Securing Financial Services Desktops from Cyber Threats

with the Latest Secure KVM Technology

Financial services are a lucrative target for cybercrimes carried out by nation-state and state-sponsored threat actors, ideological hacktivists, ransomware gangs, and Advanced Persistent Threat (APT) groups. Preferred attacks may involve phishing, malware, ransomware, web application, vulnerability exploitation, and distributed denial of service (DDoS). Incidents are becoming more frequent and sophisticated, resulting in compromised data, heavy financial losses, and impacted confidence in institutions.

Compounding the challenge to protect potentially valuable network data, is the interconnected nature of financial institutions. They are required to store and exchange client information with other organizations and databases to facilitate rapid decisions and transactions. CIOs must focus on securing their own network as well as mitigating the risks that external partners may introduce, all without disrupting business processes. Outdated legacy systems and digitizing financial services are additional factors increasing vulnerability and risk.

The threat of debilitating cyber-attacks on financial institutions escalated during the pandemic and has not ebbed since. According to PwC's Global Economic Crime Survey 2022 (global-economic-crime-fraud-report-snapshot-2.pdf (pwc.com), "39% of cybercrime incidents in the past 24 months are a result of platform fraud, and enterprise platforms help companies interact with customers, process transactions and move funds. The survey states almost half of all platform fraud cases take place on financial platforms – the most vulnerable model, particularly those involving funds transfers. But financial impact is just the beginning. Brand damage can be devastating. The undoing of customer loyalty and trust – catastrophic."

Parachute Technology's 2022 statistics by industry delves into the data associated with specific types of attacks. "Phishing attacks against financial institutions such as banks held the highest share at 23.2%, representing the most cyberattacks in the financial sector. Financial sectors saw a 35% increase in ransomware attacks in Q1. On average, financial organizations bore the second-highest data breach costs, at USD 5.97 million, just behind healthcare institutions."

The emergence of AI (Artificial Intelligence) and ML (Machine Learning) in the financial sector has been a double-edged sword for cybersecurity. AI is beneficial for prioritizing vulnerabilities, hunting threats, automatically creating security controls, and monitoring and optimizing data centers. Robust capabilities for deep learning and the capacity to analyze and mitigate big sets of potentially malicious data

make it an effective deterrent against cyberattacks. On the downside, generative AI can be used by threat actors to develop smart malware for malicious purposes. They may automate social engineering attacks to evade data security protocols and create phishing emails capable of learning from past mistakes. Sophisticated ransomware campaigns range from AI models creating realistic-sounding speech to use in phone-based vishing attacks, and using deepfakes with doctored images and video to fool targets.

Steps to combat cybercrime in the financial sector range from enacting strong detection measures to implementing recommended remediation including installing new firewalls, endpoint protection, and multi-factor authentication. Updating formal cybersecurity policies and training, incident reports, and recovery plans are additional tactics to stay ahead of the rising tide of attacks. But these ever-evolving attacks cover a wide range of areas. Phishing attacks try to trick employees into revealing sensitive information, ransomware attacks focus on disrupting operations to lay the groundwork for extortion, and DDoS attacks cripple critical financial systems by preventing customers from using essential services.

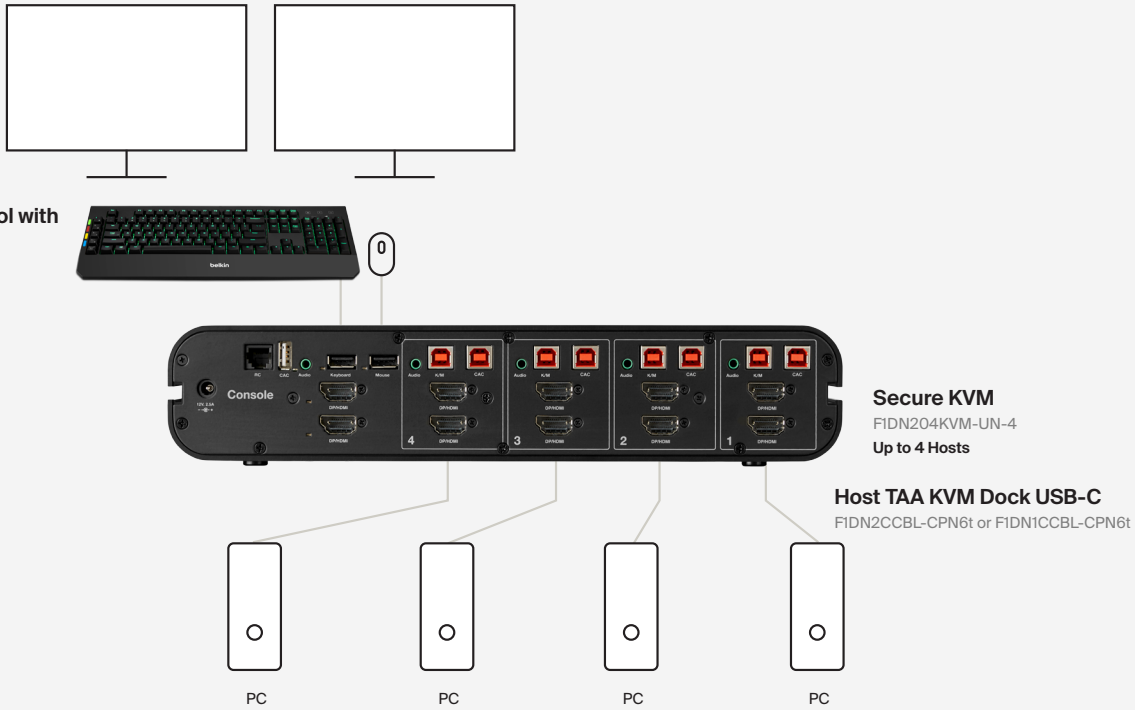
One preventative security measure adopted by other sectors including oil & gas and healthcare is to physically isolate networks and network assets. Creating an air-gap network limits access to mission-critical data to users with tightly controlled permission without ever posting it on the public internet or an unsecured LAN. This way, advanced signaling attacks that may compromise a desktop have no clear route to restricted systems with sensitive information. Forward-thinking financial institutions are following the lead of other industries by integrating air-gap isolation as part of their cybersecurity strategy.

Secure keyboard-video-mouse (SKVM) switches are vital components to defend against attacks adopted by sectors ranging from healthcare to government. SKVMs allow access to multiple computing systems at different security classifications, from a single desktop. This segregates secure and non-secure computing use and ensures a vulnerable element in the network cannot be used to breach more sensitive assets. Now, SKVMs are becoming appealing for the financial services industry as well.

A critical, powerful piece of the solution is SKVM switches. SKVM switches have been utilized effectively to protect high security government and military networks for years and can be equally effective in helping meet CIP standards for maintaining guaranteed isolation between multiple classes of network assets. Further, SKVMs can enhance operator efficiency by eliminating desktop clutter and allowing one keyboard and mouse to control multiple systems, without the possibility of sharing any data between them.

These devices are a win-win solution for financial services companies, helping meet CIP requirements while simultaneously delivering greater efficiency and effectiveness for operators.

Use Case Univeral 2nd Gen Secure KVM



Secure KVM for financial services

Many organizations have mandated the use of NIAP-certified SKVMs and SKMs at operator stations to isolate sensitive systems from those exposed to the public internet and corporate intranets. Financial institutions are adopting these solutions as well. With these switches, users have access to multiple computing systems from one desktop console, easily switching between various systems as their jobs require. This practice helps segregate secure and non-secure computing use. For example, an employee accessing internal email systems with a lower level of security can then switch and log into a more secure system to perform more sensitive tasks.

The chief advantage is to make certain that malware or viruses that may reside on a less-secure system, peripheral, or other IoT device never see a path to jump onto more critical systems. Additionally, it ensures operators are not encumbered by having to use multiple keyboards, mice, or monitors to perform their jobs. But not all KVM switching systems are secure. While they eliminate desktop clutter by allowing a single keyboard/mouse/monitor to be used to access multiple systems, unsecured KVM systems are at risk from both intentional and unintentional security vulnerabilities.

A typical cyber attacker generally probes networks for vulnerabilities, sneaks in and finds a way to hide from detection, all while eavesdropping on user activity and learning as much as possible about network paths to more valuable assets. Anyone looking for a KVM should consider using a NIAP-certified SKVM as these are designed to block any path for signals to travel from one system to the other and create guaranteed air-gap isolation.

Possible threats from unauthorized and untrusted peripheral devices

Is your KVM solution secure enough?

Many unsecure KVMs lack the comprehensive security features that financial services should require. Is your KVM hiding these vulnerabilities?

USB peripheral vulnerabilities

USB ports facilitate the high speed, bidirectional flow of data to and from the computer, making them a threat that can be used to gain control, intercept, and/or access resources beyond the PC itself and into any computer network attached to the PC. USB thumb drives are a popular way for social engineering threats to get introduced to enterprise systems and to copy and steal confidential information from servers. Only SKVMs force USB ports to be unidirectional (thus preventing copying of data) and filter commands to just HID information (thus blocking malware from being introduced into the system).

Video vulnerabilities

LCD monitors store display parameter data in the form of EDID, which could be exploited. EDID can be used to leak data from a secure network to an unsecured network by using the monitor display memory as a vehicle to transport data when being used with a KVM system. SKVM devices must prevent the reading or writing of display memory with a protected display interface to stop leakages.

Audio vulnerabilities

Integrated speakers on PCs and desktops can easily be hijacked and turned into microphones with no indication. As such, adversaries can easily eavesdrop on private conversations and closed-door meetings. SKVMs isolate the audio and ensure unidirectional flow for audio output.

Memory buffer leaks

KVM switches use onboard buffering to increase performance and have the potential to inadvertently leak data from channel to channel as they use the same switching processor for multiple ports. SKVMs have no buffering and utilize dedicated processors for each channel, thus eliminating the ability to leak data from one system to another.

Support for smart card authentication

Two-factor authentication can be deployed as an additional layer in controlling who has access to sensitive data. SKVMs have fully isolated and dedicated Common Access Card reader ports that are compatible with the latest smart card technologies and allow an operator to use a single reader with multiple systems. The SKVM fully manages each session, ensuring that session tear down and log-in requirements are never violated.

Poor casing and design

Because so much security enforcement relies on the integrity of the KVM components themselves, it is important that purchasers take a close look at the internal and external components that go into the manufacture and design of the KVM switch. The external housing of the switch must be demonstrably tamper-proof, ensuring that it cannot be opened and modified at any time. The switch's internal components must also be constructed to prevent tampering of any kind. Purchasers should make certain that they select only trusted vendors such as Belkin with proven security measures in the design, production, and handling of the product throughout their operations.

Choosing the right KVM solution for your financial services desktops

The National Information Assurance Partnership (NIAP), a government-sponsored program based within the National Security Agency, formulates specific requirements and recommendations to secure nearly every aspect of computing environments. The following are a few of the most concerning KVM scenarios that the NIAP testing program examines:

1. Users should not be allowed to connect unauthorized USB devices to the peripheral switch.
2. The KVM must prevent residual data transferred between peripheral port groups with different IDs.
3. Connection shall not be accessible by any other peripheral group with a different group ID.
4. The KVM should prevent a user error when setting shared peripheral connections from one computer system to a different one.
5. A connection, via the KVM, must not allow information transfer between computers.
6. Chassis design and supply chain must guarantee that the KVM switch has not been tampered or altered by any intermediary during transit and after deployment.

To continually improve security and reduce vulnerabilities in computing systems, NIAP directorates are used as the basis for testing and certifying commercial components. They also serve as a trusted security conduit between manufacturers and consumers of computer products used in secure environments.

One aspect of the NIAP program is the evaluation and recommendation for improvements in KVM switches. The agency's 2020 directorate, NIAP Protection Profile (PP) for Peripheral Sharing Devices (PSD) version 4.0 provides certification for products that have been vetted and found to conform to the strictest level of air-gap network isolation. As a part of its program, NIAP tests devices submitted by manufacturers for security compliance. Devices receive evaluation assurance levels that purchasers can use to confirm that any potential KVM device they purchase conforms to the NIAP recommendations.

When deciding on a SKVM product, NIAP is the single best resource to start your research. Additional information on the standard and a list of certified SKVM switches can be found on the NIAP web page at www.niap-ccevs.org.

With cyberthreats on the rise, financial systems rank among prime targets for nation-state and state-sponsored terrorists, ransomware gangs, and insiders. The internal threat posed by improperly secured desktops in financial organizations should be addressed with as much due diligence and vigorous security measures as firewalls, intrusion detection, and other external threat mitigations. Purchasers of KVM equipment must carefully weigh all the security and functional features of these devices to ensure the units provide the safest, most secure and user-friendly functionality to prevent any possible compromise of company and customer assets.

The Belkin Solution

Based in California, Belkin is among the world's most respected and successful computer component designers and manufacturers. For the past 30 years, Belkin has worked with financial leaders and IT specialists in financial work environments. Its SKVM switch solution is NIAP-listed and approved to the latest SKVM testing standard NIAP PP 4.0. Belkin provides the industry-leading Secure KVM solution, and one of its exclusive innovations is the use of true data path isolation.

Optical data diodes

Isolated processors are integral to the Belkin solution, but its next-generation engineering takes a unique step forward. Introducing optical data diodes to provide unidirectional data paths eliminates the opportunity for data leaks or data capture on keyboards and mice. The Belkin optical diode connects input and output data paths with a signal that uses light in the following process.

First, it transforms input signals — such as keyboard strokes — into light signals. This light signal is sent along a dielectric channel where the light is captured on the output side of the circuit. Within the isolated diode, this light signal is then transformed back into an electric signal. This innovation goes far beyond isolated processor engineering because data to and from peripherals is never exposed to any form of electrical sniffing or capture. Signals pass, in light form, in one direction, eliminating the typical peripheral vulnerabilities of bidirectional signaling through copper.

Dedicated processors for every port

Belkin's SKVM switch contains dedicated, program-once processors with up to 16 emulators for each KVM, completely isolating the data path between every post and peripheral. Each component is hard-soldered to the electrical board and any removal or tampering renders the entire SKVM inoperable. Audio, USB, video, and peripheral ports support the latest standards and are isolated and secure.

Advanced audio filter

The Belkin SKVM switch secures audio with 40dB isolation up to 60KHz and an 8th-order elliptic filter. Advanced audio filtering requirements add significant technical complexity and cost, but block attacks enacted outside of human audible frequency range.

Tamper-proof design, packaging, and shipping

Belkin SKVM products are designed, built, and shipped in the U.S. under the strictest security. Every Belkin SKVM switch includes tamper-proof sensors and seals on external and internal components and on the outside shipping container. Customers are assured that the product is in its original, securely manufactured state from one end of the process to arrival at their facility. Any attempt to access the internal electronics of the SKVM will immediately render it permanently inoperable.

Advanced USB and cabling technology

USB signals are monitored in real-time and never allow unauthorized traffic or the attachment of unauthorized devices such as flash drives, disk drives, or unapproved peripherals. This is done in hardware out of the box and does not rely on domain profiles managed by system administrators. Belkin provides smart cabling that enables enterprises to connect their Belkin SKVM switch simultaneously to legacy VGA and newer high-resolution computers and monitors. In addition, the Belkin SKVM switches allow for CAC-reader connectivity on dedicated ports that are separated from the keyboard and mouse ports.

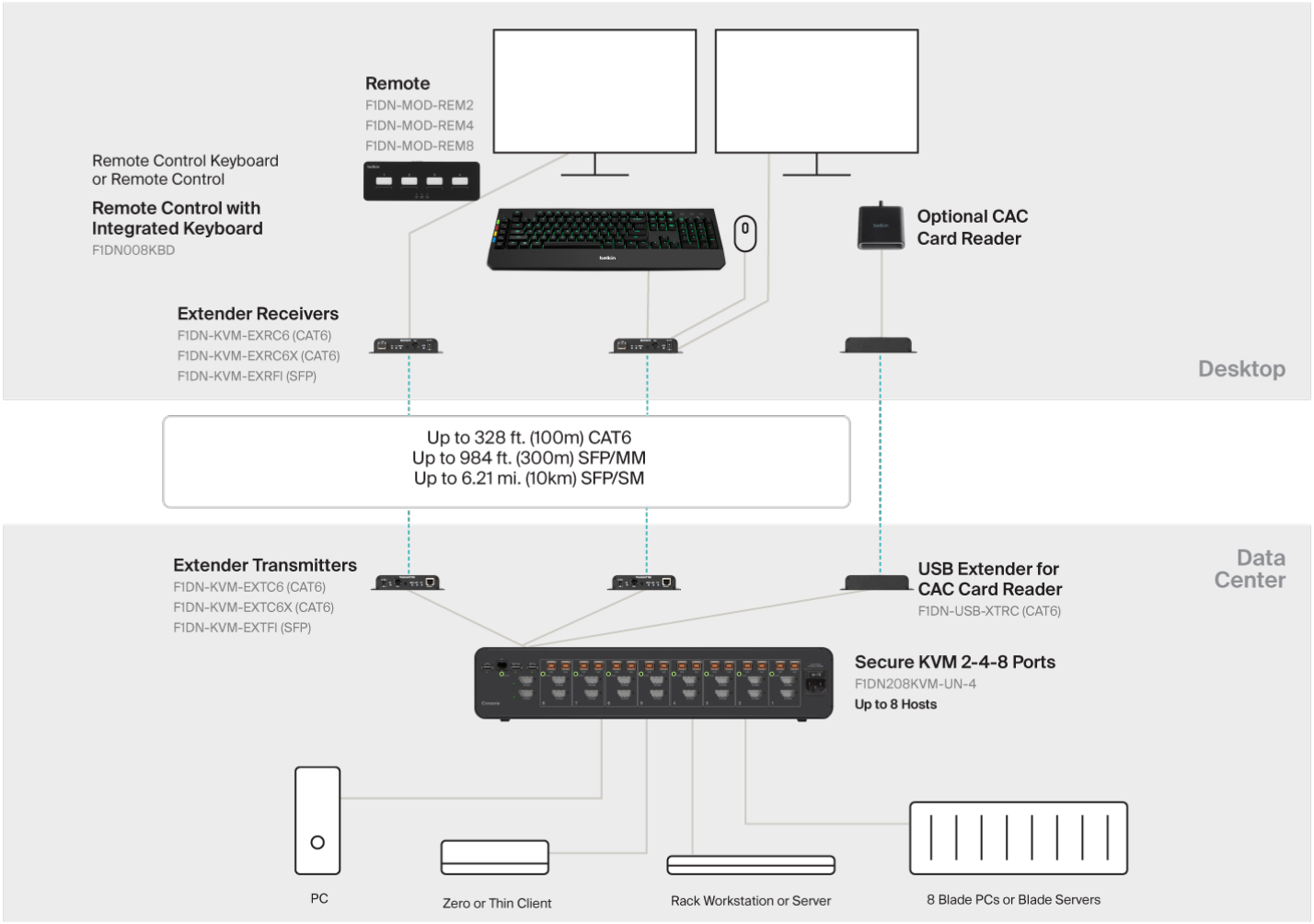
The color of efficiency

Customizable port coloring and naming on the front panel of the Belkin SKVM facilitates channel identification and reduces operator errors. When combined with the industry-first SKVM Remote Control with Integrated Keyboard, the SKVM can be located off the desk for a clean and decluttered workstation. The keyboard's LED backlighting and status indicators mimic the front-panel configuration of the SKVM to enhance operator channel and enclave awareness, minimizing operator error and exposure to uncleared personnel.

Universal video compatibility with combo connector and internal conversion

DisplayPort/HDMI combo connectors on each input and output allow the same SKVM to accommodate systems with DisplayPort, mDP, HDMI, DVI, VGA video outputs and modern and legacy monitors. This eliminates the need, cost, and uncertainties associated with external converters. This flexibility enables IT managers to deploy the same SKVM switch across their network and prolong the useful life of the SKVM simply by matching the appropriate Belkin cable with each connected system and monitor.

Security Use Case



Better than a zero or thin client — it's a no client

The combination of Belkin Secure KVM remote controls and extenders solves security and distance issues with groundbreaking technology that enables enclave switching control over long distances from the users' desktops. This valuable security feature allows the processing side and the SKVMs to be located in a locked, secure data center rather than on the desktop. Users have the flexibility to switch across multiple networks remotely even though there are no processing components at the desktop. This is ideal for remote desktops, conference rooms, command and control, server farms, and secure video access.

Other advanced features

The Belkin SKVM switch incorporates many other advanced features:

- Smallest SKVM/SKM in the market
- No memory buffering of any type
- Ultra-fast protected video-display switching through EDID emulators
- Tested and validated multi-platform compatibility and support
- Intelligent Common Access Card switching to prevent unwanted system log-off
- Guard mode for keyboard-mouse (SKM) switching
- No keyboard or mouse delays when switching ports
- Integrated mounting track to allow under-desk or side wall mounting to improve desk space
- High-resolution support for graphic-intense applications used on larger displays
- Dual-monitor support to increase user productivity

The Belkin SKVM combines cutting-edge cybersecurity provisions, video performance and user experience to deliver a no-compromise solution for the most demanding applications.