TRUEFORT™

E-BOOK

Why **MICROSEGMENTATION IS ESSENTIAL** for PCI DSS 4.0 Compliance

+1 201 766 2023 | sales@truefort.com

TRUEFORT.COM

In March 2022, the PCI Security Standards Council released an update to the PCI Data Security Standard (PCI DSS). The regulations apply to all businesses handling payment cards, including any software that stores, processes, or transmits account data, or that could impact the security of account data.

It's the first update since 2018 and addresses the growing challenges of protecting payment card account information in modern data environments. In particular, the new controls around assessment highlight the advantages of segmentation – dividing a network into smaller, more isolated segments, each with its own set of security controls – for any networks in which payment card data may reside.

As organizations consider ways to bring their networks into compliance, they'll find that network segmentation alone no longer suffices. Instead, they should look toward intelligent microsegmentation solutions that help security teams quickly and nimbly implement segmentation strategies, keep the costs and maintenance of compliance down, and provide enhanced protection against breaches and penalties.

PCI DSS 4.0 Stresses the Importance of Segmentation

According to the latest standard, PCI DSS requirements apply to the entire cardholder data environment (CDE) which includes:

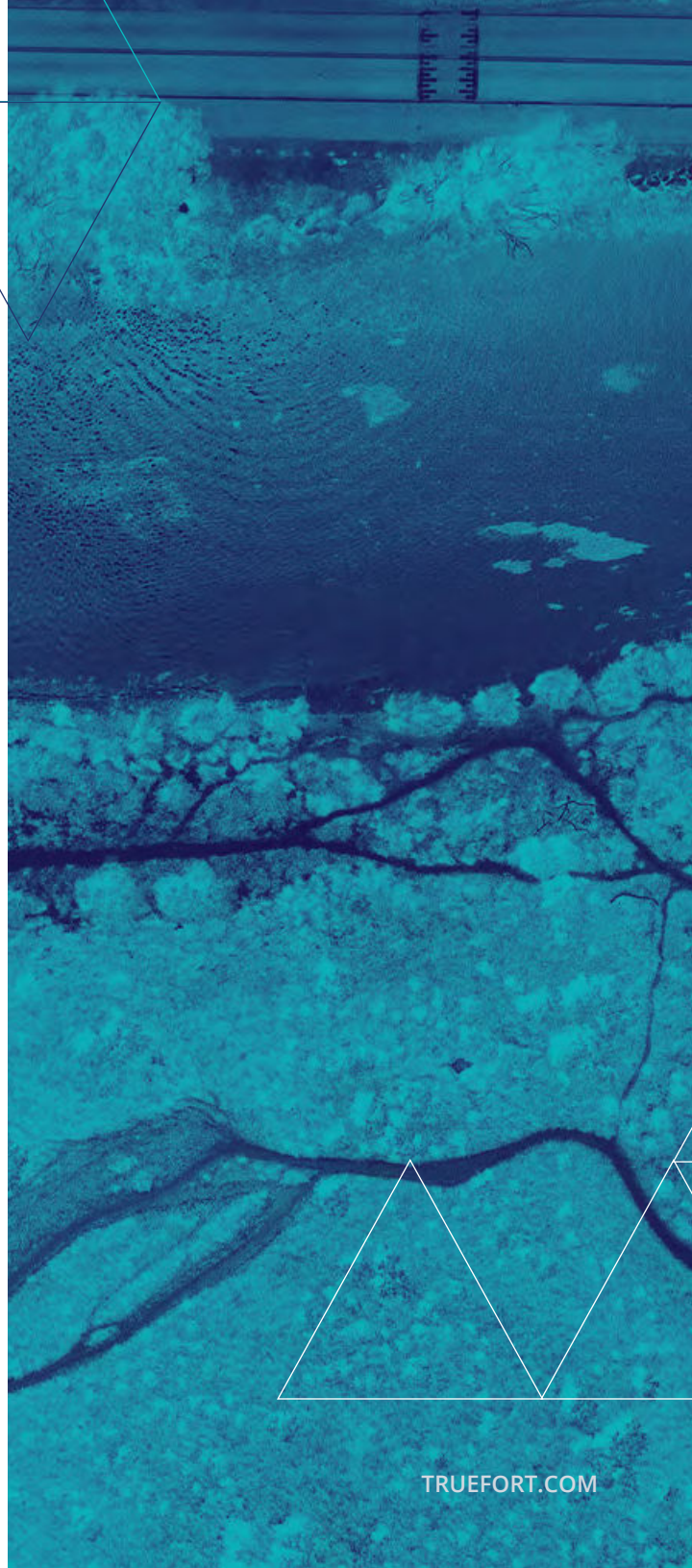
- System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data
- Components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD
- System components, people, and processes that could impact the security of the CDE

Also, based on the standard, any system which is not securely segmented from a system or sub-network that may hold PCI data must adhere to the PCI DSS requirements and must undergo regular assessments to ensure compliance.

The PCI DSS recommends using segmentation to isolate the CDE from the rest of an entity's network to:

- Limit the scope of the PCI DSS assessment
- Reduce the cost of the PCI DSS assessment
- Simplify the implementation and maintenance of PCI DSS controls
- Lower organizational risk of a breach of payment card account data

Using segmentation, organizations who handle payment card account information can clearly delineate the areas of the network which must adhere to the PCI DSS and avoid the work and cost of applying higher security levels to branches of the network that don't need it. However, relying entirely on traditional network segmentation may not provide the cost savings and security posture that merchants and acquiring banks need in today's environment.



E-BOOK

Network Segmentation Struggles to Protect an Increasingly Complex Attack Surface

A modern CDE may span several networks and reach across cloud and on-premise environments. The network segmentation and firewalls that most companies use for protecting data weren't designed for these modern environments and can become cumbersome to maintain at scale. Network segmentation was designed to manage north-south traffic, but most of the data flows east to west in today's CDEs. It's extremely difficult to keep traditional rules-based policies up-to-date, especially when workloads may be ephemeral and may come on- and off-line automatically.

Also, because network segmentation works at the network level and not the workload or application level, it cannot provide visibility into traffic patterns and application dependencies, which is essential for defining the CDE and ensuring least-privileged access for all connection requests within it.

Microsegmentation Offers a Stronger Defense Posture Than Network Segmentation

Microsegmentation is designed specifically for modern networks, which often feature a combination of physical hardware and virtual servers. It's based on application and workload protection which offers the flexibility and visibility security teams need for PCI DSS compliance.

Microsegmentation abstracts security controls from the network, which allows organizations to apply consistent policies across on-premise, cloud-based, and containerized workloads. Security teams can devise fine-grained policies which apply least-privileged access for all systems that need to connect to and within the CDE but exclude those which don't need that level of security. The technology uses workload behavior attributes and runtime context instead of just IP addresses to generate and apply policies across hybrid environments, so security measures are customized for each workload and connection request.

With security customized at the workload level, microsegmentation controls east-west traffic, which helps frustrate attackers and prevents them from jumping from one system to another in search of valuable data. Microsegmentation solutions also provide the visibility needed to map traffic flows, assess connection requests against expected activity, and quickly identify, isolate, and remediate security incidents. As a result, organizations have the ability to apply Zero Trust principles and minimize the attack surface for the CDE.

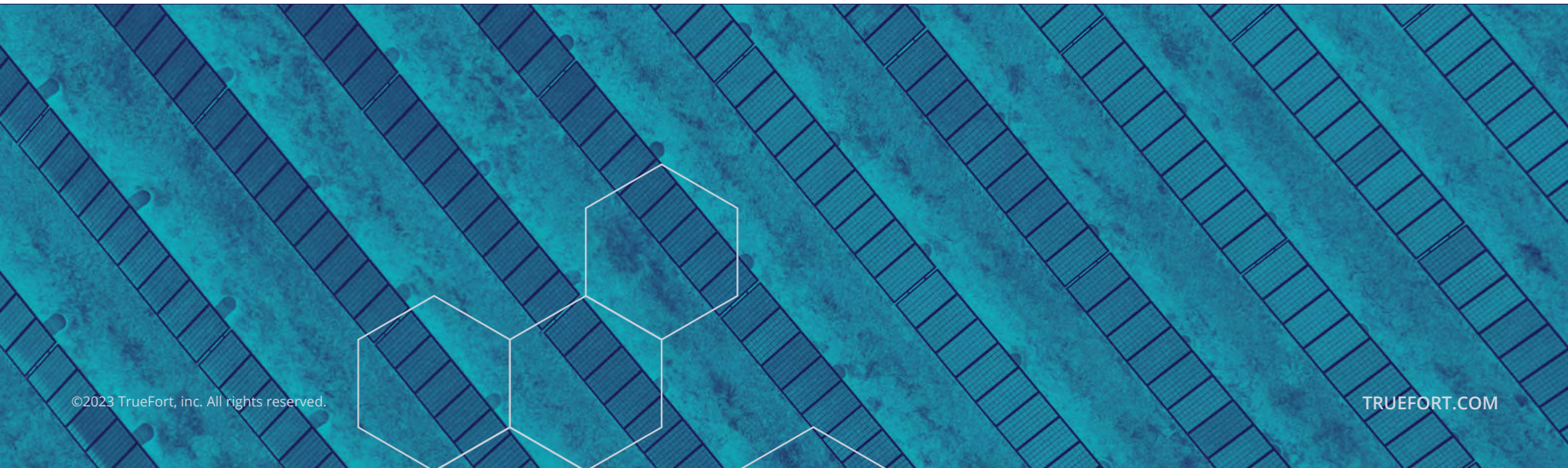
While the PCI DSS doesn't explicitly require a Zero Trust model for merchants and acquiring banks, it does recommend the approach as a good practice for managing user access to resources as stated in Requirements 8.3.9 and 8.3.10, which stipulate that either passwords are changed at least once every 90 days or "the security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly." The dynamic approach, which microsegmentation enables, is easier for technical teams to maintain and less cumbersome for business users.

PCI-DSS Implementation and Assessment May Stress Budgets and Resources

Depending on the size of an organization, reaching and maintaining PCI DSS compliance can cost tens to hundreds of thousands of dollars. Security teams must assess their current level of adherence to the standard and map out steps for implementing required technology and processes.

Depending on the existing security model, technical teams may need to implement additional layers of security, such as data encryption, antivirus software, improved employee training, and PCI DSS-compliant policies. After implementation, teams need the resources and budget to run the certification assessments regularly and maintain their systems going forward.

As part of completing the assessment, organizations also need to conduct penetration testing and have third-party approved scanning vendors (ASVs) scan all possible entry points for vulnerabilities. Finally, security teams need resources for the self-assessment questionnaire (SAQ) and report on compliance (ROC), which payment brands and acquiring banks require along with the attestation of compliance.



E-BOOK

Microsegmentation Reduces the Cost of PCI-DSS Implementation and Assessment

Intelligent microsegmentation solutions help reduce these costs. For example, in defining the CDE, security teams must map the traffic patterns and dependencies between all workloads on the network to isolate those that carry payment card data. This process takes significant time and resources, and it's easy to overlook some vulnerabilities, such as old, unused service accounts, that attackers can exploit.

Intelligent microsegmentation solutions automatically collect application and identity data from network communications to speed discovery of traffic patterns across cloud, hybrid, containerized, or traditional server environments and highlight the dependencies between applications. They also help discover forgotten accounts and close those potential back doors into the network.

The visibility into network activity allows security teams to closely define the CDE, ensuring that PCI DSS assessments cover only systems that store, process, or transmit payment card data and avoiding the cost of implementing highest security standards on network segments that don't require it.

The detailed activity data which microsegmentation solutions provide also makes it easier to collect the information needed to complete assessments, reports, and audits. Microsegmentation also reduces audit expense by reducing scope. Demonstrating baselining and miscrosegmentation reduces the need for costly QSA on-site time. And with centralized traffic information, security teams can more easily manage segmentation policies across diverse environments, lowering maintenance costs in the long-term.

E-BOOK

The Costs and Consequences of Payment Card Data Breaches Run High

For organizations handling payment card data, the consequences of non-compliance are serious and costly. Companies who stray from the standards could face fines and penalties, forensic investigations, lawsuits, and reputational damage. For example, if there's a data breach in a merchant's systems, the payment card brand, such as Visa, investigates the acquiring bank which processes credit card transactions for the vendor. Vendors who are not PCI DSS compliant face stiff penalties.

These breaches may also kick off expensive and time-consuming forensic investigations which require merchants to present all documentation and records related to compliance, and the investigation may result in additional fees, which typically run $5 to $10k per month of non-compliance. On top of everything, if consumers have been affected by the data leak, vendors may be on the hook for restitution running between $50 and $90 per customer.

It's not unusual for these incidents to generate lawsuits which rack up additional expenses in legal and court fees, plus the cost and effort of the discovery phase. And with many customers concerned about the security of their personal data, reputational damage from a breach may affect business revenue long after the security vulnerabilities have been addressed.

Microsegmentation Solutions Lower the Risk of Cardholder Account Data Breach

Considering the potential charges and damage from non-compliance and breaches, companies need security solutions like intelligent microsegmentation that meet PCI standards and go further to provide the most robust protection possible. Teams that implement microsegmentation reduce vulnerabilities, minimize response time, and isolate breaches from lateral movement in the network.

Microsegmentation lowers overall risk because it can generate and apply context-based segmentation policies automatically. These policies are based on analysis of the workload activity rather than a set of rules or rigid framework. They adapt to changing requirements and help teams keep their policies effective and data secure with less work.

With customized security control by application or workload, technical teams can easily apply the most effective policy for each point of traffic flow. And software developers can incorporate security policies early in the development process, lowering the risk of introducing new vulnerabilities via service implementations and upgrades.

To help improve response time, microsegmentation solutions employ machine learning to analyze normal traffic patterns and generate a baseline of expected, authorized activity. Any suspicious behavior breaks the normal pattern and stands out for easy identification and investigation. The traffic baseline also keeps false positive security alerts from distracting and overwhelming response teams. With more detailed visibility and insight into application and workload behavior, security teams identify breaches, isolate them, and remediate any damage faster than with traditional segmentation alone.

If attackers do get past the authentication and authorization, microsegmentation ensures they can't move laterally in the network. Malware may take over one server or application, but it still won't have the authorization to access other workloads. Thus, malicious actors cannot break into the network through one segment and move through the network collecting payment card data as it goes. It gets stuck where security teams can locate and eliminate the threat.

E-BOOK

Microsegmentation Provides Essential Payment Card Protection for Modern Environments

While many security teams may have the best intentions and strong operational policies, if they are relying on technology that wasn't designed to secure today's distributed, hybrid computing environments and agile development processes, they'll have a hard time keeping payment card data secure and avoiding the massive costs of successful attacks. Security teams need technology that can help them reach and maintain compliance by improving their visibility, easing management, and simplifying auditing. Because microsegmentation lowers the cost and effort of securing the CDE, leverages connection data for visibility and automation, and minimizes the overall attack surface, it's an essential strategy for avoiding the destructive consequences of non-compliance and breaches.

About TrueFort

TrueFort provides real-time visibility, application intelligence, and immediate response to acquiring banks, merchants, and any organizations handling payment card data. Over and over, mature businesses have seen traditional security approaches fail in today's threat environment, but TrueFort's technology helps customers quickly and seamlessly implement essential PCI DSS standards with microsegmentation and behavior analytics.

TrueFort speeds microsegmentation deployment and success by leveraging your existing host-based agents.

- Capitalize on existing infrastructure for day-one microsegmentation.
- Leverage deployed EDR agents to secure on-premises, hybrid, and cloud environments.
- Discover and map all intra-application dependencies, workloads, and data flows to closely define the CDE and understand the attack surface.
- Define a trusted baseline of acceptable behavior across workloads and accounts to reduce unauthorized activity and speed investigations and mitigation.
- Ease segmentation policy automation by application and workload profile to minimize attack damage and prevent breaches of payment card data.
- Enforce role-based, process-based, and user-based Zero Trust segmentation to expand the scope of containment capabilities.

To learn how TrueFort can help lower the costs and increase the effectiveness of PCI DSS compliance in your organization, CONTACT US HERE.

TRUEFORT™

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM