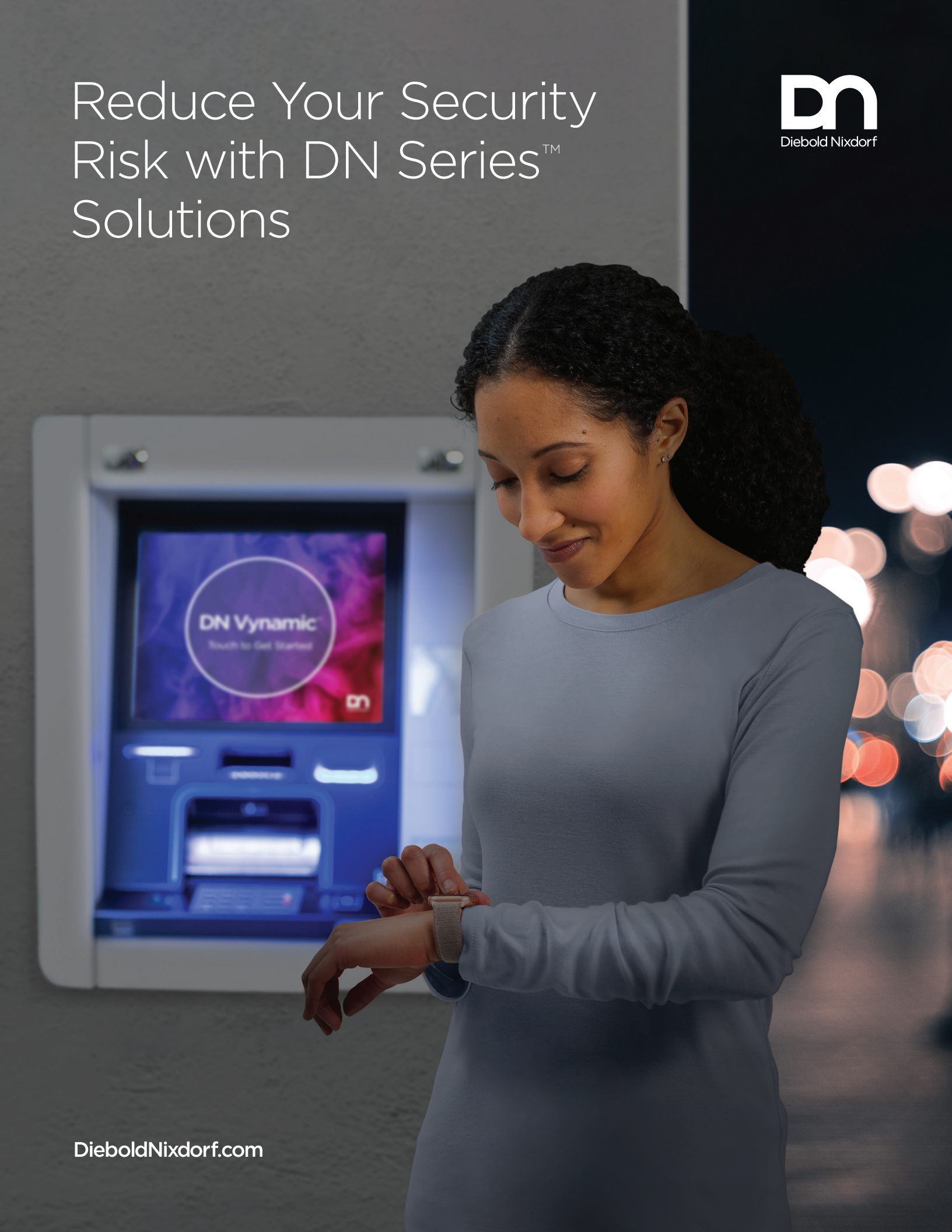
Reduce Your Security Risk with DN Series™ Solutions

Diebold Nixdorf



DieboldNixdorf.com

Security for a Complex World

The emerging self-service threat landscape continues to evolve. The attacks and methods criminals employ vary widely and can be extremely complex as we continue to see threats migrate from one region to another.

At Diebold Nixdorf, we continuously track and investigate reported threats to better understand and adapt solutions to fight emerging attacks in three categories: Cyber, Data and Physical. DN Series was designed to combat these threat vectors with industry-leading innovations that will reduce your ATM fleet's overall security risk.

Global Threat Vectors

	Physical	Data	Cyber
Definition	All fraud and security incidents, aimed at gaining physical access directly to ATM cash	All fraud and security incidents, aimed at gaining physical and/or digital access to card data	All fraud and security incidents, aimed at gaining physical and/or digital access to systems/ communications data and ATM cash
Attack Types	Explosion ATM burglary ATM theft Drilling, Torching, Cutting Cash Trapping Internal Misuse Transaction Reversal Fraud	Skimming Shimming Software Skimming Eavesdropping Card Trapping Shoulder Surfing	Host Spoofing Jackpotting (Malware) Jackpotting (Blackbox) Other Malware (Ransomware) Cloud/Host data breach

For more than 160 years, Diebold Nixdorf has protected people, data and assets.
We understand that security is not one-size-fits-all, so DN Series features intelligence-driven, targeted security solutions that mitigate risks and balance your business needs with your consumers' expectations for privacy.

DN Series was designed with a foundational level of security that comes standard, direct from the factory, with the ability to scale additional protections to accommodate your risk-based strategies and varying deployment environments.

Physical Attacks

WHAT THEY ARE

The majority of physical attacks consist of explosives or ram raids that completely or partially destroy the ATM, making it unusable. Criminals can then gain access to the cash inside.

WHY THEY MATTER

These types of attacks can be extremely costly, as banks must not only replace the destroyed ATM but also deal with additional damage that may have occurred to the surrounding area. Physical attacks also put others in harm's way due to their violent nature.

DN Series physical security is designed in—not just bolted on as an afterthought.

The DN Series Difference:

SECURE SAFE AND NOTE TRANSPORT DESIGN
The note transport path is further back from the cash slot, which makes it almost impossible for criminals to gain access to the safe and insert malicious devices into the safe area.

ANTI-CASH TRAPPING SENSORS
Intelligent sensors can detect when malicious devices are inserted into the cash slot interface.

HARDWARE REINFORCEMENT (CHASSIS AND SAFE ENFORCER)
Chassis Hardening
We added additional strengthened steel chassis plates and fascia locks for improved resistance.

Safe Enforcer
We added cable hole caps and reinforced steel plates for additional strength against prying and gas attacks.

WIDE BREADTH OF SAFE SECURITY LEVELS
Ranging from UL to CEN IV EX GAS

ADVANCED ALARM OPTION
ActivGuard detects and intelligently reports on 12 different input sensors so dispatchers have a better idea of what is happening to the ATM.

INK STAINING CASSETTES
Devalues all cash inside cassettes when sensors detect unauthorized tampering.

RECYCLER MODULE HEAD LOCKING
An additional layer of locking security that only allows authorized personnel to gain access to the recycler's upper module should there be cash inside the escrow or upper compartment.

Reduce the possibility of damaging physical attacks with DN Series. More security features built in, so your self-service terminals are more resilient against traditional attacks.

Data Attacks

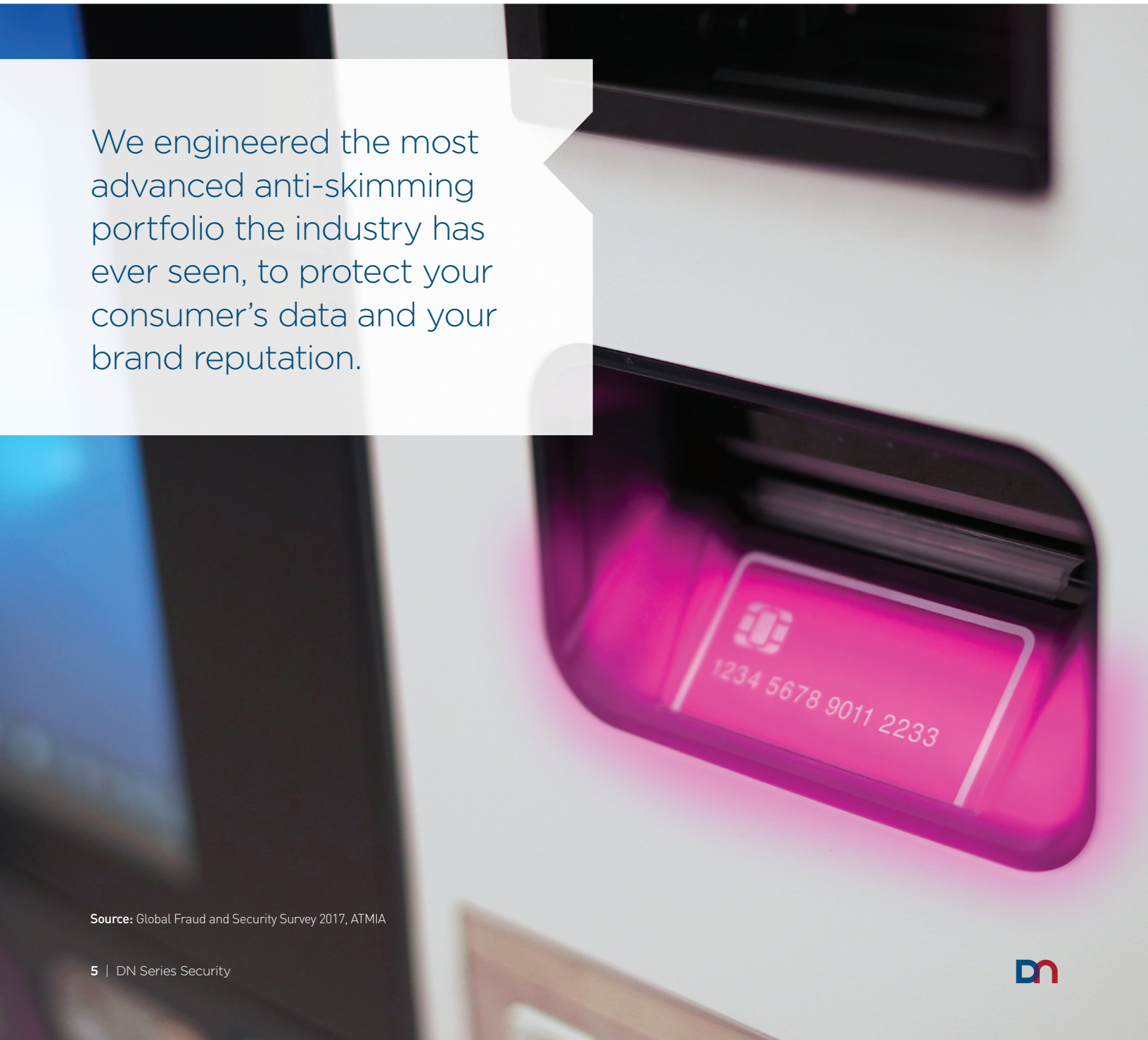
WHAT THEY ARE

Skimming technology continues to get more advanced, making it easier for criminals to steal cardholder data via electronics attached somewhere in the ATM—most commonly on the card reader with additional cameras focused on the PIN pad to gain the user's PIN. Criminals are now able to create a skimmer that is as thin as a piece of paper.

WHY THEY MATTER

Skimming is the largest threat in the Data category. Skimming attacks at the ATM can cost an institution $100,000–$350,000, not counting brand damage and trust lost by consumers toward the institution[1].

We engineered the most advanced anti-skimming portfolio the industry has ever seen, to protect your consumer's data and your brand reputation.



Source: Global Fraud and Security Survey 2017, ATMIA

The DN Series Difference:

ANTI-SKIMMING CARD READERS

Wide solution set of modular, scalable options for skimming security when and where you need it, to fit any deployment environment.

Chip Only	Basic	Advanced	Security Pack 1	Security Pack 2	Security Pack 3	ActivEdge
Removes all magnetic stripe reading capability & only reads chip cards. Reserved for specific countries.	Foundational level security protection — comes standard on every DN Series card reader.	Foundational level protection + intelligent anti-fishing defense	Foundational level protection + intelligent anti-fishing defense + multi-signal jamming	Foundational level protection + intelligent anti-fishing defense + multi-signal jamming + detection	Premium Protection with all security features + encryption and scrambling technology	The industry's most secure card reader with its long-edge design and encrypted moving read head

FOUNDATIONAL SECURITY STANDARD ON ALL CARD READERS

Trusted Device Communication

Encrypted communication that protects against eavesdropping attacks on USB connections and also protects against device substitution.

Anti-tapping defense

Provides a physical barrier on electronic nodes to prevent eavesdropping attacks where sensitive data can be exposed.

Internal space defense

Minimizes void space inside the card reader throat to protect against razor-thin internal skimmers, protecting three times the number of card data tracks versus competitors.

Internal skimming recognition

Prevents the insertion of a razor thin internal skimmer through a software algorithm that recognizes when a device has been placed inside the card reader throat for too long.

EMV compliant

Every card reader is EMV capable even if your network isn't. We're not only future-proofing your fleet if and when you do migrate, but also protecting those who have chip cards from other areas of the world.

IMPROVED DETECTION AND JAMMING TECHNOLOGY

Always-on protection through four multi-signal, random-noise-jamming technology to provide better protection against more advanced, external stereo skimmers

PREMIUM PROTECTION

The highest level of skimming protection in the market with Security Pack 3 and ActivEdge.

EPP V8 WITH PIN PAD PRIVACY SHIELD

Adheres to the industry's latest version of compliance (PCI PTS V5), protecting user's PINs with the latest security standards. With available SHA256 signature or TR-34 certificate remote key loading functionality.

ALTERNATIVE AUTHENTICATION

Mobile, NFC, biometrics. Eliminates the possibility of skimming altogether by adding NFC capability where no magnetic stripe is used. Or, it can provide additional layers of authentication beyond the traditional card and PIN to include biometrics capabilities with a fingerprint reader.

OVERALL DESIGN

Secure and private transaction experience. Cash-over-keyboard design, illuminated privacy wings, awareness mirrors and more.

Don't let a skimmer, shimmer or emerging data threat compromise your fleet. DN Series features world-leading fraud protection, so your consumers feel more secure.

Cyber Attacks

WHAT THEY ARE

Cyber-attacks look to gain access to cash, consumer data, or both. Criminals around the globe have executed jackpotting attacks through which criminals inject malware or, via blackbox attacks, manipulate the ATM software to perform illicit commands.

WHY THEY MATTER

The number of cyber-attacks increased 83% from 2016–2018[2], the largest increase out of any of category.

DN Series solutions offer a host of standard intelligent software to render these attack types and the data inside – should a criminal gain access – useless.

Source: DN proprietary research

The DN Series Difference:

ANOMALY DETECTION ENGINE (ADE)

Built-in intelligent software to identify, log, and correlate anomalous behavior occurring on the ATM for fraud analysis. Examples include:

- An excessive number of cash withdrawals using the same card – signaling a jackpotting attack.
- A user's card is never removed from the card slot – signaling a possible card trapping attack.

CORE COMPUTING SECURITY

Trusted Device Communication (TDC)

- Software that encrypts the communication running on the USB subsystem between the PC Core and security relevant modules. TDC ensures only DN modules and components can be inserted into the ATM, preventing unauthorized devices from being inserted.
- TDC comes standard on every DN Series model, protecting more critical modules than competitors.
- Trusted Platform Module (TPM) serves as the foundation of trust to ensure that only authorized DN modules communicate to one another.

Basic Endpoint Security (BES)

- Foundational level cybersecurity software that provides base-level protection against cyber-attacks. Protections include USB whitelisting, OS base hardening, and Windows firewall. This protection can be uploaded direct in the factory or out in the field. No professional services are needed; just plug and play.

APPLICATION LAYER SECURITY

Vynamic Security Suite

- A comprehensive, advanced, flexible software security suite that was built for the ATM environment and designed in-house. Scale to your unique security needs with the ability to layer one or more offerings. Defends against unauthorized system access, unauthorized system behavior (i.e. jackpotting, etc.) and malware injection.
  - Hard Disk Encryption (HDE)
  - Intrusion Protection (IP)
  - Access Protection (AP)

Vynamic View Security Manager

- When integrated with Vynamic Security, Vynamic View Security Manager enables central management for all events, alerts and activations of new policies.

TRUSTED APPLICATION SOFTWARE

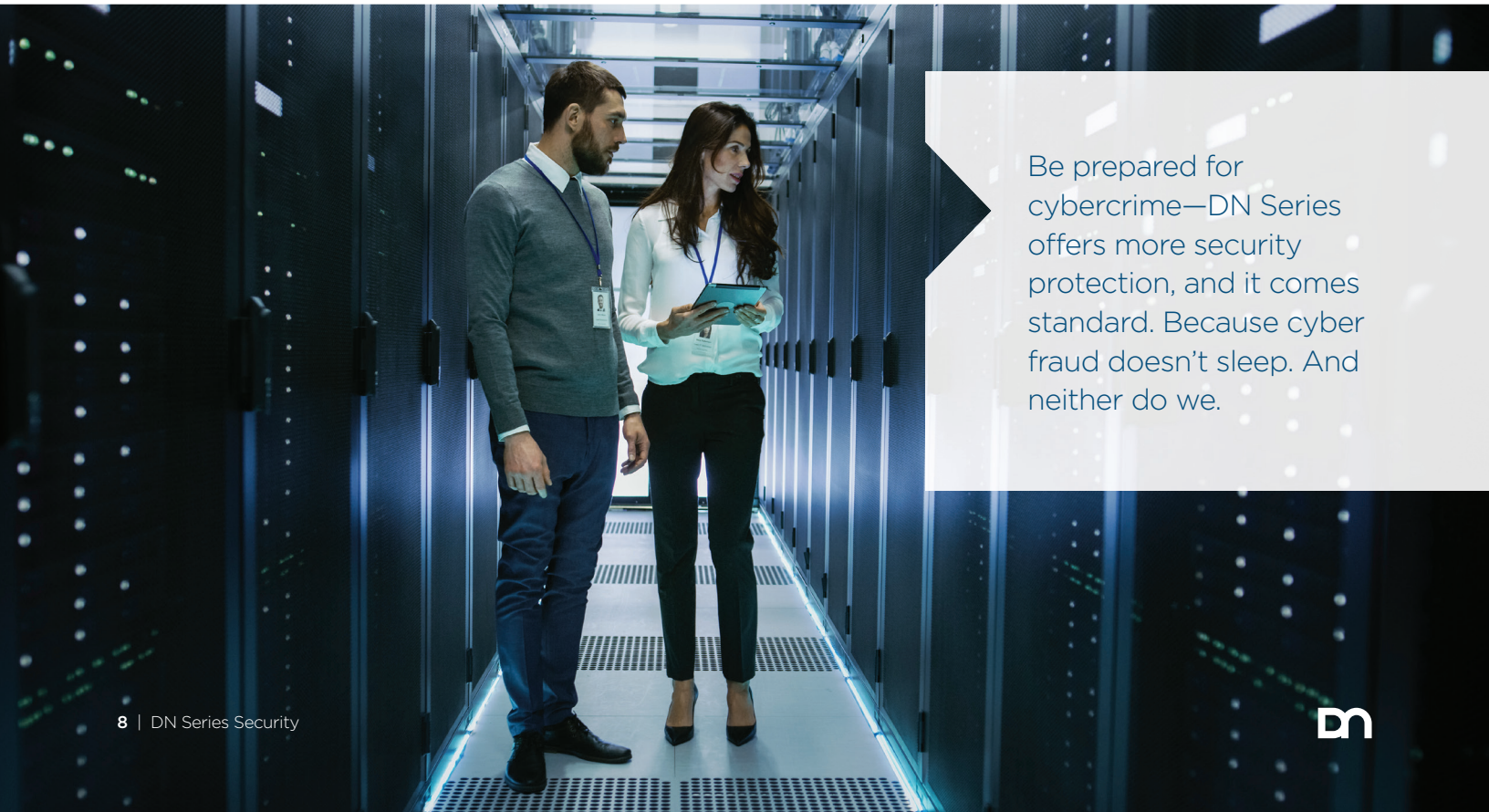
Application software security PCI PA – DSS version 3.2; requires TLS 1.2 + to defeat man in the middle attacks.

AUTHENTIC DN PLATFORM SOFTWARE

Signature validation via Vynamic Security Intrusion Protection.

CRYPTA STICK

Authorized service token (USB) that is inserted into the ATM; ensures that only authorized personnel can access and use internal software and functions.



Be prepared for cybercrime—DN Series offers more security protection, and it comes standard. Because cyber fraud doesn't sleep. And neither do we.

Take ACTion

Our ACTion-based approach to security ensures you have three ironclad pillars of defense.

Analyze

Communicate

Track

DIG IN TO OUR GLOBAL SECURITY PORTAL

Be in the know all the time regarding the latest threats affecting your region. Subscribe to our ACT Global Security Portal so you have visibility you need to ensure your ATMs avoid attacks.

GET SUPPORT FROM DN ALLCONNECT MANAGED SECURITY SERVICES℠

Is security too much for your team to handle alone? Work with experts who can support you as much or as little as you need. Our Managed Security Services allows you to focus on more important items while we take a comprehensive approach to securing your data, channels, and endpoints.

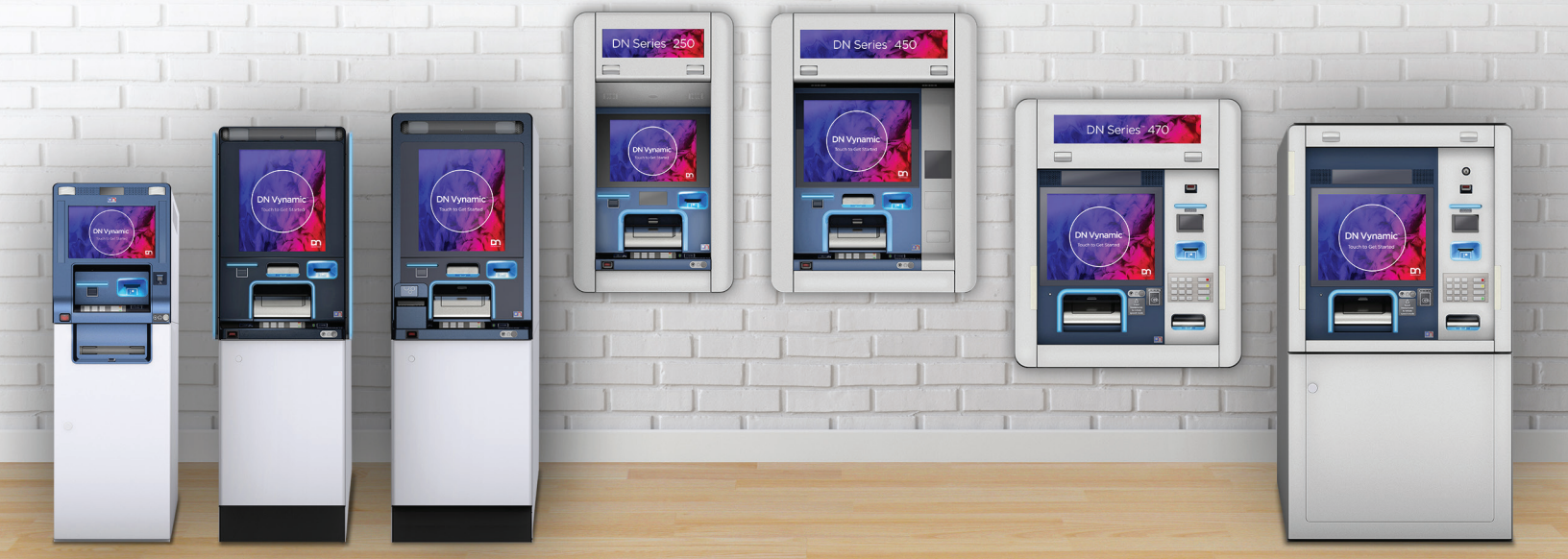
EXPLORE THE BENEFITS OF DN SERIES INNOVATIVE DESIGN

DN Series was designed for a modern, connected world. Learn more about how the DN Series family of self-service solutions can bridge physical and digital channels, automate transactions and enable you to offer your consumers more, all in a secure, compliant environment.

TAKE ADVANTAGE OF OUR BUNDLED SECURITY SOLUTIONS

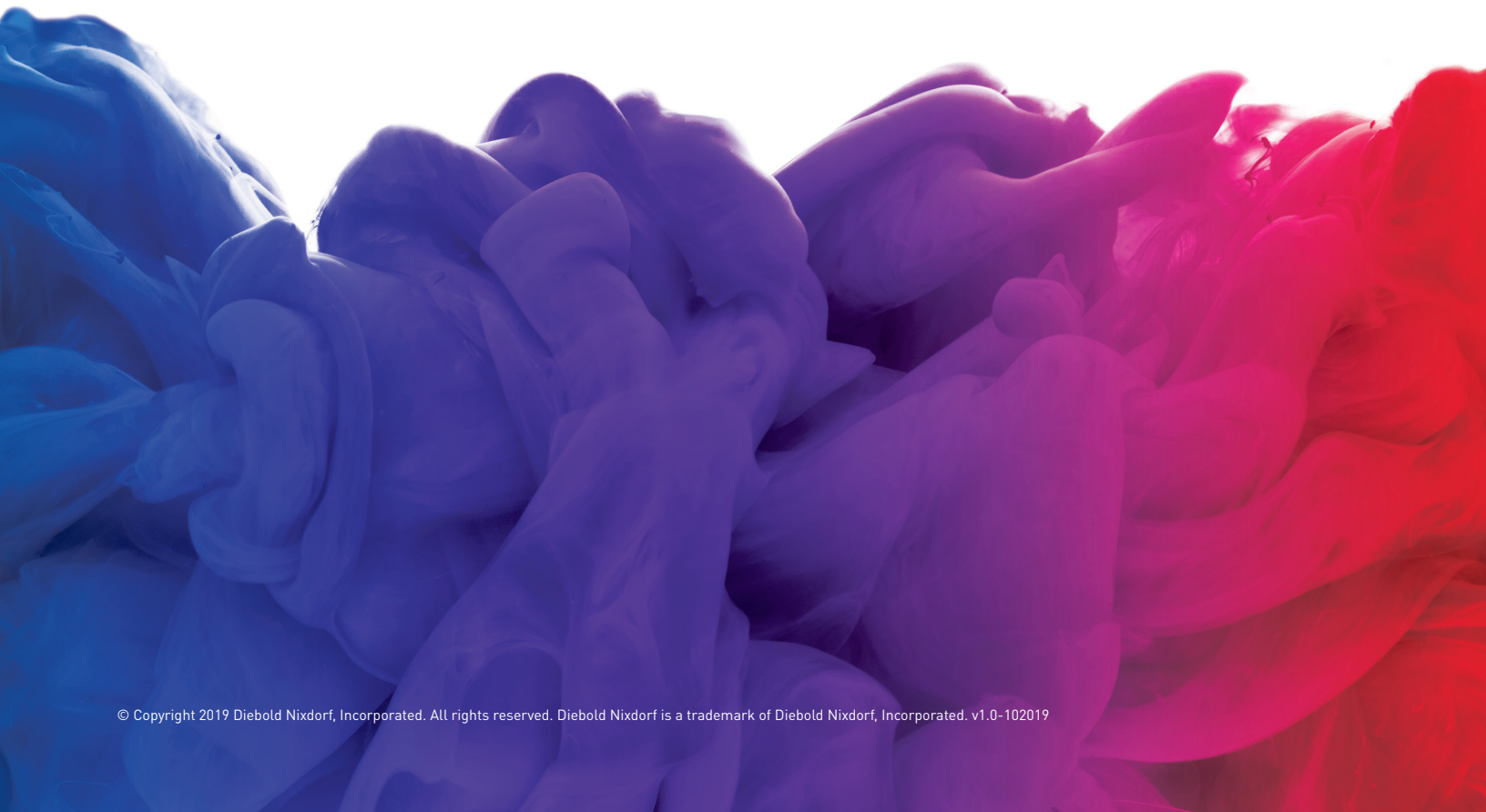
Get more value from DN Series™. Our "MORE SECURE" solution packages feature the flexibility to build a self-service solution that meets your strategic needs. Talk to your sales rep to explore packages and options that fit your needs.

Visit DieboldNixdorf.com/DNseries.



Diebold Nixdorf

DieboldNixdorf.com



© Copyright 2019 Diebold Nixdorf, Incorporated. All rights reserved. Diebold Nixdorf is a trademark of Diebold Nixdorf, Incorporated. v1.0-102019