Whitepaper

Risks of legacy access control systems

Genetec™

Contents


1 2 3
4 5 6
7 9

Executive summary

Many organizations are holding on to access control systems that date back 15 years or more. Older access control systems may seem to work well enough to allow employees to badge in and out, but this kind of legacy technology can be vulnerable to cyber threats.

New and more cyber secure access control solutions feature end-to-end encryption and advanced authentication, and other features to defend against cyber attacks and malware. A modern, unified approach to access control can make your organization more resilient to cyber threats, while also delivering far more value than simply locking and unlocking doors.

1

Introduction

Around the world, savvy cybercriminals are hunting for security gaps to gain access to facilities, surveillance systems, and sensitive data that they can sell on the black market or use to extort an organization. Those that are affected pay a heavy price; the average cost of a data breach rose from USD 3.86 million in 2020 to USD 4.24 million in 2021[1] , but the cost for some companies has been in the tens of millions. In 2021, one company was asked to pay a $70 million ransom[2] — the highest yet demanded in a cyberattack.

Computers and servers aren't the only devices that are vulnerable to cyber threats. Any device connected to the internet or your local area network can be a weak point when it comes to cybersecurity.

Vulnerabilities in legacy access control systems can introduce cybersecurity weaknesses that put your organization at risk. Emerging cyber threats can target these vulnerabilities at every level: the credential, the controller, and the server or workstation.

If a cybercriminal breaches your network in order to gain access to sensitive data such as proprietary information or customers' private information, the impact of a cybersecurity breach in your access control system can cause damage far beyond your doors. It can not only impact your bottom line, but also potentially you and your employees' reputation, your customers' privacy, and more.

You need to protect what's protecting you. That's why enterprise, government, education, and public safety organizations are moving away from proprietary solutions in favor of secure access control solutions. They're looking for a unified physical security platform built with cybersecurity in mind.

[1] https://www.ibm.com/security/data-breach
[2] https://www.welives`ecurity.com/2021/09/30/eset-threat-report-t22021/

If a cybercriminal breaches your network in order to gain access to sensitive data such as proprietary information or customers' private information, the impact of a cybersecurity breach in your access control system can cause damage far beyond your doors.

2

Cybersecurity weaknesses in legacy access control systems

Most access control systems today are Internet Protocol (IP) based, connected to a local network through the internet. IP-based systems are powerful, but legacy systems lack vital cybersecurity features that are necessary to defend against ever-evolving cyber threats.

Your access control system is only as strong as its weakest link. Cybercriminals can exploit weaknesses in access control system credentials, controllers, servers, or workstations connected to the network. Once someone has breached your network, they can gain control of other building systems, view or steal sensitive information from internal records, or launch attacks designed to take key systems offline.

Some common cybersecurity threats involving access control systems include:

- **Man-in-the-middle attacks** — When a cybercriminal gains access to a network to glean information exchanged between devices, such as door opening codes or device logins and passwords
- **Skimming and relay attack** — When a criminal uses their reader to access and clone information on the victim's card without consent
- **Controller attacks** — When a criminal overwrites the controller firmware, rendering the device unusable

Once someone has breached your network, they can gain control of other building systems, view or steal sensitive information from internal records, or launch attacks designed to take key systems offline.

3

Vulnerabilities at the credential level

Access control systems rely on user credentials to determine who is and is not allowed to access specific areas. There are many types of credentials used by these systems, including PIN codes, smartphone apps, fingerprints, and key fobs or cards.

Cybercriminals can steal user credentials in skimming attacks. This is when they use their own, unauthorized, reader to access information without the user's knowledge. Alternatively, if they can gain access to your network, they may intercept credential data sent on the network and store it for later use. They can use this data to 'spoof' or clone some types of older key cards or fobs that are still in common use. Many older credentials, such as proximity cards, can be very easily copied using a cheap device that can be bought online.

Some common credentials used in legacy access control systems with magstripe and 125kHz proximity cards also have known vulnerabilities. Many communicate through the Weigand protocol, which has become the industry standard since its invention in 1974. Unfortunately, hackers have learned how to tamper with the card readers commonly used with this type of system to retrieve sensitive information.

Wiegand communication is one-directional, so if the reader is tampered with, the controller is not notified unless wired to a tamper switch. Data sent via a Wiegand-style system is also unencrypted, so even when using secure credentials, sensitive information can be retrieved.

To mitigate the risk of man-in-the-middle attacks, look for a system that has a secure, bi-directional protocol between the reader and the controller, such as OSDP2. This will ensure that if someone attempts to steal credentials by tampering with the reader or replacing it with a fraudulent reader, they will be unable to retrieve

The most common vulnerability at the credential level, however, is human error. Sharing PIN codes or key fobs, losing key cards, holding or propping doors open.

sensitive information. The bi-directional protocol will also notify the operator that there has been an attempt to tamper with the system, so your security team can quickly respond and neutralize the threat.

The most common vulnerability at the credential level, however, is human error. Sharing PIN codes or key fobs, losing key cards, and holding or propping doors open are common little decisions that can have a big impact on the security of your building.

Choosing advanced secure credentials or biometrics is the best approach to reduce vulnerabilities at the credential level. Improving cyber hygiene can also help to reduce risks related to human error. Ensure all staff are offered training, prompts, and reminders to create a work culture that encourages and reinforces good cyber hygiene. This requirement should extend to the partners you work with, as a breach on their end could impact your security as well. Ask all software partners to describe the actions they take to ensure their staff follow cyber hygiene best practices – and include cybersecurity as a component of Request For Proposal requirements – when seeking new software partners or suppliers of network-connected hardware.

Managing access rights is another process that is prone to mistakes when information is managed and tracked manually. Choose security partners that can also provide a unified solution to manage access rights based on roles and user status, not individuals. This allows you to automatically upgrade, downgrade, add or cancel access rights for groups of people as needs change. For example, when an employee goes on maternity leave, changes roles, or leaves the company. When the employee's status changes in the linked database, their access rights change too, so you can eliminate the risk of someone using an old key card to enter areas where they no longer belong. This system also allows you to revoke access quickly if someone's key card or another credential is lost or stolen.

4

Vulnerabilities at the controller level

Controllers interpret the credentials from the reader and compare them to a whitelist synchronized from the access control server. If the credentials match, it sends a signal to the door lock to either open or deny access.

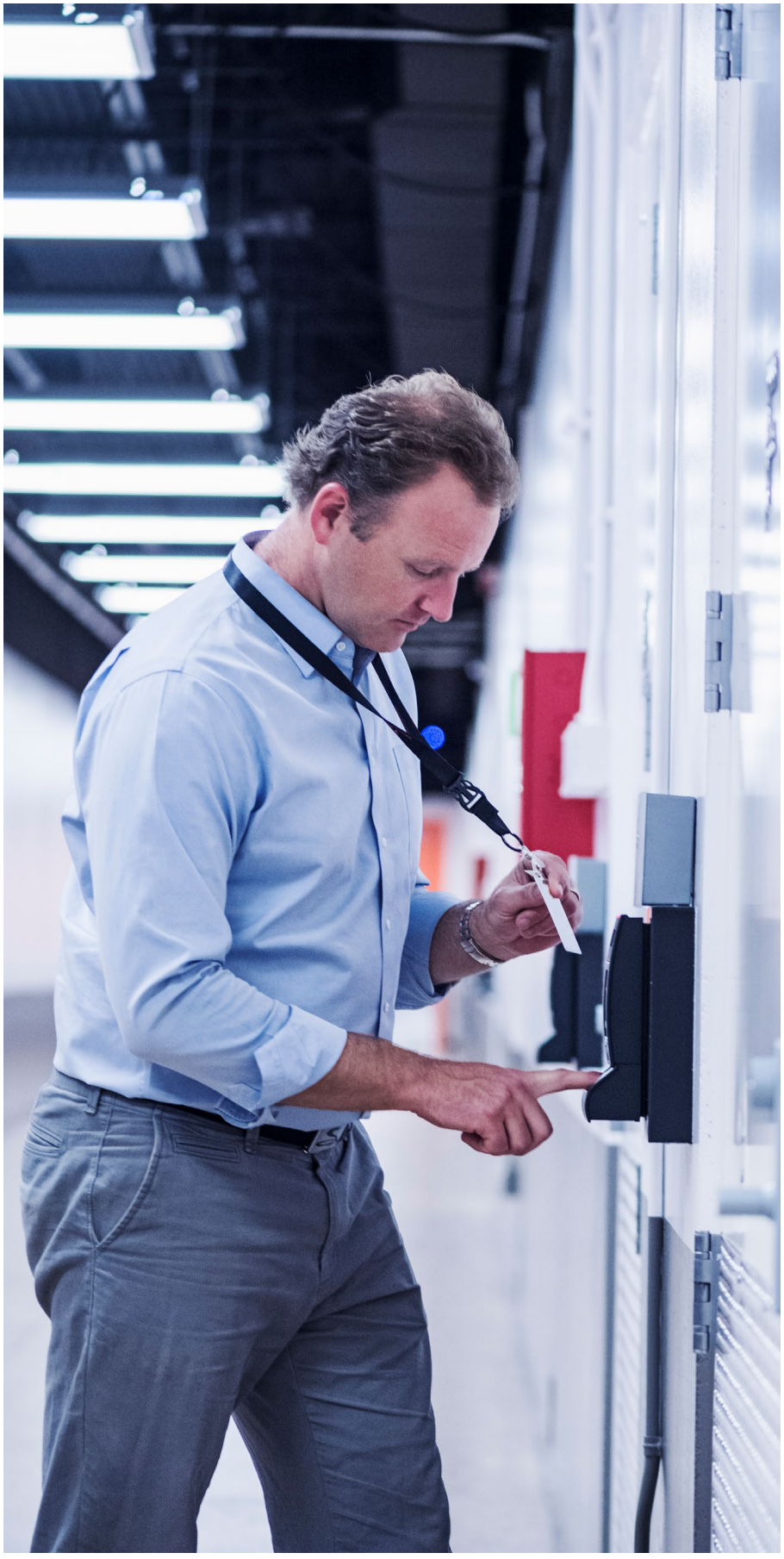
A weak encryption or password could allow cybercriminals to gain access to your controllers, therefore getting the keys to your facility.

Modern access control systems use an intelligent certificate management tool to authenticate the controller and ensure secure communications between the access control server and controller. The authentication will confirm that an authorized controller is connected to a legitimate server from which it receives instructions. To secure communications between the two components, it is recommended to encrypt communications by using the Transport Layer Security (TLS) protocol versions 1.2 and above.

Controllers require regular firmware updates to ensure security is up to date. It's important to ensure your security team checks for updates regularly or outsources this to a reputable third party or vendor so they are installed promptly.

Finally, a simple but important action to take to secure your controllers is to ensure that default passwords have been changed to something unique that cannot easily be guessed. Another best practice is to have a password management system that automatically changes the passwords that are used between devices on a regular basis.

Controllers require regular firmware updates to ensure security is up to date. It's important to ensure your security team checks for updates regularly so they are installed promptly.



5

Vulnerabilities at the server or workstation level

Servers store and manage the list of approved credentials given to individuals, and communicate with the controllers to authenticate credential data. This information must be transmitted over a network. If the data is unencrypted, cybercriminals who gain access to the network can poach credential information and other sensitive data.

Credential data captured from readers and stored in servers should be protected by strong encryption, authentication, and authorization methods. Most vulnerabilities at the server level involve:

- Unauthorized users exploiting weak methods of authentication
- Overly generous user permissions, which allow people to access data that should be restricted, or to make unauthorized changes to the system
- How well the server manages user authentication to ensure only approved people can view sensitive information

Credential data captured from readers and stored in servers should be protected by strong encryption, authentication, and authorization methods.

6

Cybersecurity best practices for access control systems

Access control technology has undergone a huge transformation in recent years. This traditionally proprietary market has now shifted to a more open one. Customers are not always locked in with one provider, and as a result, companies are developing more innovative products and services. These new, more cyber secure, solutions feature end-to-end encryption and advanced authentication, and other features to defend against cyberattacks and malware.

To improve the cybersecurity of your network

- Upgrade your system: older systems were not built to address today's threats
- Use secure, smart, and/or mobile credentials, and the latest communication protocols to secure data sent over the internet
- Provide training to employees to educate them about cybersecurity best practices, and ensure they are often prompted to update passwords
- Use an identity management system to ensure users can only access areas and data that relate to their role and current employee status
- Create separate local networks for devices that store or share highly sensitive information, so that it cannot be accessed from your regular network
- Choose a security provider who can demonstrate compliance with established security control frameworks

Many organizations prefer a hybrid approach, so they can take advantage of the flexibility and scalability of cloud software and data storage options, while also maintaining some locally managed servers.

- Ensure your access control system uses proven data encryption methods as well as multi-step authentication
- Work with a partner that has a dedicated team to monitor cyber threats and ensure software is updated frequently and patched as needed

You don't have to choose between a cloud-based or an on-premises solution. Many organizations prefer a hybrid approach, so they can take advantage of the flexibility and scalability of cloud software and data storage options, while also maintaining some locally managed servers.

7

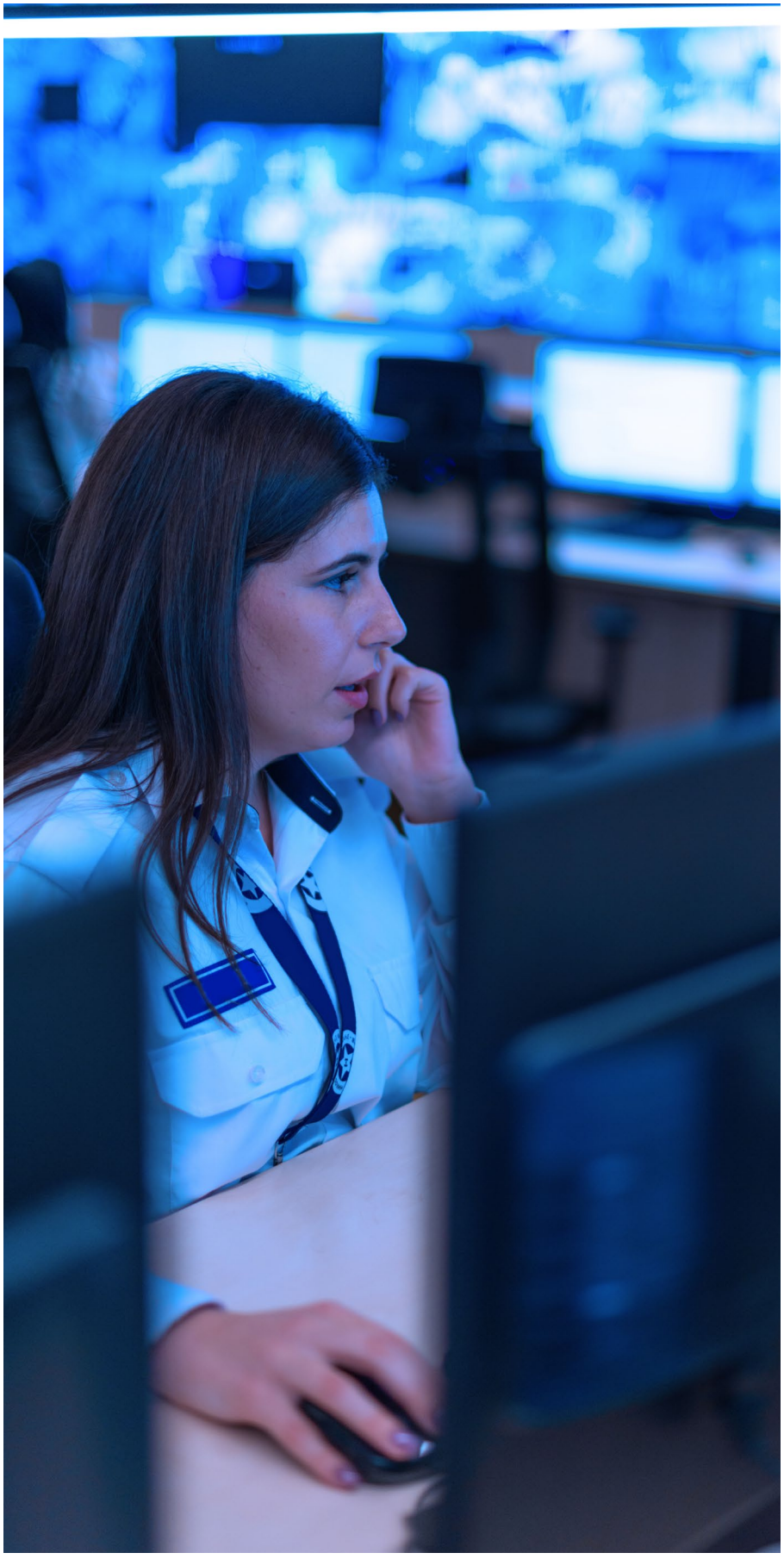
Modern access control systems are more than just cyber secure

A unified access control system that uses the latest cybersecurity standards will secure communications, servers, and data. The Genetec™ Synergis™ access control solution can better protect an organization's assets and people but also help improve business operations and decision-making. By choosing an open architecture IP-based access control system, organizations have the power to upgrade to the latest supported technology at any time, move at their own pace, and work within their available budget.

The Synergis™ access control system uses the latest cybersecurity standards to secure communication, servers, and data at every level of your architecture. With advanced protection from access cards to software, you can manage access to your premises with confidence knowing that prying eyes are kept out.

Genetec™ Security Center is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), comm unications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live.

Security Center is an open architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics.



8

Modern access control systems offer benefits beyond locking and unlocking doors

Newer, and more cyber secure access control systems like Synergis can do much more than just lock and unlock doors on a specific schedule. They can make use of the wealth of data gathered by access control systems and combine this with data from other sources to surface powerful new insights that can help you improve everyday operations as well as security. As a result, the return on investment in these systems is far more impressive.

Synergis goes beyond the door to unlock new insights that help you make better decisions and improve everyday operations. As a truly open system, it connects to a large and growing selection of third-party access control devices. It aggregates and displays data in a dynamic format to empower you to do business smarter.

For example, during the COVID pandemic, Synergis customers were able to quickly and easily install new biometric readers that reduced the need for physical touch[3], so they could limit the spread of germs. They were also able to use access control system data to support contact tracing[4] if an employee tested positive for the virus, as well as to manage occupancy levels and physical distancing requirements[5] mandated by public health authorities.

Access control systems collect a lot of data, but older systems make it difficult to gather and make sense of it. Synergis has dashboards that provide a unified view of all your security systems and sensor data, so you can spot trends and be proactive rather than reactive with operational decisions.

From real-time occupancy management to the monitoring of remote infrastructure, Synergis can help protect your operations – not just your doors.

From real-time occupancy management to the monitoring of remote infrastructure, Synergis can help protect your operations – not just your doors. You can address changing needs by easily adjusting software settings or adding/upgrading hardware, without having to change the whole system. You can use access control data to enable building automation, to turn lights off, for example, or to adjust heating and cooling when people are not present. You can also gain a better understanding of which areas of buildings are used most, so you can tell whether you need that much space.

[3] https://www.genetec.com/podcasts/engage/episode-10-stepping-up-cybersecurity-biometrics-and-multifactor-authentication
[4] https://www.genetec.com/press-center/press-releases/2021/02/genetec-helps-westminster-property-ventures-ensure-safe-return-to-work-for-its-commercial-tenants
[5] https://resources.genetec.com/en-industry-focuses/genetec-occupancy-management-package

9

Conclusion

A unified access control system that uses the latest cybersecurity standards to secure communications, servers, and data such as Security Center Synergis can not only better protect an organization's assets and people but help them improve their business operations and decision-making that go beyond locking and unlocking doors. By choosing an open architecture IP-based access control system, organizations have the power to upgrade to the latest supported technology at any time, move at their own pace, and work within their available budget.

Ready for more?

Download our checklist for the top 7 things you need to consider when migrating to an IP access control system.

Get the checklist

Genetec Inc. is an innovative technology company with a broad solutions portfolio that encompasses 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 and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live. Founded in 1997, and headquartered in Montréal, Canada, Genetec serves its global customers via an extensive network of resellers, integrators, certified channel partners, and consultants in over 159 countries.

Video surveillance: Achieve greater situational awareness and enhance security within your city with the ability to share cameras across agencies and organizations, providing a common operational picture and improving incident response time.

Access control: Heighten your organization's security, effectively respond to threats, and make clearer and timelier decisions with a unified, IP-ready platform, whether deploying a new access control system or updating an existing installation.

Automatic license plate recognition: Automate the detection of vehicles of interest, increase parking enforcement efficiency and accelerate public safety investigations through the ability to share license plate data with selected agencies and partner organizations, without forfeiting ownership and privacy.

Operational decision support: Create efficiency for incident handling and decision making with advanced workflows that guide operators from situation alerts through policy-based procedures to detailed case compilation export.

Investigative case management: Simplify case management and speed up investigations with a platform that allows you to centralize digital evidence and securely collaborate with investigators, outside agencies and the public.

Cloud services: Extend the capabilities of your on-premises security system and reduce IT costs with highly scalable, on-demand cloud services that allow your city to easily cope with rapidly changing security requirements and operate with greater efficiency.

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

UDPT: JAN-26-2024