PCI COMPLIANCE:
RISKS THAT FINANCIAL INSTITUTIONS CAN'T AFFORD
TO IGNORE

UNISYS

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance security of cardholder data. All members of the payment card industry (financial institutions, credit card companies, and merchants) are expected to comply with the standard. As per PCI, the payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations.

By complying with PCI DSS, financial institutions (FIs) can significantly decrease their risk of data breach that could seriously hurt their business brand and reputation. Data breach can cause a cascade of cancelled accounts, severed customer relationships, high-stakes lawsuits, and expensive fines and sanctions by individual payment brands.

PCI DSS compliance can be a complex, time-consuming, and disruptive process and can introduce ongoing costs with audits and continuous compliance assessments. So, reducing the scope of audit while providing end-to-end data protection can significantly reduce the complexity and costs associated with meeting and maintaining PCI DSS compliance.

Unisys Stealth™ is an innovative software-based, micro-segmentation, cryptographic solution that can:

- securely segregate environments, workstations, applications, databases, and networks
- considerably reduce the scope of environments being assessed for PCI DSS compliance
- effectively safeguard critical and confidential assets

UNISYS APPROACH TO PCI SCOPE REDUCTION

PCI Audit Scope
Without Stealth

Figure 1

PCI Audit Scope
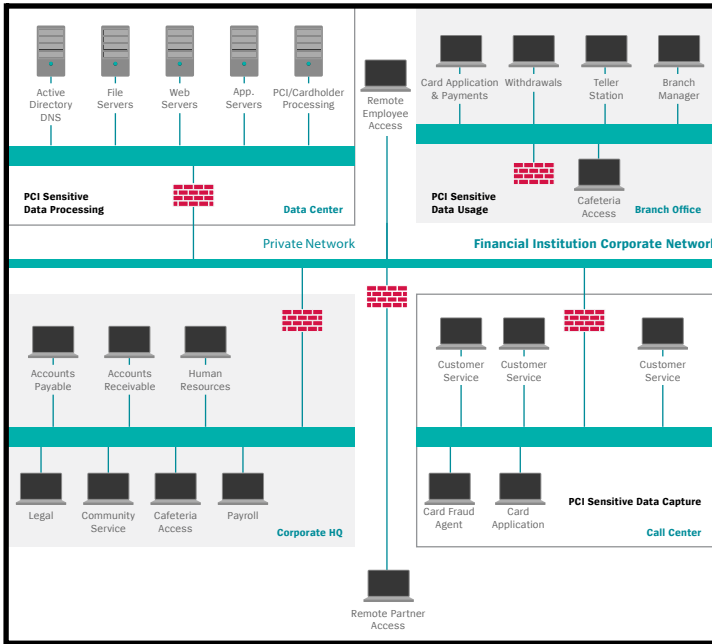### Micro-segmentation with Stealth

Figure 2

Figure 1 shows all the areas where cardholder data are captured, stored, and transmitted, and the entire network is in the audit scope for PCI DSS compliance. The scope extends to mobile phones, Internet, and email, as employees could theoretically use these tools to transmit cardholder data out of the environment.
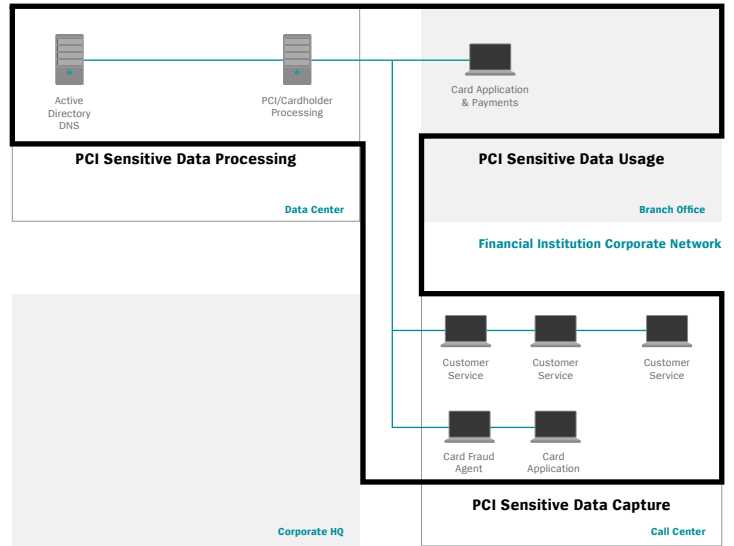
Figure 2 shows how micro-segmentation allows FIs to simplify the complexity of PCI scope and reduce the cost of an audit.

Stealth can isolate the PCI environment from the scope of audit due to the assessed environment being smaller. It offers an innovative approach that has been assessed by teams of security experts. The overall assessment findings validate that with proper deployment in today's threat landscape, Stealth offers tremendous value to IT functions on several fronts.

- First, Stealth delivers functionality that effectively covers a range of required PCI controls. This reduces the security application footprint so that there are fewer products to purchase and administer.
- Second, Stealth is integrated with enterprise directories, enabling it to be updated dynamically and eliminating the need for constant reconfiguration and administration. The elimination of administration activities reduces the chance of manual error.
- Finally, the granular access control removes the requirement for traditional physical and logical segmentation to be continually maintained, further reducing time, effort, and margin of error in the IT management cycle.

Serving more than half of the world's top 25 banks and 10 of the world's leading insurance companies, complemented with 40+ years in security excellence, Unisys understands the importance of PCI compliance to maintain the security posture of your organization.

Write to us at stealth@unisys.com and one of our representatives will answer your questions and set you on the path to PCI compliance. For more information, visit: www.unisys.com/ms/pci-compliance

About Unisys

Unisys is a global information technology company that works with many of the world's largest companies and government organizations to solve their most pressing IT and business challenges. Unisys specializes in providing integrated, leading-edge solutions to clients in the government, financial services and commercial markets. With more than 20,000 employees serving clients around the world, Unisys offerings include cloud and infrastructure services, application services, security solutions, and high-end server technology.

Printed in the United States of America   11/15