Make Your ATM Network More Secure

The 7 Shields to Protect the Self-Service Channel

DieboldNixdorf.com

Navigation

- Introduction
- The 7 shields to protect the Self-Service Channel
  - Security Assessments
  - Physical Security
  - Data Security
  - Cyber Security
  - Security Monitoring
  - Processes, Procedures & Compliance
  - Cooperation & Collaboration
- Conclusion

Introduction

Security at the self-service channel is critical: cash, customer data, and financial transactions need to be protected from all sides.

Methods of attack and intensity vary across geographies, but attack patterns are also travelling the globe. They are evolving with worrying speed, and in many cases, grow into a global problem. To ensure security of your entire ecosystem, you must consider every element – from consumers to bank staff, from technicians to cash transport operatives, from hardware deployments to software maintenance – every aspect needs to be included to create a user-friendly and secure self-service ecosystem.

At the same time criminal groups are becoming far more organized, highly specialized and focused on certain attack vectors, specifically for ATMs. They perform intensive preparation and technical research, develop specific toolsets and procedures, create individual infrastructure, and even provide training courses for those who will perform the attack.

Faced with this variety and speed, what steps can you take to secure your self-service channel?

Diebold Nixdorf's commitment to security is ingrained in our DNA. By taking a comprehensive look at the entire self-service ecosystem, our security specialists have identified 7 shields to secure your fleet long-term. Keep reading to find out what they are.

"As a global company with security experts around the world, Diebold Nixdorf has the unique, capabilities and experience needed to provide threat intelligence regarding trends in different areas of the world. We know which countermeasures will be most effective in preventing successful attacks and provide a comprehensive portfolio of security solutions. Methods and tools change at a regular pace as attackers attempt to circumvent controls that are in place. Diebold Nixdorf can help you stay ahead of the trends as they evolve."

– Bernd Redecker, Senior Director, Product & Solution Security, Diebold Nixdorf

[1] *Please note that the measures listed in this document while comprehensive are not intended to be an exhaustive list. Security is a highly dynamic topic with constant development and there may be other steps to take besides the ones listed here.*

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

- Security Assessments
- Physical Security
- Data Security
- Cyber Security
- Security Monitoring
- Processes, Procedures & Compliance
- Cooperation & Collaboration

Conclusion

The **7 Shields** to Protect the Self-Service Channel

Security Assessments

Attack patterns and security technology change and develop quickly. To ensure your self-service channel continues to be secure, conduct regular security assessments to expose weak points.

Physical Security

Using brute force to get to the cash inside the ATM continues to be the weapon of choice for some attackers. There are several measures you can take to protect against this.

Data Security

Some steal the card data and PIN of consumers, so they can then access their victims accounts. You can prevent this by ensuring the privacy of users and using a secure card reader.

Cyber Security

Cyber-attacks have become more common. Securing the communication between components of the ATM and the host as well as preventing unauthorized access to devices and information are effective countermeasures.

Security Monitoring

A quick reaction to an attack can make a decisive difference. The easiest way to ensure this is to closely monitor the self-service fleet to detect possible fraudulent activity in real time.

Process, Procedures & Compliance

Secure and compliant procedures should be implemented throughout an ATM's lifecycle: The development process, the installation, and the day-to-day operation.

Cooperation & Collaboration

Information sharing among all players – financial institutions, law enforcement and ATM manufacturers, software, and service providers – is key to quickly analyze and counteract new security threats.

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

Security Assessments

Physical Security

Data Security

Cyber Security

Security Monitoring

Processes, Procedures & Compliance

Cooperation & Collaboration

Conclusion

Security Assessments

The Risk

We are seeing an increased dynamic in the development and spread of new attack patterns. Financial institutions (FIs) and independent ATM deployers (IADs) have responded with new and expanded security measures. The result is a complex security infrastructure. While you can't avoid complexity, it can be difficult to keep every component up to date. In addition, emerging threat scenarios are another serious concern.

How to keep the shield in place

The first step is to know your status quo. This is the basis to ensure every component of your security strategy is up to date, and to ensure they remain effective against existing and emerging threats. With regular assessments of your security infrastructure, you can identify your weak points and proactively fix them before they are exploited.

But that alone is not enough. You also need to be aware of the threat landscape you operate in, including attack trends. Understanding your own defenses helps you assess new threats. Will they become dangerous to your fleet?

Regular security assessments also help you in building a roadmap. This can help you determine which changes, if any, you need to make to your security infrastructure — both in the short and long term.

Protected by DN

Ensuring your fleet and network are secure is a priority for Diebold Nixdorf. That's why we offer to conduct security assessments. Our experts are aware of ongoing attack trends, both on the global and regional level. They can help you assess the status quo of your fleet. How does your existing security strategy hold up against the risk landscape in your area?

Then they visualize the results in a heatmap[2]. This reveals potential weaknesses in different levels. From high risks that you should address immediately to lower-level risks and those that do not need immediate attention. Our security experts then help you develop a short-, mid-, and long-term strategy, if necessary and requested. This strategy will consist of physical, electronic, and local strategies as well as security procedures.

Schedule your Assesment now

[2] *May vary depending on the region.*

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

- Security Assessments
- Physical Security
- Data Security
- Cyber Security
- Security Monitoring
- Processes, Procedures & Compliance
- Cooperation & Collaboration

Conclusion

Physical Security

The Risk

Physical attacks aim to get direct access to the cash in the ATM. Many are destructive, and include explosions, ramming attacks or ripping the ATM out of the ground. Criminals are both ruthless and relentless in their attacks. Other scenarios are less destructive, but still costly. Yet, the greatest danger is that they can put innocent bystanders in harm's way due to their violent nature.

How to keep the shield in place

Branch design

Security and privacy for consumers, as well as branch staff and third-party operators, should be top of mind in branch design. A secure design can include the placement of pods and teller windows/desks. Generally, moving cash transactions away from the teller to the ATM can improve security. This way cash is no longer handled by people, and they stop being targets.

Detect Attacks

You can make use of sensors to prevent attacks, such as cash trapping or transaction reversal fraud. Both require the installation of a physical trap or manipulation of the cash exit. Once detected – depending on your policies – the ATM can send an alarm or go out of service. This prevents any cash from getting caught in the trap.

Delay Attacks

If an attack takes too long, the risk of capture increases, prompting attackers to give up and flee. The design of the ATM can be a big factor in how long an attack takes. A lack of accessible openings in the safe makes attacks harder and more time consuming. Also, inserting gas or solid explosives into the safe becomes more difficult. Likewise, without any openings in the safe door, ripping it off is also harder. The choice of the right safe for the right level of threat adds another security layer. You can complement these with reinforced steel plates and extra locking mechanisms.

Neutralize The Cash

Another route is to ensure the cash will be unusable to attackers even if they make it into the safe. Ink staining cassettes devalue all bank notes when the ATM detects unauthorized tampering. By advertising that your ATMs are equipped with ink, attacks stop before they begin.

Protected by DN

Providing security from physical attacks depends on the ATM and its components. The DN Series® is the most secure ATM solution DN has ever built:

- DN Series ATMs are more secure by design. The pathway for bank notes from the top to the safe is in the middle of the device. This makes it almost impossible for criminals to gain access to the safe. Additionally, we offer various levels of safes, ranging from thinner, ultra-light (UL) safes to the resistant CEN IV EX GAS safes. So, you can choose one that is fitting for the risk landscape you operate in. Learn More.
- For an even stronger protection we have developed the Chassis- and Safe Enforcer packages. These consist of added steel plates, locking mechanisms and cable hole caps that prevent unauthorized access to the inside of the ATM. Learn More.
- Additionally, you can equip our DN Series ATMs with our Anti-Cash Trapping Solution: built-in sensors can detect cash traps and secure the cash if a trap is detected during a transaction. Additionally, the device can detect shutter drillings related to Transaction Reversal Fraud attacks. Learn More.
- All cassettes used in the DN Series are also ready to be equipped with inking solutions.

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

- Security Assessments
- Physical Security
- Data Security
- Cyber Security
- Security Monitoring
- Processes, Procedures & Compliance
- Cooperation & Collaboration

Conclusion

Data Security

The Risk

Data attacks continue. In these, criminals add electronic devices somewhere at the ATM. One is often on the card reader to capture card data. Meanwhile, a camera directed on the PIN pad records the user's PIN. Some of these devices are tiny, making them challenging to spot. Skimming is the largest threat in this category. Other examples for data attacks include shimming, or eavesdropping attacks. These attacks can cost up to $350,000. But the damage to your brand reputation and loss of trust can be much worse.

How to keep the shield in place

Privacy features

You can improve privacy to prevent criminals from gaining consumers' data. Examples are security mirrors and environmental cameras that help users survey their surroundings. That way they can spot people trying to spy over their shoulder. Display filters and privacy wings on the ATM and on the encrypted PIN pad also make it harder for criminals to see a users' PIN.

The card reader

The design of the card reader is essential. By limiting space within, you can prevent the installation of a second reading device. Meanwhile, a physical barrier in areas where sensitive information could be tapped can prevent eavesdropping attacks. Apart from these you can use skimming recognition. These sensors detect internal and external skimmers and can set off an alarm. You should also consider jamming technology, which protects against external skimming and eavesdropping. With anti-phishing defense you can protect against card trapping. The card reader will hold a trapped card with increased force inside the card reader. It can later be released with a software command.

Alternative methods for identification

Use alternative authentication methods. This could be your own mobile app, QR-codes, NFC, or biometrics can also protect against data attacks[3]. You can also use these methods to provide extra layers of authentication.

Use of EMV Chip

Many countries have switched from storing information on a magnetic stripe to an EMV chip. These have seen a considerable drop in the number of skimming attacks. While some FIs still prefer the magstripe, but from a security standpoint, an EMV chip is still the way to go.

Protected by DN

The design of our DN Series ATMs focusses on a secure and private transaction experience. Illuminated privacy wings, a PIN pad shield and display filter protect transactions from prying eyes. Integrated awareness mirrors and a live feed from an environmental camera on the screen aid in the surveillance of the surroundings.

- Additionally, we engineered the most advanced anti-skimming portfolio in the industry. Security Pack 3 and ActivEdge® offer all the above defense measures, making them the most secure solutions in the industry.
- We offer a variety of other authentication methods on our DN Series like a barcode reader, NFC reader, or biometrics (e.g., fingerprint). Additionally, we can enable mobile authentication via pre-staged transactions or QR codes.
- Our Encrypted PIN Pads (EPPs) adhere to the industry's latest standards, such as the PCI Payment Terminal Security standard, to protect user PINs.

[3] *They may still fall prey to other attack scenarios.*

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

Security Assessments

Physical Security

Data Security

Cyber Security

Security Monitoring

Processes, Procedures & Compliance

Cooperation & Collaboration

Conclusion

Cyber Security

The Risk

Cyberattacks aim to gain physical and/or digital access to system and communications data or ATM cash or both. Examples are jackpotting or ransomware attacks as both have become more prevalent. Some attacks are even referred to as cyberwarfare. In the past, the main target was user data. Today, hackers can operate IoT-connected devices to steal valuable assets. So, why connect ATMs at all if the risk is so high? For one thing, the demand for a more connected banking experience is strong. Also, connectivity enables better monitoring and maintenance, increasing ATM performance availability. The added convenience and efficiency are too great to pass up, making effective cyber security even more important.

How to keep the shield in place

Zero-trust

Considering the pace at which new attack vectors develop, new vulnerabilities surface all the time. To combat this, any inherent trust within the ATM network needs to be eliminated. You can do this with explicit verification of users, applications, devices, and network connections. You should apply such zero-trust principles from the time of system start. Where device identities are verified and are carried to all aspects of ATM operations. Reducing the attack surface is another key tenant of a zero-trust approach.

Encryption of data in motion

You should use encryption for the communication between security relevant components. This includes the card reader or the cash handling device and the ATM PC. This protects against eavesdropping on USB communications and the installation of fraudulent components.

Encryption of data at rest

The hard drive should be encrypted to prevent criminals from removing or accessing it. They may attempt this to get the information stored on it, reverse engineer the device's software stack or to boot from an external USB drive and install malicious software on the ATM. Encrypting the hard drive prevents unauthorized access to sensitive data. Once encrypted, unauthorized data cannot be written to the hard disk. Also, the encrypted data from a stolen hard disk cannot be used without the cryptographic keys unique to the ATM.

Sandboxing

Criminals are now also attempting to gain access by infiltrating back-office systems. Such attacks need security software designed and built for self-service environments. These should put in place sandboxing in combination with strict out of the box modular policies. Sandboxing means your software environment isolates specific applications from critical system resources and other programs. An application can then only interact with other software, files, or resources within its sandbox. This ensures the integrity of the runtime environment is upheld, optimizes compliance and minimizes risk. Any application, process or service that is not explicitly allowed, is forbidden.

Protected by DN

Diebold Nixdorf delivers an integrated, multi-layer approach. It protects against customary and evolving attack vectors.

- Trusted device communication (TDC) encrypts the communication between the PC Core and security relevant modules. It comes standard on every DN Series model.
- To defend against unauthorized access, device behavior and malware injection, we offer Vynamic® Security Hard Disk Encryption (HDE). It protects your network from criminals who are trying to connect a USB device to the ATM or tamper with the software itself. Your hard disk will only work when it's inside a single, designated ATM and only when it is connected to all its paired devices. Learn More.
- Vynamic Security Intrusion Protection (IP) utilizes a full-stack security model that provides unparalleled protection and protects your ATMs from known dangers, but also zero-day threats. It operates using sandboxing techniques by establishing a ruleset that goes beyond "what is allowed." It considers "when, where and what" in terms of specific privileges. These controls detect and prevent specific actions that an application or user might take. As such, it upholds the integrity of the runtime environment. Learn More.
- Both HDE and IP solutions are available for you to use by your operations teams, as well as part of our DN AllConnect Security Management Services. By shifting the burden of developing, implementing, and managing the security strategy for your self-service channel to DN, you will enjoy reliable, scalable, and globally standardized managed processes paired with local expertise. Learn More.

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

- Security Assessments
- Physical Security
- Data Security
- Cyber Security
- Security Monitoring
- Processes, Procedures & Compliance
- Cooperation & Collaboration

Conclusion

Security Monitoring

The Risk

A short reaction time is essential to prevent attacks –not only for hit and run attacks, but also where criminals install fraudulent devices and remove them within a short time. In any case, a quick detection of possible threats can limit losses. As such, 24/7 real-time security monitoring can make a real difference.

How to keep the shield in place

Monitoring with cameras is one way to keep track of an ATM, but built-in sensors with intelligent software can detect and track incidents from within and recognize security-related incidents. Sensors can track the doors, vibrations, temperature, safe bolts, and other components. The data is collected, stored, and analyzed based on pre-defined security policies.

Software solutions can identify, log, and correlate unusual behaviors. For example, many cash withdrawals with the same card could signal a jackpotting attack. Advanced applications can even combine information from the ATM and on from inside the branch itself. Based on what processes you define; you can then have the ATM react in different ways: activate a remote camera, take the ATM out of service, trigger an alarm to your security control center and/ or dispatch a security guard.

You can also outsource the security monitoring of your fleet to a trusted third-party vendor. By doing so, you profit from a high degree of automation and expert support 24/7, so you can concentrate on your core business and gain peace of mind.

Protected by DN

Keeping track of every event that happens can be a challenging task. Diebold Nixdorf offers solutions to make it easier for you to manage, or we can take it off your hands.

- The Anomaly Detection Engine (ADE) is a built-in intelligent software. It identifies, logs, and correlates anomalous behavior for fraud analysis. This software comes as a standard on DN Series ATMs.
- Besides its standard alarm board, you can also equip DN Series ATMs with ActivGuard®. This advanced alarm board functions as a security "nerve center. " It features a processor-based design that acts as a central interface for all security devices and sensors at the ATM. It collects and logs critical information and passes it along to an external alarm system or the ATM's host processor. Learn More.
- You can integrate Vynamic View with Diebold Nixdorf's Vynamic Security Suite. Use the Security Manager module as a central monitoring point for receiving events and triggering alerts. Together with the Vynamic View Availability Manager, it can even detect if a device is being compromised by cyber-attacks. It bases this information on event patterns and correlating events. Learn More.
- Some FIs manage their security monitoring in-house, requiring them to have or develop the required capabilities. For those who don't, Diebold Nixdorf offers security monitoring as part of its Security Managed Services. Our state-of-the art monitoring platform detects attacks in real-time. A broad team of experts safeguards the ATM channel of hundreds of FIs from our security operations center.

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

- Security Assessments
- Physical Security
- Data Security
- Cyber Security
- Security Monitoring
- Processes, Procedures & Compliance
- Cooperation & Collaboration

Conclusion

Processes, Procedures & Compliance

The Risk

All processes and procedures should be compliant with industry best practice and global, regional, and national standards. This includes the acquisition of solutions with a high level of security, but also the implementation of proper procedures throughout the solutions lifecycle. Without, the threat of both external and internal fraud increases. A breach – intentional or accidental – could cause financial damages, service interruption, and loss of consumer trust, or the risk of sanctions if you fail an audit.

How to keep the shield in place

Out of the box security

There are items you can include in your policies when purchasing new solutions to ensure higher security later. Ask yourself, what is the development process and are security concerns ingrained in it? Are penetration tests performed by the manufacturer and/or even independent third parties? Does the vendor remove software components that are not needed, to prevent vulnerabilities? Posing these and similar questions can increase a fleet's security from the get-go.

Access protection

Over-permissive services or users and security loopholes in the operating system can create a security risk. Set up appropriate access mechanisms and safeguards. These prevent tampering, data misuse, and unauthorized access. It also ensures that self-service devices run smoothly. Also, service technicians should be equipped with an authorized service solution. With this, only authorized personnel can access and use internal software and functions of the ATM.

Password management

Automate your password management. If you do, the authentication information to log into your ATM's application and BIOS remain secure and trustworthy. This removes the burden of password management from your IT team, so they can then use their time for more critical missions. It also reduces the risk of a security breach and related damages. At the same time, you can address compliance for local Windows administrator passwords. Not to mention the considerable cost decreases compared to a manual password management solution.

Software lifecycle management

You need to protect components and software by installing the latest security patches. This takes constant effort, especially if your network is composed of different makes and models. You'd need

constant testing and deployment capabilities, both to maintain the required levels of compliance and to protect against current and emerging threats. With the correct device administration and maintenance in place, you can simplify these processes, while minimizing the risk of business disruption. Besides standard maintenance cycles, you should also consider establishing a "Fast Track" path. Attacks needing quick response can be addressed immediately, preferably via remote distribution.

Inventory management

An inventory management solution is also key to running your fleet efficiently and securely, ensuring it is high performing and fully compliant. You should be able to collect data remotely and access accurate information in near real time such as software versions, patches installed, hardware configuration and firmware updates for each ATM. The information can be used to ensure that the correct updates are applied to the proper ATMs and provide consistency across the entire self-service network.

Seamless integration of your monitoring tools, support desk and inventory management solution ensures consolidation of all operational data, enabling increased availability, compliance, optimized operations and cost savings. (Continued on next page)

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

- Security Assessments
- Physical Security
- Data Security
- Cyber Security
- Security Monitoring
- Processes, Procedures & Compliance
- Cooperation & Collaboration

Conclusion

Processes, Procedures & Compliance

Protected by DN

To ensure our customers' fleets are compliant and secure, we have put cost-effective processes in place. DN offers a variety of solutions:

- Diebold Nixdorf follows the strategy of Security by Design. This includes stringent security principles. We conduct penetration tests and vulnerability analysis during the development of our solutions. All DN Series devices come with a foundational level security software. This base level protection includes USB whitelisting, OS base hardening, and Windows firewall.
- The CrypTA solution is a user authentication mechanism for the technical service and operations platform (T/SOP). CrypTA is required for every 2nd level service intervention on the ATM to unlock specific service options on the T/SOP. Access to tools, information documents, and specific T/SOP functions is in accordance with the individual's job role and certification level.
- Vynamic Security Access Protection is available for enhanced OS hardening and customization. It reduces the attack surface and reduces the threat potential by blocking keyboard shortcuts and mouse options. Access Protection offers a higher level of security while ensuring fast access via a convenient user interface. Both Vynamic Security Intrusion Protection and Vynamic Security Hard Disk Encryption can – besides protecting against cyber threats – optimize the self-service channel's compliance.
- With Vynamic View BIOS Management ATM deployers can manage and enhance the security of ATM terminals. How? It sets and updates the BIOS passwords. This protects the integrity of the boot process and ensures that no one can boot from removable devices. With it, changing BIOS or UEFI settings without authorization is impossible. Learn More.
- Or outsource this task with DN AllConnect Windows Password Management Services. It is a state-of-the-art, cost-efficient solution. Use it to automate the end-to-end lifecycle management of your local administrator password for each of your self-service devices and stay compliant with PCI-DSS requirements. Learn More.
- Mastering OS security patch distribution can be a challenge. If you prefer managing your software stack in-house, consider Vynamic View Software Manager. It allows the remote deployment of OS security patches and application updates to any device in your network from a central console. Also, it enhances the security of your self-service network. It controls the type and functionality of software distributed and limits access to authorized users. Learn More.
- Or let someone else handle your software lifecycle management with DN AllConnect Software Deployment Services. It uses state-of-the-art deployment tools and controls all the steps of the process. We track all utilities, drivers, and the software stack for each device end-to-end and in real-time. We complete an automated, remote daily check against the desired state of each device and execute adjustments as needed. Learn More.

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

- Security Assessments
- Physical Security
- Data Security
- Cyber Security
- Security Monitoring
- Processes, Procedures & Compliance
- Cooperation & Collaboration

Conclusion

Cooperation & Collaboration

The Risk

How can we combat the fast-paced development of new attack scenarios, or the high level of organization on the side of the attackers? By organizing ourselves. Cooperation among financial institutions, law enforcement and solution providers is essential to combat threats and prevent attacks. Trustful and intense collaboration and close communication is the key. This also means that your CISO or CSO should involve themselves in discussions about the security of your self-service channel. It is more than an operational topic.

How to keep the shield in place

Stay connected. Join local and global security associations to stay up to date on the threat landscape and attack patterns, especially those that may become a threat to your own self-service fleet.

Solution providers may have their own channels of communication to distribute information about risks and suggested updates to both hardware and software, and for you to report incidents. . This may be the result to an attempted attack or an ongoing development or testing efforts to reach the highest possible availability.

Sharing threat intelligence during emergencies is one thing, but you can also benefit from staying connected when there are no imminent threats. You can better inform evaluations of your own security strategy with a wider knowledge base. Also, you can be informed about new security solutions available for your network. As with any technological advancements, being a first mover is an advantage. Especially when security has become a race to stay ahead of attackers.

Protected by DN

The Product & Solution Security (PSS) group is part of information security. It is the department within Diebold Nixdorf responsible for product and solution security. They are also in charge of portfolio security improvement and incident management. Team members are based in the USA, Mexico, Germany, and India. They cooperate with several national and international teams across the globe, such as the European Association for Secure Transactions (EAST), the FBI, Europol, the ATM Security Association and many more.

- PSS activities focus on all Diebold Nixdorf products and solutions: hardware, software, and services. They manage all incidents and monitor new vulnerabilities. They use public communication channels as well as contracted channels, providing intelligence information from the dark net.
- The PSS has two Rapid Response Teams – one in Eurasia and one in the Americas. Experienced security professionals evaluate and manage attacks. Together with the base teams, the PSS team will assess and stabilize the threat, by logically defining post attack steps, help coordinate activities among DN teams, networks, and third-party vendors. In "peace times," the Rapid Response Team will also raise awareness, prepare for future incidents, and evaluate the state of control of self-service fleets. They also share overall recommendations and new security concepts with FIs.
- To facilitate communication with industry peers like authorities or financial institutions, the PSS team has developed Diebold Nixdorf's Global Security Portal (GSP). It provides FIs, third parties and associates with access to information concerning security incidents or fraud events targeting the self-service industry and Diebold Nixdorf's solutions. Sign up now.

Navigation

Introduction

The 7 shields to protect the Self-Service Channel

- Security Assessments
- Physical Security
- Data Security
- Cyber Security
- Security Monitoring
- Processes, Procedures & Compliance
- Cooperation & Collaboration

Conclusion

Conclusion

With a complex and broad risk landscape, taking a holistic and in-depth view of your security environment is essential to protect your assets, consumers, and employees as well as your brand image. Each shield is important to protect your fleet against threats from different directions and on different levels. If only one of them is vulnerable, criminals might take it as an opportunity to attack.

For Diebold Nixdorf, security is an integral part of our DNA. As a hardware manufacturer, software developer and solution and service provider with years of experience and a global network, we are expertly positioned to offer a holistic security framework. With our innovative, integrated solutions we can help you secure all layers of your self-service channel or take the task off your hands entirely. We understand that security is never one-size-fits-all, so our solutions are intelligence-driven and targeted to meet your individual requirements, mitigate respective risks, and balance your business' needs.

Get in touch today and start with a complimentary security assessment.