Unified security solutions for military sites

Arm your most sensitive locations with a unified security approach

Military and government establishments are among the most secure sites in the world. Airfields, bases, surveillance centers, and weapon storage protect high-risk assets. To safeguard them against every eventuality, multiple lines of defense are exercised.

Operators must be able to secure the complex landscape with a broad ecosystem of tools. But these tools tackle unique challenges and can be siloed from core systems. Simultaneously operating all these applications requires data consolidation.

Bringing your defenses together for greater resilience

To cover all bases, military locations must deploy several solutions. Video surveillance, access control, automatic license plate recognition (ALPR), and intrusion detection all play a role. But often, these modules have been built in isolation. The uniqueness of Genetec Security Center lies in its singular platform, which embeds all physical security capabilities and encompasses a unified system where individual modules are created to work together. By unifying existing systems, military and government agencies can:

Increase situation intelligence

Multiple site-wide sensors help you keep a vigilant eye on your environment. Our unified platform boosts situational awareness by consolidating the data from these sensors. It provides operators with intelligence that might otherwise go unseen.

Scale and adapt

An open platform allows you to build a system that meets your unique requirements. Security Center supports a wide range of advanced features and plugins. Its flexibility makes it a reliable investment for the future.

Simplify operations

Protecting against unique threats means deploying a comprehensive ecosystem of tools. Managing these from one interface simplifies operations and makes response times quicker.

How military and government locations are using Security Center

Visualizing environments with Plan Manager

Agencies can visualize their environment through an interactive mapping module in Security Center. It helps provide context by displaying the location of events and devices using maps and floor plans. Security devices such as cameras, doors, and ALPR units operate within one interface. Information from external systems is also consolidated, enriching operators' comprehension.

Aerial surveillance

Integrations such as Skeyetech carry out patrols to identify threats and monitor crises 24/7. This can be centralized in the AdroneX task in Security Center. The task allows mission launch, provides drone position on the map, and gives the drone status.

You can also send drones on pre-configured flight missions or direct them to the GPS coordinates of a Security Center alarm. They are viewed and controlled on maps where operators can view no-fly zones and see drone footage alongside other devices.

Restricted Security Area Surveillance

Perimeter and area management are under pressure from new threats such as drones.

Security Center Restricted Security Area (RSA) Surveillance combines data from multiple devices to detect and track objects. Moving targets are automatically tracked on maps that show the geography. This makes it easy for security personnel to understand where the targets are and how they are moving. By using RSA Surveillance, security teams can save time and respond faster.

Weapon detection

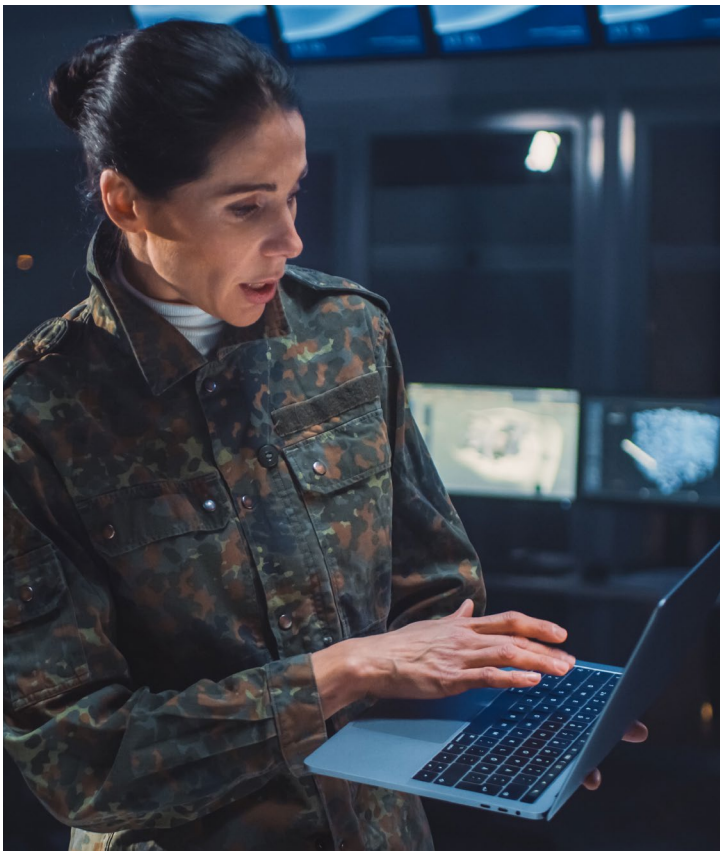
Shooter detection analytics integrations utilize acoustic gunshot detection and infrared flash detection. It alerts operators in under one second with zero false alarms.

Weapon detection integrations such as the X-ray Screener Support System enhance video monitoring. It captures input and output interactions, personnel screening interactions, and a complete video archive capture of the X-ray scan.

Cybersecure by design

Regardless of where threats originate, government agencies need to be ready. Whether it's an online hacker trying to steal intelligence or an intruder on the premises, security teams must be able to identify and stop threats. That's why all government agencies must now adhere to industry standards.

Our comprehensive approach to security incorporates multiple layers to protect your data. It secures communications between devices and servers and ensures the safety of your data storage. Whether your security infrastructure is on-premises or in the cloud, our products can help keep your operations and data secure.



Key benefits

- Deploy a cyber-resilient system that evolves with time to face current and future threats
- Improve your efficiency with automated services and features
- Protect your data's confidentiality, integrity, and availability (CIA)
- Safeguard the privacy of patrons, employees, and their personally identifiable information (PII)
- A multi-layered software security model
- Government-approved cybersecurity certifications include ISO/IEC 27017, SOC 3 Compliance, SOC 2 TYPE II Compliance, and the European Privacy Seal

Certifications

Our unified platform meets stringent qualifications outlined by governments globally. That's why we support government agencies worldwide to secure their most sensitive sites. Our certifications include the following:

- SAFETY Act Designation and Certification from the U.S. Department of Homeland Security
- General Services Administration for U.S. Government Agencies certification
- Centre for the Protection of National Infrastructure certification
- FBI CJIS Compliance
- FICAM/FIPS 201-2/HSPD-12 - GSA Approved for U.S. Federal Agencies

As threats continue to evolve, operations become more reliant on intuitive technology. Agencies need a solution that gives them greater control, knowledge, and visibility.

Our military solutions offer an intelligent and secure way to manage your infrastructure. Unifying your security into one system will help tackle today's challenges and tomorrow's.

Contact us today to learn how to overcome current challenges and reduce future threats.

Genetec Inc.
genetec.com/contact-us
info@genetec.com
@genetec

UPDATED: 24-MAY-2023