Cybersecurity checklist

Every day, cybercriminals are finding new and sophisticated ways to capitalize on vulnerabilities. The increase in remote work, connected devices, and data has amplified cybersecurity risks.

According to our 2026 State of Physical Security report, end users are seeing an increase in cybersecurity incidents like malware and device hacking for network access. As a result, 47% of IT specialists said that deploying cybersecurity tools is a top priority.

Having a comprehensive cybersecurity strategy is crucial at every stage in your physical security journey. Below are some checklist questions to help inform a stronger cybersecurity posture before, during, and after your physical security deployment.

Genetec™

Pre-deployment checklist

Are you implementing or adding a new system to your physical security infrastructure? Be sure to set yourself up for success. This checklist will help you assess your vendors, optimize your deployment plan, and mitigate potential risks.

Best practices

- [ ] Do I have a proper cybersecurity strategy plan in place?
- [ ] Have I assessed cybersecurity in the scope of my physical security system?
- [ ] Did I conduct a vulnerability assessment to identify gaps that can be closed through the convergence of physical and cybersecurity?
- [ ] Did I perform a thorough vulnerability assessment of all connected physical security devices to identify models and manufacturers of concern?
- [ ] Am I only using genuine products and avoiding counterfeit and unlicensed products?

Risk management

- [ ] Do I have a comprehensive risk management strategy in place?
- [ ] Did I create new baseline protocols to guide security operations and incident management?
- [ ] Are my IT and physical security teams aligned on a comprehensive security program?
- [ ] Have I identified all users who can access physical security devices and systems?
- [ ] Am I using edge devices from trusted manufacturers?
- [ ] Do I have a breach management policy and procedure?
- [ ] Do I need cyber insurance?
- [ ] Do I have a plan to back up my important data and protect it against disasters?
- [ ] How do I ensure my system is available when I need it?

Certifications and regulations

- [ ] Which data protection regulations, directives, or frameworks apply to my specific situation?
- [ ] Have I assessed what we need to do to comply with the GDPR, NIS2, PIPEDA, or other applicable data protection regulations and directives?
- [ ] Do the solutions considered include any international or relevant certifications?
- [ ] Does the solution architecture align with industry-specific compliance standards and also support relevant regulatory authority compliance standards (ISO 27001)?
- [ ] Do the chosen solutions come with tools and features that can support us in meeting regulatory compliance and maintaining cybersecurity best practices?
- [ ] Is there evidence that can be provided that due diligence mapping of regulations and standards to controls/ architecture/processes has been done?

Vendor assessment

- [ ] Does the vendor have notifications warning about maintenance time or other events requiring a system to be put offline or rebooted?
- [ ] Does the vendor have notifications when the system should be put offline?
- [ ] How transparent are vendors with cyber vulnerabilities?
- [ ] Does the vendor have a documented security incident response plan that they're willing to share?
- [ ] Does the vendor have a comprehensive strategy to close security gaps and vulnerabilities?
- [ ] Does the vendor prioritize cybersecurity in the development of their products?
- [ ] Who's liable if your equipment is used to access private information?
- [ ] Who owns the manufacturing company that builds their software and hardware?
- [ ] Does the vendor engage third-party auditors and conduct penetrating tests to identify and address security gaps?
- [ ] Does the vendor have any certifications from regulatory bodies and international associations, and do they adhere to information security standards?
- [ ] Do they carefully vet and select partners to ensure the highest levels of cybersecurity and compliance?
- [ ] How stable and established is the vendor? Are there signs that we can trust this vendor and that they will continue to support and develop the solution in the future?

Appliances and cloud services

- [ ] How am I making sure that my security appliances are configured securely?
- [ ] Do I have a specialized antivirus and antimalware protecting my edge devices and security appliances?
- [ ] Is the cloud solution built and tested with privacy and data protection in mind?
- [ ] Does it come with built-in cybersecurity defenses and default privacy protection to help me enhance risk mitigation and regulatory compliance?
- [ ] Is my cloud provider ensuring the security and governance of my data?
- [ ] Does the cloud service provider have the capability to restrict the storage of our data to specific countries or geographical locations?
- [ ] Is the data exchanged and stored in the cloud fully protected?
- [ ] Has the hosting infrastructure had a SOC 2 Type 2 audit?
- [ ] Does the cloud service provider ensure that the latest security patches are applied to operating systems/assets/applications in a timely manner?
- [ ] Can the cloud service provider isolate our environment/data from other customers' environment/data?
- [ ] Does the cloud vendor have a plan in place to return or destroy the data at the end of the relationship?
- [ ] What is the cloud solution's track record for reliability and uptime, and what measures are in place for backup and disaster recovery?

Deployment checklist

Ready to deploy your new physical security system? Follow this checklist to stay on track with your upgrade or installation, mitigate risks, and ensure a smooth deployment.

Best practices

- [ ] Have I trained my employees properly on cybersecurity best practices?
- [ ] Do I monitor and share intelligence about current cyber threats and trends in the industry and encourage collaboration on preventative actions and responses?
- [ ] Do I have an up-to-date inventory of all physical security and IoT assets?

Data protection

- [ ] Is the multimedia data stored in my system protected?
- [ ] Is the multimedia data protected when exchanged in my system?
- [ ] Is the command-and-control data protected?
- [ ] Have I implemented end-to-end encryption?
- [ ] How are my encryption keys managed?
- [ ] Am I leveraging all available built-in mechanisms to ensure data integrity and prevent unauthorized modifications or tampering?

Device security

- [ ] Are my video, access control, license plate recognition hardware and other physical security devices secured?
- [ ] Do I maintain detailed information about each physical security device, e.g. manufacturer, and firmware version?
- [ ] Do I have an up-to-date inventory of all devices connected to the network?
- [ ] Do I have a plan for the replacement of unsecured devices?
- [ ] Do I know how to identify and use the various encryption and cybersecurity capabilities supported on each device or firmware version?
- [ ] Have I confirmed that my video and access control software is up to date along with the devices and servers used for storing data and hosting monitoring consoles?
- [ ] What is my strategy to patch my device firmware promptly?

Authentication and authorization

- [ ] Am I managing passwords correctly?
- [ ] Did I establish a policy and process for credentials lifecycle management?
- [ ] Have I changed all default usernames and passwords?
- [ ] Am I using strong passwords to access my security system and every connected device?
- [ ] Have I implemented multiple forms of authentication to prevent unauthorized access?
- [ ] Have I implemented a multilayer strategy that includes multifactor authentication and defined user authorizations to strengthen the security of users' access to the systems?
- [ ] Do I centralize identity management for all my security systems as much as possible?
- [ ] Do I have any protection in place against password brute force attacks?
- [ ] Have I set up my user groups correctly and assigned permissions to the right people?
- [ ] Are we using tools that support role-based access management?
- [ ] Do I have any protection to restrict user access after prolonged inactivity?
- [ ] Do authorized users only have access to what they need?
- [ ] Are we applying the principle of least privilege in granting access?

Post deployment

Once your deployment is complete, the job doesn't end there. This checklist will help you monitor the health of your system, check your cybersecurity posture, and plan preventative measures to keep your system running smoothly.

Maintenance and updates

- [ ] Do I have tools to keep my devices and physical security software up to date?
- [ ] Am I on the lookout for critical security updates for my on-premises systems?
- [ ] Have I verified the source and legitimacy of each software and firmware update before installation?
- [ ] Have I checked device inventory against published information about manufacturers and models that have identified security risks?
- [ ] Do I have a plan to improve the network design as needed to segment older devices and reduce potential crossover attacks?
- [ ] Am I applying the proper software patches and hotfixes?
- [ ] Am I properly maintaining my Windows ecosystem?
- [ ] Do I have the proper tools to keep everything up to date and cyber secure?
- [ ] How can I keep my list of users up to date?
- [ ] Do I have tools to automate my maintenance activities?
- [ ] How do I keep the operating system of my security appliances up to date?
- [ ] Do I have tools to review which users have access to our systems, applications, and data and update user privileges?

Health monitoring and risk management

- [ ] Do I have the proper tools to monitor the status of my systems and devices?
- [ ] Can I centrally monitor the status and health of multiple deployments?
- [ ] Is automated alerting set up for critical events and thresholds?
- [ ] Am I keeping a chain of custody?
- [ ] Am I conducting reviews of audit trail logs or automating reports on user actions, system events, and access attempts?
- [ ] Am I on the lookout for new threats and vulnerabilities?
- [ ] Do I have log analysis techniques to investigate in case of a cyber incident?

Genetec Inc. is a technology company that offers on-premises and cloud-based solutions encompassing security, intelligence, and operations. The company's flagship product, Genetec™ Security Center, is a physical security platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security in the communities in which we live.

UDPT: 15-12-2025

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

Genetec™