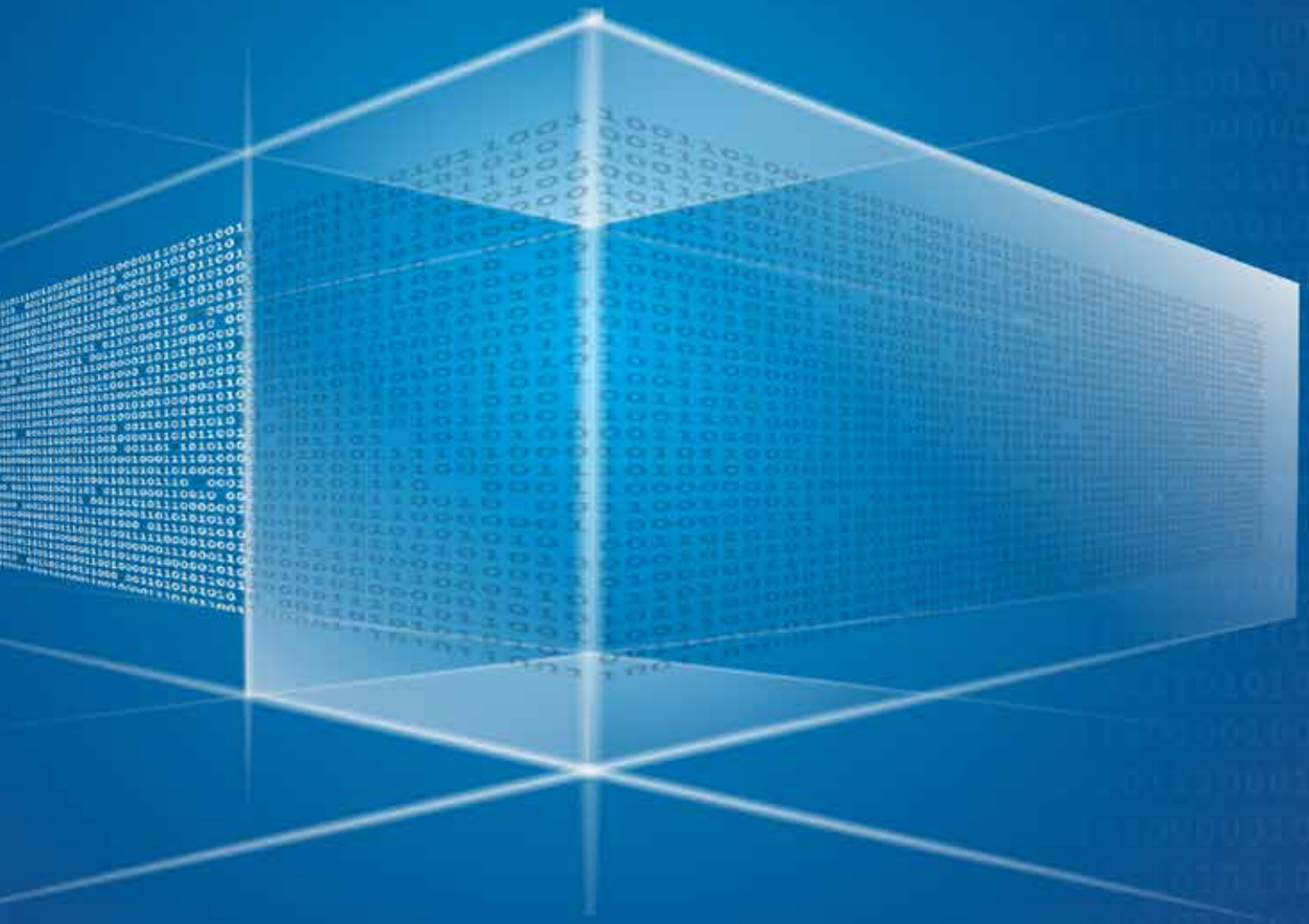
Using Data-Centric Security to Shrink PCI Compliance Scope



A best practices guide to reducing compliance costs while improving security for omnichannel business

CYBEREDGE GROUP

LICENSED BY Hewlett Packard Enterprise

THE CREDIT CARD CONUNDRUM

Accepting credit and debit cards for payment is a necessary—but costly—part of doing business. In addition to processing fees, it can cost a small fortune every year to make sure your business is in compliance with the mandatory Payment Card Industry Data Security Standard (PCI DSS). With the advent of PCI DSS 3.2, merchants have more requirements than ever for complying with PCI regulations.

Adding insult to injury, complying with PCI DSS doesn't necessarily mean you won't get breached. Just ask Target Corporation or any of the many other companies in the news over the past few years, who despite security precautions and PCI compliance, suffered significant breaches.

Unfortunately, moving to all-cash transactions isn't an option, and neither are alternative forms likely to offer much relief as they also present security challenges of their own. In a world where omnichannel business is a top priority for merchants, airlines, insurance companies, and other consumer-facing businesses, credit and debit cards are still the most ubiquitous form of payment across all channels.

That said, now there's a better way to comply with PCI DSS that saves you time, money, and effort—while doing a better job of protecting your data at the same time. Read on for insight into how IT and security professionals can help their companies both shrink their PCI compliance scope and costs, and improve data security across the omnichannel landscape.

54%

Companies in a recent study that experienced an average of four breaches involving payment data in the previous two years

74%

Respondents who say their companies are not fully compliant or only partially compliant with PCI DSS

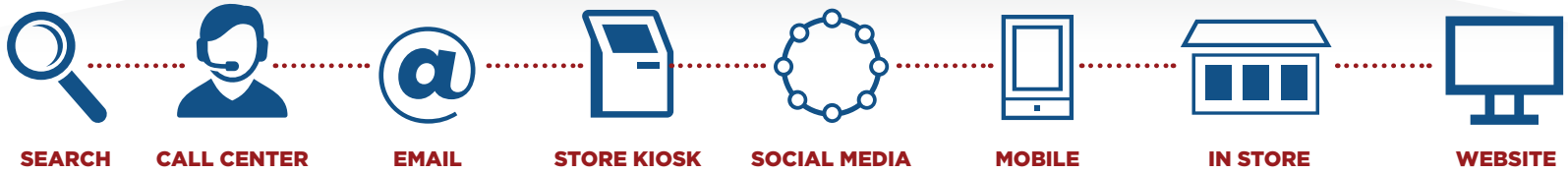
Source: "Global Study on the State of Payment Data Security," Ponemon, 2015.

OMNICHANNEL PAYMENTS = GREATER COMPLIANCE AND SECURITY CHALLENGES

Today's discerning customers want to interact with your brand wherever and whenever they feel it's convenient—whether that's in your brick-and-mortar locations, online from their desktop, or using a mobile device. That's the essence of today's omnichannel merchant strategy.

- **The upside for your business** is that an omnichannel strategy can deliver a more personalized, timely, and seamless customer experience, helping you differentiate your business and build customer loyalty.

- **The downside of omnichannel business** is that it introduces new security and PCI compliance challenges. Protecting sensitive data coming through multiple, various channels requires a more comprehensive payment security and compliance strategy—potentially increasing the cost and complexity for your business.



Don't EMV cards help with PCI compliance?

Named after the original developers (Europay, MasterCard, and Visa), EMV chip technology offers enhanced anti-fraud capabilities compared to magstripe cards at the physical point of sale. However, similar to magnetic strip devices, EMV devices also send clear text card numbers to the point-of-sale system. You still need to protect the card data according to the PCI guidelines.

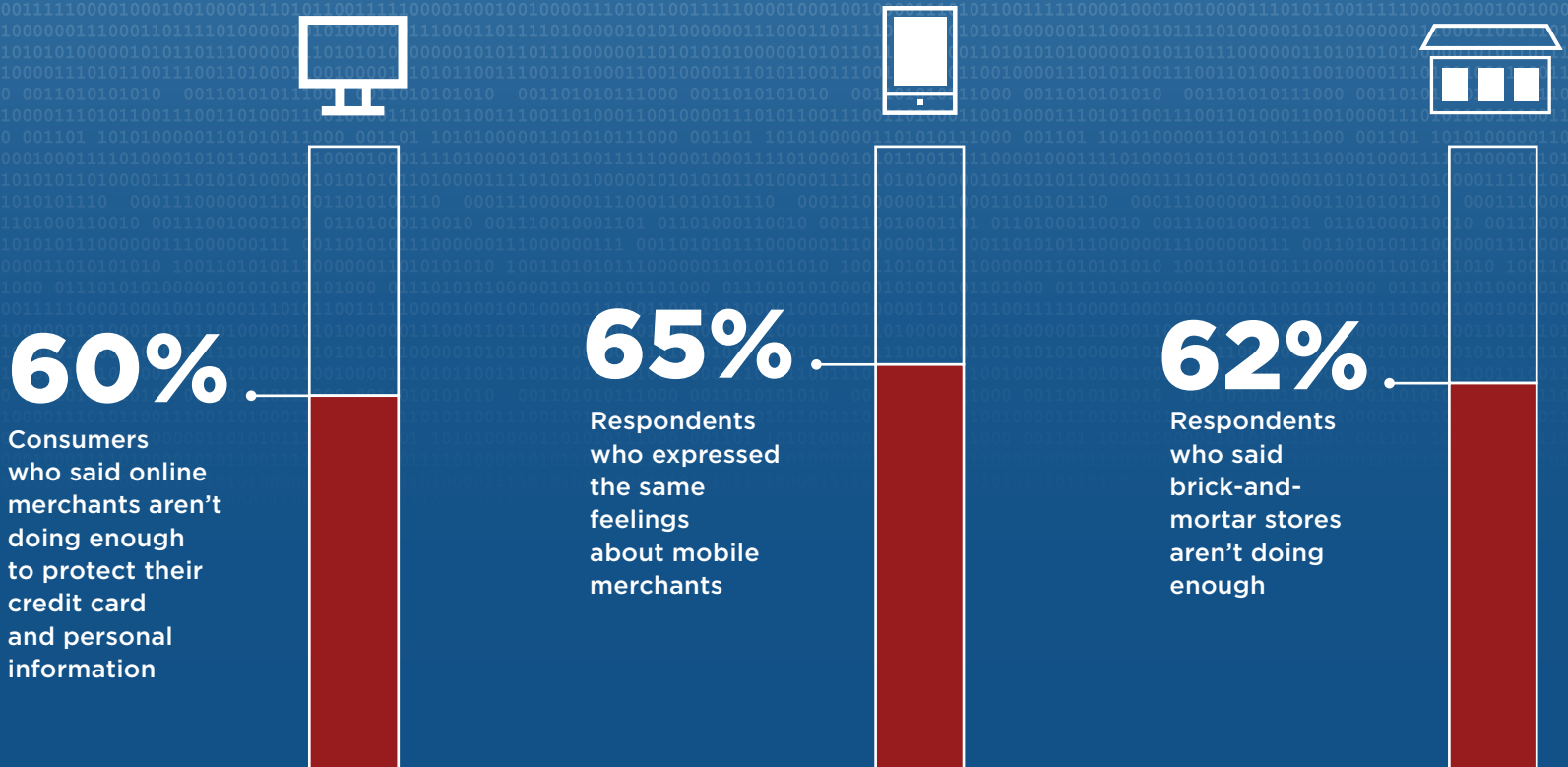
EMV alone doesn't satisfy PCI requirements nor does it reduce PCI scope. While it protects against counterfeit card fraud, it does not protect against malware and hacking, which aim to steal primary account number data between the card reader and point-of-sale device or from other security gaps in the payment ecosystem.

MINIMIZING COMPLIANCE EFFORT AND COST

We can all agree that the goal of PCI DSS—to protect both cardholders and merchants from the damaging effects of data breaches and theft—is a highly beneficial one. However, with more than 300 controls to address, the effort to comply is significant for businesses of all sizes, especially those adopting an omnichannel strategy.

An industry-accepted best practice to help reduce the cost and effort of compliance is to shrink the scope of PCI compliance—that is, the parts of your business that must comply with the PCI DSS standard. Essentially, the scope includes whatever falls within the cardholder data environment (CDE), which includes systems that process, store, and/or transmit cardholder data.

Logically, keeping the CDE as small as possible—by minimizing the systems and technology that touch cardholder data—shrinks the size of the compliance and audit effort, in turn reducing cost and complexity. The question is how best to shrink the CDE, especially given multiple channels of sale?



60%

Consumers who said online merchants aren't doing enough to protect their credit card and personal information

65%

Respondents who expressed the same feelings about mobile merchants

62%

Respondents who said brick-and-mortar stores aren't doing enough

Source: "Bizrate Insights Payment Security Study #2," February 3, 2015.

SHRINKING SCOPE WITH TOKENIZATION

Industry experts and the PCI Security Standards Council recommend using a technology called tokenization to reduce the scope for PCI audits, thereby reducing your business's cost and effort.

What is tokenization?

Tokenization uses random tokens to replace sensitive data to mitigate the chance that cyberthieves can monetize the data if they are able to steal it.

How does it reduce scope?

A token comprises random digits that cannot be derived back to the original value, so systems interacting with the tokenized data can process payments without ever processing, storing, or transmitting live cardholder data. Therefore, those systems can remain out of audit scope for PCI compliance.

Is tokenization an elegant solution to PCI compliance woes? The short answer is yes, it can be. However, most traditional and homegrown database-centric tokenization solutions have major drawbacks:

- **Large database to manage**
  Traditional tokenization solutions require a token vault, a database that stores primary account numbers together with randomly generated tokens. If you store data for one million credit cards, then you have one million tokens to manage. As you can imagine, this becomes cumbersome and expensive.
- **Additional PCI audit scope**
  Because it contains account numbers, the token database itself becomes a high-value target for cyberthieves and actually adds to your PCI audit scope, negating some of the reduction you achieve from tokenization.
- **High costs and efforts**
  For traditional tokenization solutions, you need corresponding hardware, software, and IT processes to continually protect the token database and replicate or back up cryptographic keys from site to site.
- **Failures or inaccuracies**
  Replication delays can mean that sometimes two tokens are generated for the same card number, resulting in failures or inaccuracies in applications such as loyalty and marketing systems, or fraud analytics.

A BETTER SOLUTION FOR REDUCING SCOPE

Unlike conventional, first-generation tokenization solutions, a data-centric solution—as opposed to database-centric—with secure, stateless tokenization reduces PCI scope, closes security gaps, secures omnichannel payments, and enables greater scalability and flexibility.

Why data-centric?

With a data-centric security approach, the data is protected so that it can move between applications and devices without creating security gaps and without requiring changes to existing processes and the user experience.

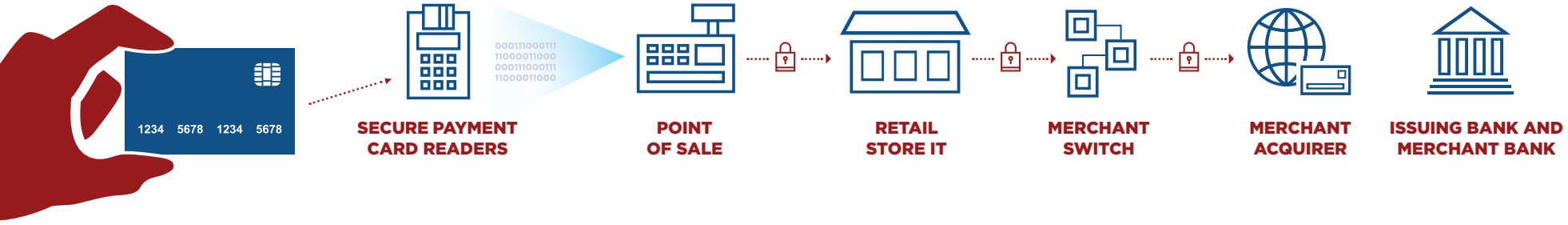
Why stateless?

Stateless technology eliminates the token database and removes the storage of card data from the solution. This dramatically improves speed, scalability, security, and manageability compared to conventional tokenization solutions.

How does it work?

Secure stateless tokenization uses a set of static, pre-generated tables containing random numbers created using a FIPS random number generator. These static tables are used to consistently produce a unique, random token for each clear text primary account number (PAN) input, resulting in a token that has no relationship to the original PAN. No token database is required. The PCI DSS guidelines consider systems that only hold tokens to be out of audit scope, greatly reducing audit costs.

Once the card is processed, **tokenization** replaces the live card data after authorization



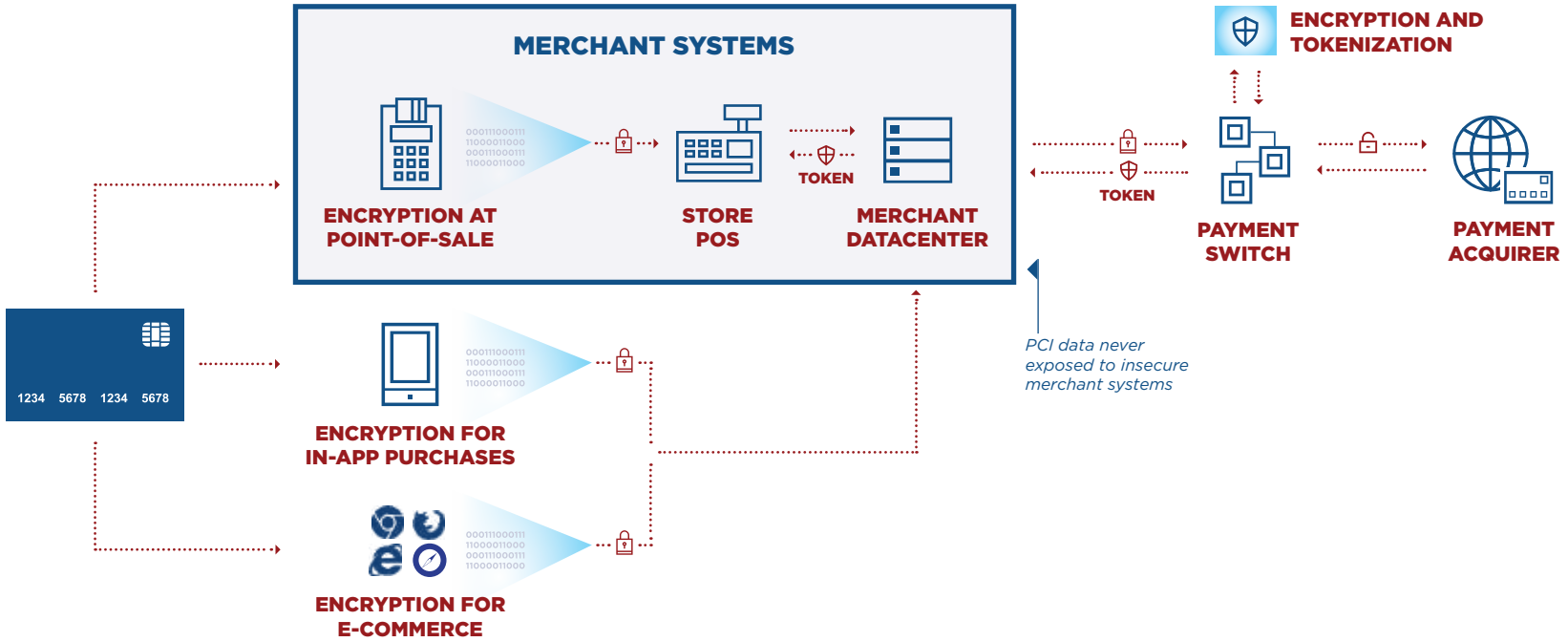
> **Secure Stateless Tokenization represents a paradigm shift in tokenization. It provides service at higher performance and with greater security than conventional, database-centric solutions ...**
>
> — Coalfire, a leading independent IT governance, risk, and compliance firm

SUPPORTING OMNICHANNEL WITH END-TO-END, DATA-CENTRIC SECURITY

While secure, stateless tokenization protects card data and reduces PCI scope, for other sensitive data such as customer name, birth date, and email address, encryption is the gold standard.

To derive maximum value and protection while requiring the least amount of effort and change, you should choose a solution that uses format-preserving encryption. With this type of encryption, a standards-based (U.S. Government National Institute of Standards) method is used to encrypt data in a way that does not alter the data format, meaning that the encrypted value has the same size and format as the original data. This results in little to no change being required for databases and applications that utilize the data. You should also look for a solution that maintains referential integrity, i.e. stores consistent values across different databases, without the need for an application-specific reference database.

Finally, to protect sensitive data in an omnichannel environment, you should choose a data-centric solution that can secure sensitive payment data from the moment of the transaction—whether online, from a mobile device, or a card-swipe device in a store—all the way through to the back end.



MAXIMIZE DATA PROTECTION AND RETURN ON INVESTMENT

An end-to-end data-centric security solution that includes secure stateless tokenization and format-preserving encryption can significantly reduce PCI scope while improving data security. Beyond reducing scope, choosing the right solution can help your business:

- **"Kill the data":** PCI compliance isn't a guarantee that your environment can't be breached. To protect your company and customers, you should choose a solution that renders the data unusable if stolen from your environment—essentially "killing the data" (term originally coined by John Kindervag of Forrester) through encryption or tokenization.
- **Expand protection beyond PCI:** Choosing a unified security solution helps your business secure multiple sales channels and situations using one platform. This eliminates gaps and improves data protection beyond the scope of PCI compliance, enabling you to apply the solution to meet other regulatory or business security challenges. Look for a solution that can also protect other sensitive data types, such as personally identifiable information (PII) and protected health information (PHI), as well as PCI data, and will work across the enterprise, securing sensitive data on multiple platforms and environments.
- **Adapt to changing requirements:** When you choose a solution where your applications and systems don't have to change every time compliance requirements change, you can adapt and comply more quickly and easily.
- **Support omnichannel payments:** Having the same solution with end-to-end protection across sales channels, applications, and devices reduces gaps in protection and improves your security posture.

FROM THE SPONSOR: HPE SECURITY—DATA SECURITY

HPE Security—Data Security provides best-in-class data encryption and tokenization for structured and unstructured data and enables cost-effective PCI compliance, scope reduction, data privacy, and secure analytics. Relied on by leading enterprises worldwide, HPE Security—Data Security solutions reduce risk and protect your brand while enabling business.

The HPE SecureData product family provides a comprehensive, data-centric approach proven to reduce PCI DSS scope by up to 80% and cut compliance costs by up to 95%.

HPE Secure Stateless Tokenization (SST) is an advanced, patented, proven data security technology—stateless because it eliminates the token database that is central to other tokenization solutions and removes the need to store cardholder data. Eliminating the token database significantly improves the speed, scalability, security, and manageability of the tokenization process. Every application handling the tokenized data, including back-end applications such as fraud analysis and loyalty programs, may be removed from PCI audit scope.

HPE SecureData Payments provides complete point-to-point encryption and tokenization for retail payment transactions, enabling PCI scope reduction. By protecting the data itself, HPE SecureData Payments eliminates security gaps that exist between networks, databases, and applications. HPE SecureData Payments protects data-at-rest, in-use, and in-motion, securing sensitive data point-to-point.

HPE SecureData Web protects payment data captured at the browser, from the point customers enter their cardholder information or personal data, and keeps it protected all the way through the web, applications, cloud infrastructure, and upstream IT systems and networks to the trusted host destination.

HPE SecureData Mobile provides security at data capture on the mobile endpoint. HPE SecureData Mobile enables end-to-end sensitive data protection from native mobile iOS/Android applications through the entire enterprise data lifecycle and payment data stream. Data is protected anywhere it moves, anywhere it resides, and however it is used.

Relied on by industry leaders around the world

HPE SecureData products and unique technology are used by 7 of 9 top payment acquirers, as well as top global credit card brands, top retailers around the world, card issuers, banks, and service providers.

REGIONAL AIR CARRIER CUTS COMPLIANCE COSTS

Challenge

A growing regional air carrier—which describes itself as an "e-commerce business with airline attached"—needed a way to protect its customer data and achieve PCI compliance at both level-1 and level-2 classifications. The airline accepts customer credit card information at several points:

Ticket purchases online

Through its call center

At ticket counters

Through a branded mobile application for customers using smartphones

In-flight for refreshment purchases using mobile devices

It also retains customer payment and passport information for future expedited checkout and to process refunds.

Solution

The airline deployed an HPE SecureData solution across the entire company. The comprehensive solution can be easily extended as volume grows or requirements evolve and includes: HPE Secure Stateless Tokenization, HPE Format-Preserving Encryption, and HPE Page-Integrated Encryption.

Results

- Radical PCI audit scope reduction
- Reduction of compliance cost and complexity
- Superior performance and system stability
- Simplicity, low cost, and comprehensive set of functionality
- Significantly improved overall security profile

About HPE Security—Data Security

HPE Security—Data Security, is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption, tokenization and key management solutions, enabling our customers to effectively combat new and emerging security threats. Our powerful data protection solutions allow any company to seamlessly secure all types of sensitive corporate and customer information, wherever it resides, while efficiently meeting regulatory compliance and privacy requirements.

About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our highly experienced consultants have in-depth technical expertise in dozens of IT security technologies, including:

- Advanced Threat Protection (ATP)
- Application Security
- Authentication, Authorization, and Auditing (AAA)
- Cloud Security
- Data Protection, Encryption, and Tokenization
- DoS/DDoS Protection
- Endpoint Security
- Enterprise Mobility Management (EMM)
- Intrusion Prevention Systems (IPS)
- Network Behavior Analysis (NBA)
- Network Forensics
- Next-Generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Identity Management (PIM)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information & Event Management (SIEM)
- Virtualization Security
- Vulnerability Management (VM)