Cybersecurity in the physical security world

Your guide to defending against today's cyber threats and protecting sensitive information within your physical security systems

Genetec™

A look inside

Cybercrime is at an all-time high. Are you doing enough?

Cybercrime is accelerating faster than ever before. According to Cybersecurity Ventures, global crime costs will reach $10.5 trillion USD annually by 2025. At a growth rate of 15% per year, this is said to represent the greatest transfer of economic wealth in history.

Because of this, organizations want to remain agile and responsive to evolving threats. Building layers of protection into a security ecosystem is a good first step, but it's likely not enough.

Today, true resilience requires more offensive cybersecurity strategies. It also requires choosing trusted partners who offer you automated tools to better mitigate threats.

In this guide, you'll find everything you need to up your cybersecurity game and keep your organization protected.

The threat landscape

Common attack strategies

Hacking a security system can take any number of forms. Here are some of the most common attack strategies today:

Spyware

Installing malicious software on victims' computers or creating copycat websites to trick victims into providing their credit card information or passwords.

Ransomware

Installing malicious software to block access to essential data or systems unless the victim pays the attacker to restore access.

Denial of service (DoS) attacks

Flooding a target machine or network with traffic or sending it information that triggers a crash, making it inaccessible to its users.

Brute-force attacks

Guessing or cracking passwords to gain unauthorized access to systems and networks.

Man-in-the-middle attacks

Capturing and potentially altering communication between two parties without their knowledge, allowing attackers to eavesdrop on or manipulate the data.

Phishing attacks

Sending fraudulent communications that appear to come from a reputable source, designed to trick a person into revealing sensitive information or to deploy malicious software.

Common cybersecure architectures

Enhancing cyber resilience in 7 steps

Cybersecurity video series

Cost of breaches

Companies face legal, regulatory, and technical costs to recover from a breach

Organizations lose productivity when operations are interrupted by software, networks, or websites being down

Victims often must pay to restore or replace damaged devices or fix code on compromised websites

Customers lose trust when their data is breached, which increases turnover

Public company stock performance usually takes a hit following an attack

15% of breaches

were from phishing attacks.

Source

16% of breaches

were because of stolen or compromised credentials.

Source

4 million professionals

are urgently needed to plug the talent gap in the global cybersecurity industry.

Source

84% of CISOs

fear being personally liable for cybersecurity incidents.

Source

$4.88 million USD

The average cost of a data breach, reaching a record high in 2024.

Source

66% of Global 100 organizations

will extend directors and officers (D&O) insurance to cybersecurity leaders due to personal legal exposure by 2027.

Source

68% of global breaches

involve a non-malicious human action like making an error or falling prey to an attack.

Source

Questions to ask about your cybersecurity defense capabilities

Older proprietary security technologies weren't designed to defend against today's threats. They simply can't support cybersecurity and privacy fundamentals—ensuring data confidentiality, integrity, and availability.

Ask these questions to determine if your legacy equipment is impeding your cybersecurity posture:

1. Do you know the financial and operational consequences if you failed to secure one of your hundreds of cameras and that device becomes the pathway to a breach of customer information?
2. Are you aware of how much time your team spends every month updating different software and firmware and managing cybersecurity practices across your various systems?
3. Do you have the ability to build and maintain strong identity and access management policies and restrict who has access to your systems and data? Can you offer single sign-on capabilities with multiple layers of authentication?
4. Do your legacy systems allow you to adopt the latest encryption methods or cybersecurity features to stay ahead of evolving threats?
5. If your organization receives a request from a customer or a police officer to see collected video footage, will you be able to securely share those recordings while protecting the identities of other individuals in the frame?

See what Security Center is all about

Activating Security Center cybersecurity features

3 steps to defending against cyber threats

Building your cybersecurity strategy

Core cybersecurity measures: encryption, authentication, and authorization

Today, there are many things you can do to build resilience in your physical security deployment. The more layers you implement, the better protected your business will be. Explore the most essential cybersecurity tools below.

Layer 1 – Encryption

Encryption ensures the confidentiality of your physical security data. This applies to data sent between video cameras, access control readers, and other IoT sensors—to and from your servers and client workstations. By encoding information or scrambling readable text, you can safeguard sensitive information from unauthorized access. Remember to manage encryption keys properly, as they are critical to maintaining secure communication.

TIP

When it comes to encrypting video surveillance specifically, it's essential to use strong encryption methods for both data in transit and data at rest. Though data in transit is generally considered more vulnerable, threat actors will always target the weakest point of entry.

Layer 2 – Authentication

Authentication is a process that validates the identity of a user, server, or client application before granting them access to your protected resource. On the client side, authentication can include various techniques such as usernames and passwords, and security tokens. On the server side, the confirmation of trusted third parties is usually provided through digital certificates.

TIP

Deploying multiple forms of authentication strengthens security. Move beyond passwords by using passkeys, authenticator apps, biometrics, or hardware security tokens like a YubiKey or smart card to guard against threats.

Layer 3 – Authorization

Authorization allows you to define specific user privileges to control what users can see or do within an application after authentication. In security systems, this also includes when and what information can be shared internally or externally, and how long data is kept.

TIP

You can automate the provisioning of these granular privileges through a Microsoft Active Directory integration with your security systems. Not only does this help to simplify the authentication setup, but it also ensures that when an employee leaves the company, their system privileges get revoked.

Best practices

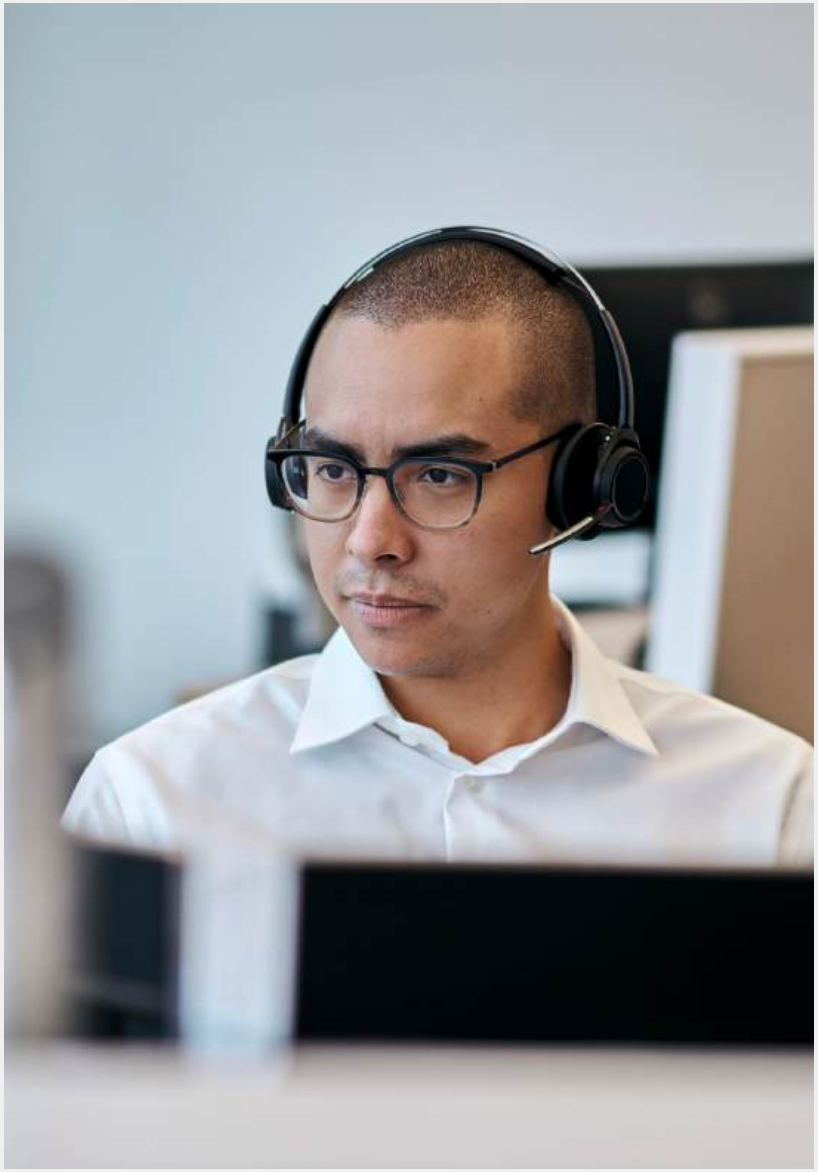
Consider products with built-in cyber defenses. This ensures that you always have what you need to protect sensitive information from prying eyes. Explore more below:

Keep information out of reach

You can rely on advanced encryption, authorization, and authentication methods to protect your data and prevent it from falling into the wrong hands. Ensure that your data isn't tampered with by adding watermarking and digital signature features on your video recordings.

Ensure your data is always available

Implement disaster recovery, continuously keep track of your cybersecurity posture, and get personalized recommendations for added resilience. These will help you ensure that your data always remains available and that every component in your system works as it should.



Maintain your software and devices

Built-in health monitoring and update services keep your system running at peak performance. You can also centralize and schedule software and firmware updates, automatically rotate passwords, and quickly address potential vulnerabilities.

Rely on vetted and compliant solutions

Choose vendors that ensure compliance with development standards and solutions. Some work hand-in-hand with international associations to adhere to the latest cybersecurity best practices. Penetration tests and audits should be routinely conducted on products as well.

Audit your system and track user activities

Maintain a full chain of custody with built-in audit trails and user activity reports. Comply with auditing requirements and corporate policies by streamlining identity management and scheduling access reviews for users and roles.

Get full transparency about risks

Receive open and transparent communication from your vendor as potential risks come up. Trust that they'll immediately share important fixes, updates, and best practices to ensure your system remains optimized and hardened.

Protecting against cybercriminal activity

Our cybersecurity certifications

Cybersecurity best practices in 3 minutes

Why unification offers an easier, more effective way to protect your data

To deter cybercriminals and protect information and assets, many organizations want to implement a single, global data protection and privacy strategy. Security Center simplifies that process by helping you standardize your cybersecurity measures across all your physical security systems. Explore how below:

Centralize your data protection

Using a unified platform, you won't have to waste time checking different solutions to ensure cyber hygiene or track your system's health status. Instead, you'll be able to stay in control of the data from all your systems through a single interface.

Get many built-in defenses

Unified tools and services alert you to potential vulnerabilities and help you simplify updates. Other features help you restrict system access and user privileges, and provide security scores to make sure you reach full-scale system resilience.

Reduce risks with single logins

Having a unified platform means your users only require a single login and password. This minimizes the chance of multiple passwords being stolen or hacked and the likelihood of a potential breach. You can also customize data retention policies across your global sites to meet local laws.

The Genetec Update Service

Cloud solutions and cybersecurity

Built-in features to secure your devices

10 questions to asses your vendor's approach to cybersecurity

One of the best ways to lower your risks is by choosing to work with trusted vendors. Though everyone touts cybersecurity these days, the following questions can help you assess the trustworthiness of your existing supply chain or a new vendor:

1. Does the vendor have a robust incident management plan, and how often is it tested for effectiveness?
2. Do they have a vulnerability management policy in place with service level objectives based on vulnerability severity to close security gaps?
3. What policies do they have in place concerning cybersecurity?
4. What risk management framework does the vendor use? How do they identify, prioritize, and address emerging risks?
5. How are they protecting the organization's data and the privacy of their customers?
6. Do they work with partners who also have security and data protection in mind? How do they vet their partners to maintain the highest levels of cybersecurity and compliance?
7. How do they communicate security vulnerabilities for their products or incidents related to their customers?
8. Are they forthcoming about known vulnerabilities and do they share strategies and fixes for quick remediation?
9. Do they adhere to information security standards such as ISO 27001? Ask them to share their policies, certifications, and full audit reports from regulatory bodies and international associations.
10. Do they use third-party auditors for penetration testing to find security gaps? Request their test reports and remediation plans.

A solid partnership on cybersecurity

Our global network of partners

Choose a vendor you can trust

Enhancing cybersecurity with cloud and hybrid-cloud

Securing your physical buildings, while maintaining cybersecurity best practices requires a lot of extra work with on-premises systems. When you have hundreds of locations around the world, the complexities skyrocket. Cloud services offer you an easier path to cyber resilience because it takes the burden of constant upkeep off your IT and security teams. Explore how below:

Get built-in cybersecurity tools

Using a cloud-based physical security solution, you'll always have access to the latest built-in cybersecurity features. That includes encrypted communications in transit and at rest, granular privacy controls, strong user authentication, and various health monitoring tools.

Receive fixes and updates right away

Genetec Security Center SaaS offers continuous access to new software capabilities and features as they become available with zero downtime. This means you can access the latest versions and fixes as soon as they are available. This helps to ensure that your physical security systems are up-to-date and protected.

Enhance your data redundancy

Opting for a hybrid-cloud deployment means you can deploy security systems on-premises while archiving video in the cloud. This approach lets you save three separate copies of video files in the cloud, enhancing redundancy and availability.

Security Center SaaS

Cloud First: A Panel Discussion

Cloud solutions that stand the test of time

Tools to keep up long-term

How to maintain an effective cybersecurity strategy long-term

Maintaining cybersecurity in physical security isn't just about defending against attacks; it's about establishing trust with your customers and partners and ensuring the success of your organization for years to come. To do that, and do it well, you need to continuously assess, re-evaluate, and update your data protection and privacy measures. Here's how:

Be aware of the threat landscape

Don't rely on other IT or security professionals to keep you informed about cyber threat protection. Do your best to keep up with evolving risks and mitigation strategies. Then educate your employees on the dos and don'ts so they become just as aware.

Conduct a risk assessment and asset inventory

Get to know the ins and outs of your environment so you can put the proper cybersecurity mechanisms in place. Make a list of the computers, IoT devices, users, types of data, etc. This will help you maintain higher levels of cybersecurity protection.

Stay on top of system updates and patching

Patches could help you specifically address security vulnerabilities and mitigate potentially huge risks. Consider automated tools that alert you to software and firmware updates, or transition to cloud services which provide those updates automatically.

Start implementing multi-factor authentication

Relying solely on passwords can put you at risk. Strengthen your security with multi-factor authentication (MFA) and use passphrases that are long and unique. Avoid forced frequent password changes. Instead, focus on complexity and use of password managers.

Have a plan for disaster recovery

Your goal is to achieve 100% cyber threat protection in all you do. Even so, that still might not be enough to fully keep attackers at bay. Having a physical security system that detects possible compromise is essential, but so is having a cybersecurity incident response plan.

Setting up Security Center best practices

State of Physical Security Report

Our System Availability Monitor

Hardening tools and built-in defenses

Not all physical security systems are built with the same levels of cybersecurity protection. Sure, some vendors might offer you the basics, but tackling today's threat landscape requires more. At Genetec, we think outside the box to deliver unique hardening tools that help you build resilience. Explore more below:

1 Automated compliance tracking

Want to get a quick overview of your security systems' health? Easy. Our Security Score widget is a dynamic hardening tool that checks the security of your system in real-time. It lays out guidelines and then monitors whether the different elements of your system comply. The widget then scores your compliance and offers recommendations for improvements.

2 Enhanced updates scheduling

Product updates often provide critical fixes for newfound vulnerabilities. But many still overlook how critical updates are to maintain cyber resilience. The Firmware Vault differentiates standard firmware updates versus new features and security updates that address vulnerabilities. This way, you can easily prioritize and manage updates, ensuring you always have the latest defenses with just a few clicks.

3 Efficient password management

Password management policies are essential for securing your devices. Within Security Center, our built-in password manager can automatically generate strong, randomized device passwords that comply with security best practices. You can also set up automatic updates for your camera passwords on a schedule or in batches.

A look at our Firmware Vault

Activating cybersecurity features

Are your cameras secure?

Build up your data protection strategy with Genetec

Every year, cybercriminals are becoming more sophisticated with their attacks. This is putting pressure on organizations to scrutinize cybersecurity measures, standards, and certifications. This goes beyond their physical security system into their entire supply chain ecosystem. Because what worked for you last year, might not be enough to keep threat actors at bay in the future.

At Genetec, we build compliant and cyber-resilient solutions that help you protect your most sensitive information—and we don't stop there. We stay on the pulse of emerging cyber threats and work with our partners and customers to advance cybersecurity measures. This ensures you're always equipped to keep your cybersecurity posture strong.

Looking for a partner you can rely on? We got you.

Visit our Trust Center

For more information about our company and products, please visit our website at genetec.com

Genetec Inc.
Genetec.com
info@genetec.com
@genetec

UDPT: 13-Apr-2026