wontok™
SafeCentral
SafeDesktop

Safe, secure transactions
for banks and their customers

Stops account takeover fraud

Financial institutions and their customers are under constant attack from organized crime.

> *"Most cyberattacks are indiscriminate and motived by greed—not revenge or public service. Most attackers are out to steal your data because of what it's worth, not who you are. Anything that can be converted to money will do."* Source: Data Breach Investigation Report 2016: Verizon

As an institution offering Internet banking services, you have invested significant time and resources to provide a safe environment for customers' online transactions and to meet the industry and governments' stringent compliance requirements.

Perimeter hardening, penetration testing, advanced encryption and strong authentication are just a few of the technologies that you have likely deployed to protect customers. However, despite these controls, business banking customers remain in the crosshairs of international cybercrime networks and their accounts are being compromised by Trojans such as SpyEye, Gozi and Zeus with their many variants.

Man-in-the-browser attacks are targeting your customers' endpoint computers. Unfortunately, it is very challenging to secure these endpoints, that you have no control over. Your layered defensive controls were not designed to prevent malware from capturing your customers' data when it's being typed or displayed on their computer screens. Nor will your current safeguards prevent the transmission of the stolen data to a server completely unconnected from your customers' banking sessions.

That said, your customers' poor endpoint security has become your institution's problem. Regulators, courts and legislatures are shifting the financial burden onto Financial Institutions, for both consumer and commercial accounts. Fraud and account takeover thefts have surpassed hundreds of thousands of dollars per incident. If this happens to one of your customers, you can choose to reimburse the account or risk going to court. But even if you win in court, the legal fees, bad press and lost confidence make this a lose-lose situation.

> "CYBER CRIME IS INCREASINGLY A THREAT TO THE WHOLE FINANCIAL INDUSTRY. THIS IS ONE DIGITAL CHALLENGE THAT BANKS CANNOT DUCK."
>
> The growing threat from online bank robbers
>
> FINANCIAL TIMES, May 2016

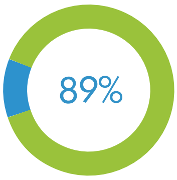
The SafeCentral approach for safer transactions

A pristine environment safe from web fraud - no more complaints, drained accounts or lawsuits.

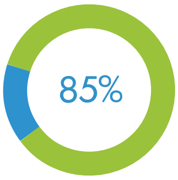
Through SafeCentral SafeDesktop and SafeBrowser, online activity is isolated from targeted threats. When activated, SafeCentral effectively blocks advanced data-stealing malware that has infected the customers' endpoint. As a result, online banking customers can complete their transactions without risk of triggering malware or exposing their private information to deviants. Even in the worst-case scenarios, when malware is already on the endpoint device, SafeCentral protects credentials, login information and any personal or financial data-in-use at the deepest layer during the active online session.

Rather than constantly reimbursing customer accounts or risking litigation, you have another choice. Financial institutions serious about security and protecting their customer accounts proactively provide their customers with SafeCentral.

Taking this proactive approach emphasizes your commitment to customer satisfaction and security while arming your customers with technology to protect their online banking activities against the increasing varieties and volumes of threats.



OF BREACHES HAD A FINANCIAL OR ESPIONAGE MOTIVE.



OF SUCCESSFUL EXPLOIT TRAFFIC WAS FROM THE TOP 10 VULNERABILITIES. THE OTHER 15% COVERED 900 VULNERABILITIES.

Source: Data Breach Investigation Report 2016: Verizon

Why offer SafeCentral to your customers?

Protect banking credentials

Protect customer credentials and financial information by preventing screen stealing, key-logging, DNS redirection and other forms of malware. Whether someone is a bookkeeper working remotely or a finance officer downloading corporate bank statements from a hotel room, SafeCentral facilitates a safe online banking environment from wherever they choose to conduct online banking transactions.

Reduce legal risks

Commercial accounts, particularly small business banking customers, are automatically prompted to use SafeCentral secure browser when going to your website. Even when they attempt to go to your website from another browser or shortcut. SafeCentral fills the gaps left by traditional antivirus, firewalls and encryption technology.

Locked down secure environment for your customers

Instead of chasing after the criminals with definition files and heuristics to nullify their malware and clean computers, SafeCentral proactively locks down the operating system and application functions that enable malware activity. By providing your customers with a secure desktop and browser environment, SafeCentral prevents malware from session access, even if the malware already exists on their devices or networks.

Stop the cycle of fraud

Oftentimes, malware that infects the endpoint leverages the browser to capture usernames, passwords and screenshots - making it easy for other data to be stolen. SafeCentral creates a secure, pristine environment that locks out man-in-the-middle and man-in-the-browser attacks.

Focused web session security

Isolate online activity from malware and critical financial data while protecting users from harmful websites and scams. SafeCentral protects data-in-use: including; authentication credentials, web session tokens, account numbers, account balances and other information that moves through the web channel and is presented in the web browser and stored on disk during and between web sessions.

Easy to use manual or automated access

Your customers can quickly and easily establish conditions where SafeCentral is automatically activated, including when logging into their bank or credit union accounts. When SafeCentral is activated, data stealing malware that might exist on users' PCs is rendered blind to credentials and sensitive financial data.

> "OF COURSE, BANKING DATA IS ALWAYS GOING TO BE A PRIMARY CONCERN AS IT'S PARTICULARLY ATTRACTIVE TO HACKERS. "
>
> Cybercrime has made brits fear online banking
> March 2016

> *"Businesses must recognize the threat that cyber crime can pose to them, their reputation and subsequently their bottom line. With the number of customers going online rapidly rising the issue of cyber security has never been more important. Companies need to consider cyber security as critical to their business operation as cost or cash flow"*- Adam Rowse, head of Business Banking at Barclays, 2016

Wontok SafeCentral is...

+ One-time install lightweight software that requires limited IT investment and support. It is easy to deploy and has minimal disruption to provide a safe online banking environment for all of your customers.

The SafeCentral difference

- SafeCentral is a next generation containerization technology that protects online banking activity on already infected computers.
- SafeCentral protects entire online sessions, from authentication to log out; usernames and passwords are kept safe, secure and barricaded from any malware.
- Simple, fast and easy to use. SafeCentral can be manually or automatically activated based on selected criteria and activities.
- SafeCentral defeats advanced malware, including ring zero rootkits.
- SafeCentral performs with minimum disruption to the user. A visual cue indicates that the SafeCentral SafeDesktop and SafeBrowser are active.
- Wontok SafeCentral's Trusted Security Extensions includes kernel drivers and hardened services that supervise operating system's events and enforce policies to block malware on endpoint devices.
- SafeCentral integrates seamlessly with other authentication and desktop security solutions.
- Easy to implement with minimal work required by user.
- Supported internationally.

Why Wontok SafeCentral?

- Protects your customer from account take over
- Compliant with FFIEC 2011 supplementary authentication guidance
- Compatible with third party financial platforms
- Deploys quickly and easily
- Turnkey, user-friendly lightweight software
- Reduces legal risk
- Strengthens fraud mitigation strategies
- Provides security with flexibility
- Protects your brand and goodwill
- Co-branding option available

Supported Systems:

Windows XP, Vista, 7, 8.x & 10 (both 32 and 64 bit mode)

Protects against:

- Account take over
- Fund transfer fraud
- Identity theft
- Man-in-the-browser, man-in-the-middle and zero-day malware
- Vulnerability exploitation
- Keylogging
- Screen capture
- DNS compromise and redirection
- SSL hijacking
- HTML form spying
- Password theft
- Session takeover
- Registry, process or file tampering

Contact Information

San Francisco – USA
americas@wontok.com
+ 1 561 472 5200

Hong Kong
apac@wontok.com
+ 852 2824 8330

Sydney – Australia
anz@wontok.com
+ 61 2 8355 5270

LEDT0008

http://linkd.in/1hZrjk1 Twitter: @SafeCentral

www.wontok.com

wontok™