated planning

- Breaks down silos between security teams (and external teams part of the incident management team) to consolidate incident response plans in one easy-to-find place
- Supports response plan management, review, revision, and awareness
- Delivers instant updates when response plans change
- Allows live adjustment to any response plan

2. Early threat detection

- Allows situational monitoring of business systems in real-time
- Receives threat feeds for earlier warning of incidents to enable faster, data-driven responses and quicker resolution
- Aggregates huge volumes of data from multiple sources (including government, media, social media, weather services, and more) and extracts relevant intelligence to assess risk

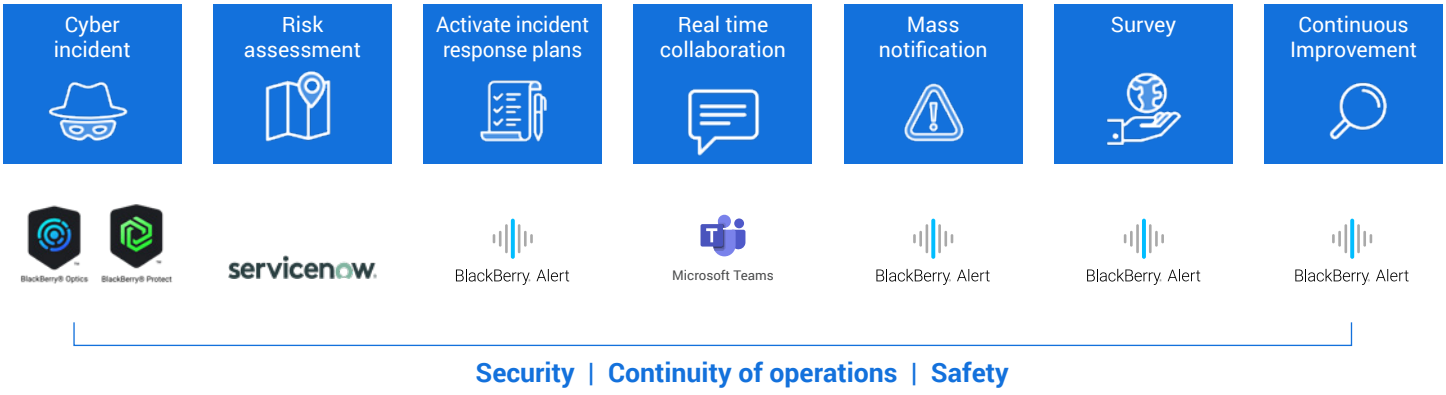
3. Reliable notifications

- Ensures alerts go to intended recipients by maintaining accurate contact information – the foundation of any CEM solution
- Enables recipients to filter out vital alerts from the noise of non-urgent messages
- Goes beyond traditional data sources, such as Microsoft® Active Directory® with tools that synchronize user information from .csv files or LDAP data sources

CEM authentication features

Look for platforms that offer operators and users the ease of secure SSO and/or smart card authentication, which help to boost adherence and adoption.

Response Timeline of Cyber Attack



4. Automated multi-channel two-way alerting

- Unifies all communication channels (email, SMS, mobile phones, etc.) to help ensure everyone gets the message – even when the network is down – with the ability to acknowledge receipt of information and initiate real-time chats to further collaborate with one-click
- Allows one-click targeting of individuals, pre-defined recipient groups, or the whole organization
- Automates alerts through integration with internal data sources, external data sources, and/or physical sensors
- Enables recipients to respond through any channel, so incident managers can easily monitor people's situation and status

5. Integrations with enterprise and collaboration tools

- Integrates with leading productivity tools for enterprise collaboration, like Microsoft Teams® and ServiceNow®
- Allows incident responders to contact, alert, chat, and further collaborate directly through these existing workflows and platforms, increasing message read rates

6.Tracking and analytics

- Tracks each alert recipient for a complete, transparent record of notifications
- Archives chats
- Provides a centralized dashboard and analytics for auditing and process improvement

Rest assured your data is safe

To safeguard your data, choose a CEM solution that's:

- Secure, with leading certifications
- Compliant with the latest industry regulations
- Mobile, for two-way mass or targeted alerting
- Trusted by a wide variety or organizations worldwide

Be Ready for Any Critical Event

The pressure on security leaders to protect organizations against cyber attacks is persistent and increasing, but so is the frequency and severity of threats in today's environment. Effective management of cyber incidents is essential for business resilience and competitive advantage.

A single, trusted, end-to-end CEM platform streamlines your organization's ability to plan, manage, and remediate incidents.

BlackBerry® Alert is a complete, cloud-based CEM solution for enterprise. With over 35 years in secure communications, BlackBerry is trusted by organizations worldwide, from the largest governments and security organizations to private companies.

Learn more at www.blackberry.com/alert

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear—to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry®
Intelligent Security. Everywhere.