everbridge®

WHITE PAPER

Executive Briefing: Security Transformation

Without the required security posture, the enterprise may experience economic, environmental, geopolitical, societal or technological disruptions.

How to Ensure Your Security Posture Builds Operational Resilience

Security transformation will differ by enterprise, depending on strategic priorities and existing security posture. Executive leaders have a continually growing list of priorities for board level discussion, yet the global pandemic has highlighted the immediate need for an effective, efficient, adaptable, and extensible security posture. Security investments can be aligned with existing strategic priorities, whether that is digital transformation, strengthening operational resilience, or enriching duty of care.

The entire c-suite is accountable for protecting people and keeping the business running. Enterprises manage extensive physical and digital assets in the form of facilities, systems, offices and factories and the associated people that use them. All these assets face increasingly credible disruptive forces. Therefore, every executive, not solely the CEO or CSO, should view safety and security as a strategic imperative. Without the required security posture, the enterprise may experience economic, environmental, geopolitical, societal or technological disruptions. It is important not to oversimplify the safety and security transformation narrative, as threats are progressing faster than enterprises can adapt.

Security Transformation

Enterprises need to build increasingly diverse strategies, tactics, and teams to handle their disparate risk factors. At the heart of a transformation is how an organization's security posture can accelerate business growth while managing risks. For most organizations, the CSO may be the only one with a background in risk management or security, and therefore, other executives may feel uncomfortable pushing a security transformation agenda. Enterprise security is

Any executive can and should feel empowered to fully align security tactics to the enterprise strategy.

a commercial investment, not a technology and/or facilities spend. Any executive can and should feel empowered to fully align security tactics to the enterprise strategy. The entire c-suite can communicate across the organization of the intent to transform their approach to security.

There is no single organizational security playbook; all c-level executives must diagnose their enterprise's unique internal and external challenges. This creates different policies and actions for each organization to deal with their strategic challenges. However, five examples of security challenges all enterprises face are:

+ Reducing operational costs through technology automation. Avoiding expensive rip-and-replace technology projects and reducing staffing needs with automation enhancements.
+ Preventing and managing critical events efficiently and effectively to mitigate business disruptions. Enhancing operational resilience to be able to respond, adapt, recover, and learn from critical events as they happen.
+ Enriching the organization's duty of care through reducing risk to safely and securely manage people in your facilities: e.g., using access control, building, and facilities management systems to heat map people's use of facilities to rationalize resources, while enhancing safety and reducing operational costs.
+ Increasing operational effectiveness while reducing operational costs. During any critical event, a flood of information flows into the organization which can be overwhelming. Reducing the noise and focusing people's attention on what needs to be done immediately through automating decision-making and compliance procedures, accelerates response times and mitigates business impacts.
+ Driving digital transformation and innovation to build an organization that is adaptable to critical events as they happen. Preparing for predictably unpredictable future crises.

Delivering a successful security transformation is often a complementary part of a larger migration to a more digital environment.

A Successful Security Transformation Program is More Than Just Security

Transformation agendas are often hampered by most organizations' limited budget and need to address improvements across multiple departments. However, the end goal of a successful security transformation is really the start to a digital transformation across an entire organization. Delivering a successful security transformation is often a complementary part of a larger migration to a more digital environment. Automation that enhances security can also introduce benefits that positively impact an entire organization's strategic, operational, and financial performance beyond the scope of pure security.

Once the strategy is created, revising the security operational blueprint is likely to be required for creating a common operating picture that works effectively in practice. The c-suite needs to organize and manage resources to achieve complete digital transformation. Ineffective siloed processes and lack of technology interoperability will hamper the effectiveness of employees; and will inevitably lead to a strategy implementation gap and a failed security transformation program.

Today's global security operations demand converged digital and physical capabilities. Within any enterprise's security ecosystem, the convergence reality may be more complex than many executives realize. Digital capabilities may sit in physical assets, such as sensors inside fire systems and alarms and CCTV that send data to command and control centers. It is illogical to view digital and physical security as mutually exclusive. Therefore, cybersecurity and physical security should be assigned equal boardroom importance through a converged common operating picture at a global, regional and local level.

The common operating picture may mean an enterprise has core security capabilities, such as visualization and communications that are powered by actionable insights. An additional integration service layer would utilize add-on capabilities and features that would mean technology could evolve more easily.

Security operations should deliver consistent treatment of incidents, emergencies, and crises; and, allow more standardized insights to be delivered to the boardroom. The overriding purpose of a robust security strategy is to drive security technology and process transformation that is fully adopted across the enterprise and makes commercial sense.

Digital Transformation of Safety & Security

Safety and security are no longer about guards, gates, observation, and reaction but about automation, analytics, and proactive control. The digital transformation of safety and security highlights the need for agile, adaptable, data-driven security executives and practices, to uphold duty of care, financial performance, and operational resilience obligations.

Ultimately, safeguarding people, facilities and assets while ensuring business continuity are everyday concerns for all executive leaders.

THE END GOAL OF A SUCCESSFUL SECURITY TRANSFORMATION IS REALLY THE START TO A DIGITAL TRANSFORMATION ACROSS AN ENTIRE ORGANIZATION

INNOVATION & TRANSFORMATION

Staying ahead of emerging and increasingly complex security threats requres ongoing innovation and transformation.

CYBER-PHYSICAL ECOSYSTEM

Today's global security operations demand converged digital and physical data and capabilities.

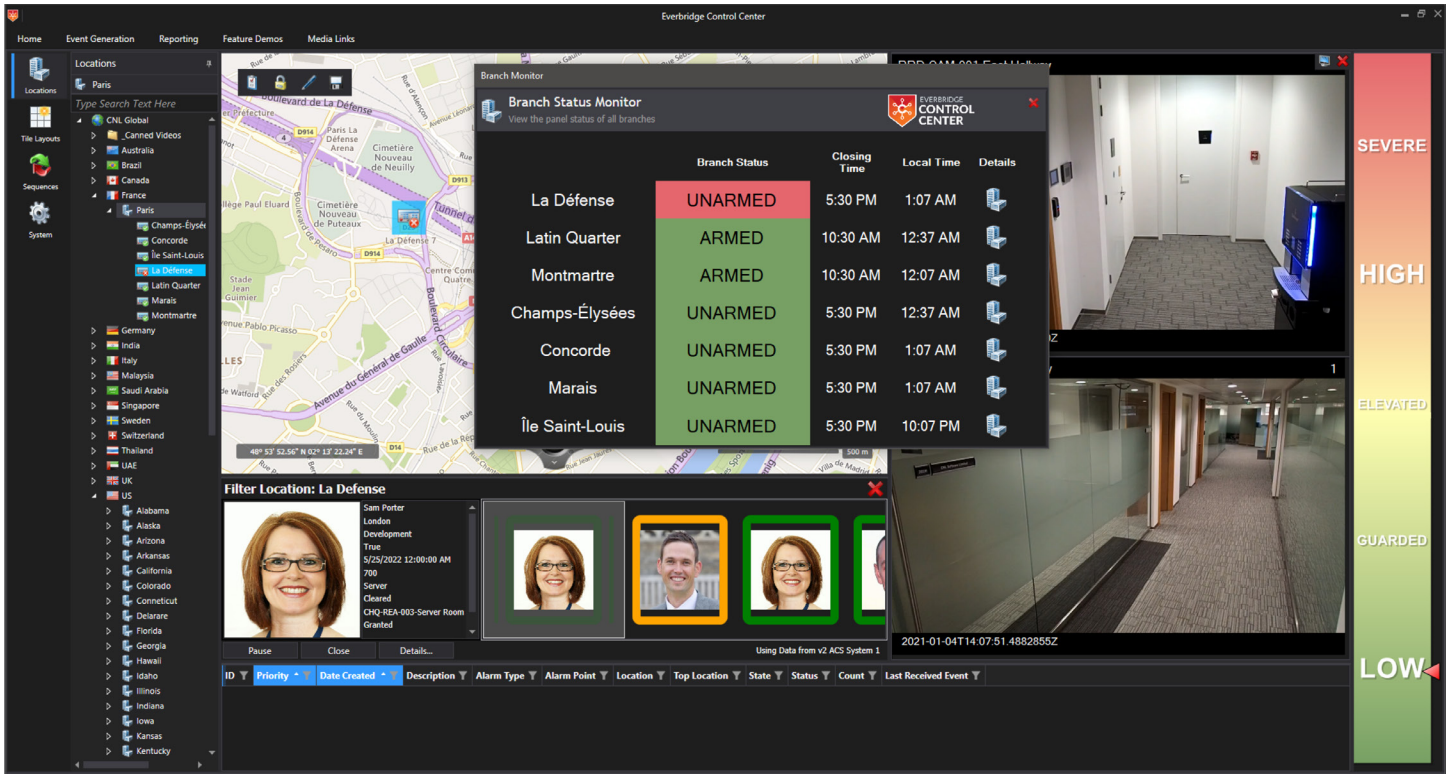
AGILITY & ADAPTABILITY

With an increasingly complex and unpredictable threat environment, it has never been more imperative to be agile, adaptable, and data-driven.

BARRIERS TO OVERCOME

Ineffective data and process silos and lack of technology interoperability will hamper digital transformation and potentially lead to failed initiatives.

Control Center benefits focus on creating strategic advantages, shareholder value and operational resilience through enhanced effectiveness and efficiencies.



Control Center correlates events from disparate safety and security systems into a common operating picture to focus people's attention on what really matters.

ABOUT CONTROL CENTER

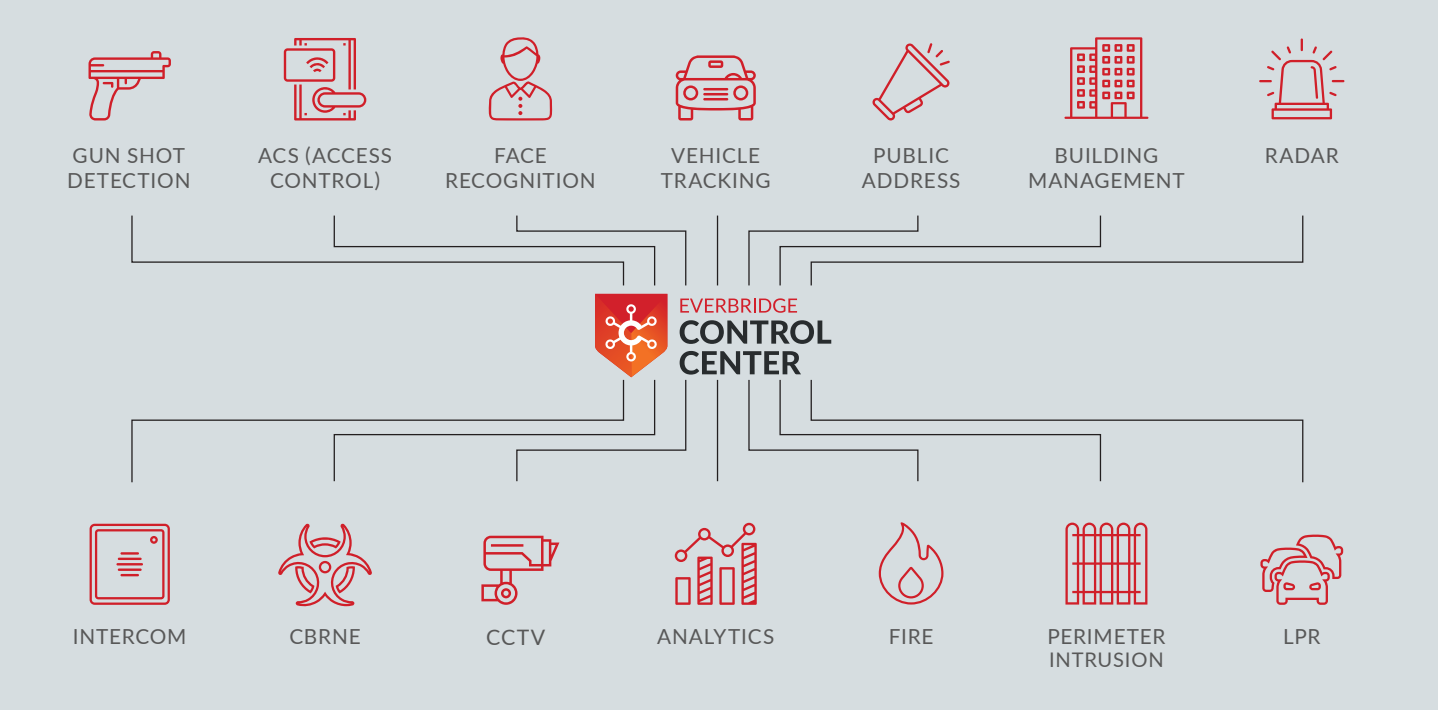
For many organizations, managing safety and security can be a daunting task. Threats are increasing and risks are becoming more diverse. Operations also continue to grow, involving more systems, more data, and many more users. All of this can be difficult to manage, and costly to control. Making sense of all your information is hard enough during normal operations. When a critical event unfolds and information floods into your organization, it can be overwhelming. You need to get the right information to the right people at the right time to protect your people and facilities and ensure operational continuity.

Maintaining Operational Control

Control Center correlates events from disparate safety and security systems into a common operating picture to focus people's attention on what really matters. The platform provides users with actionable alerts, next step actions, and automated reporting to better manage risks, ensure compliance with operating procedures and support your business continuity. Automated workflows ensure rapid, consistent responses, reducing the risk of human error. It also facilitates device activation to ensure you are always in operational control and protecting your people. Dynamic reports and dashboards provide real-time actionable insights for your operations teams and senior executives.

Integrating Systems, Devices and Sensors

Control Center integrates a variety of safety and security technologies to provide the holistic common operating picture:



Critical Event Management Integration

Control Center integrates with the wider Everbridge CEM Platform. Integration with Mass Notification and Incident Communications extends your on-premise solution to communicate with relevant people such as employees, visitors, residents or citizens. Critical information can be distributed in a timely manner, and any feedback is automatically received back to factor into the workflow for any situation. Control Center also broadens the scope of your Critical Event Management (CEM) capabilities, by enabling the on-premise data from your various systems to create hyper-relevant Risk Event feeds direct to the Everbridge CEM orchestration engine.

Let's Talk

Want to learn more about Everbridge Critical Event Management? Get in touch or just call us at +1-818-230-9700 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, cyberattacks or other incidents such as product recalls or supply-chain interruptions, over 4,800 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. The company's platform sent over 2.8 billion messages in 2018 and offers the ability to reach over 500 million people in more than 200 countries and territories, including the entire mobile populations on a country-wide scale in Australia, Sweden, the Netherlands, Singapore, Greece, and a number of the largest states in India. The company's critical communications and enterprise safety applications include Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Public Warning, Crisis Management, Community Engagement™ and Secure Messaging. Everbridge serves 9 of the 10 largest U.S. cities, 8 of the 10 largest U.S.-based investment banks, all 25 of the 25 busiest North American airports, six of the 10 largest global consulting firms, six of the 10 largest global auto makers, all four of the largest global accounting firms, four of the 10 largest U.S.-based health care providers and four of the 10 largest U.S.-based health insurers. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Beijing, Bangalore, Kolkata, London, Munich, Oslo, Singapore, Stockholm and Tilburg. For more information, visit www.everbridge.com, read the company blog, and follow on LinkedIn, Twitter, and Facebook.

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

everbridge®