

Is Your Security Solution a Secured Solution?

How community banks and credit unions should confront the insecurity of physical security.

VERINT.



INTRODUCTION

Today's Risk Landscape

A look at the evolving threats and business challenges across your financial institution.

It's a fact. The financial industry has changed significantly over the past 10 years. Community banks and credit unions are not only focused on the competitive environment and customer retention, there is a new risk paradigm: one that encompasses cyber and physical threats. ATM skimming, identity theft, data breaches, scams, and phishing are all common terms in today's environment.

“

“The amount of money taken in cyber heists, both in banking and elsewhere, was estimated at \$3 trillion overall for 2015.”

In fact, cyber threats have taken a front seat in the lineup of primary risks facing financial institutions today. And it is no surprise why: According to

Cybersecurity Ventures, the total cost of cyber heists, both in banking and elsewhere, was estimated at \$3 trillion overall for 2015. This includes associated losses such as mitigation costs and reputational loss.

As risks evolve and consumer demand for new services grows, security and fraud leaders have to take a closer look at internal operations and processes to ensure consumer and corporate data, and infrastructure is secure and protected. Security leaders are not only responsible for protecting the branch network but they also must collaborate with IT to understand how both departments can work together to mitigate overarching risks. Comprehensive risk management that takes security, IT and cyber threats into account is the best way to proactively address potential threats.

Let's take a look at how community banks and credit unions can approach security to ensure your branch is a protected one.



Cybercrime Costs
Worldwide by 2021

\$6 Trillion

Bank Robberies
in 2016

4,251



Card Skimming Losses
from 2015 to 2016 Up

70%

Number of Identity
Theft/Fraud Victims

16.7M



Chance of an Active
Shooter Incident
Occurring at Work

80%

Modern-Day Risks

According to Verizon's Data Breach Investigation Report there were than 64,199 cyber incidents in 2015, of which 2,260 were confirmed data breaches. About 1,368 of the incidents and 795 of the confirmed breaches occurred in the financial services industry. "The motives for data breaches are increasingly financial," American Banker wrote in its analysis of the report. "This obviously makes banks more of a target than ever. The report found that 89% of breaches in 2015 were motivated by greed or espionage." But cyber risks are only one piece of the puzzle. Community banks and credit unions face a number of threats on a daily basis. **Here we take a closer look at the issues:**

Expansion

As banks expand into new regions through organic growth and acquisitions, and unify organizations, systems and people, there is a greater risk for threats. Security leaders are now responsible for protecting the enterprise as a whole, which requires increased collaboration with IT and traditional security functions. As the financial industry moves forward, banks and credit unions will continue to shift from a response-centric approach to a proactive preventive approach that addresses the costly and damaging disruptions caused by a lack of protection.

Collaboration

Information sharing is crucial in today's data driven environment. Improved collaboration delivers a wide variety of benefits by allowing banks and credit unions to easily communicate across multiple sites, which can help officials detect known criminals and recognize patterns of fraud. By taking a collaborative approach, financial institutions can minimize risks that are often inherent in siloed systems and locations.

Sophisticated Criminal Networks

Modern fraudsters are becoming even more sophisticated and financial organizations must grapple with high-tech schemes and, in some cases, globally organized crime rings. In addition, a cyber breach can start with a physical break-in. With these challenges, banks are being forced to handle security in a more unified way, gathering input from a variety of departments across the entire organization.

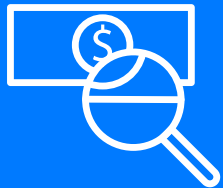
Integrated Solutions

Open systems allow users to access real-time information from multiple sources. Real-time information enables security officials and employees to make quick decisions that help improve the safety and security of the bank and its assets. Following an incident, operators can export video data, transaction records and other vital information to aid in a faster, more effective investigation. At the same time, an ongoing information exchange with regulatory agencies helps banks to easily stay in compliance.

Make the Move to Centralize Your Operations

The problem for most community banks and credit unions are that they already have hundreds of cameras deployed throughout various branches, which makes trying to address cyber vulnerabilities a tremendous challenge. Let's take the typical branch surveillance deployment, for example. There is usually a mix of both existing analog cameras and IP cameras, along with an encoder, network switch, and an NVR that is connected to the network. The NVR, switch, encoder, and IP cameras all have firmware that may need to be updated to mitigate potential cyber risks and most of them also typically have usernames and passwords that could be exploited by hackers. The prospect of trying to update these devices individually presents a logistical nightmare, which makes having some type of centralized management utility a must.

Centralized management helps identify security threats and vulnerabilities in real time, helping security personnel mitigate risk, ensure operational compliance, and improve fraud investigations. Banks can realize higher levels of intelligence and stronger protection from fraud, enhancing the customer experience while safeguarding assets. **Benefits include:**



Rapid Investigations

The time to identify a fraud source is decreased because the solution can search for potential fraud across multiple locations, allowing investigators to identify issues and quickly resolve customer concerns rapidly.



Increased Intelligence

Investigators have access to more data to maximize investigations effectiveness and reduce the time to identify fraud. This approach allows banks to realize significant cost and time savings.



Maximize Client Satisfaction

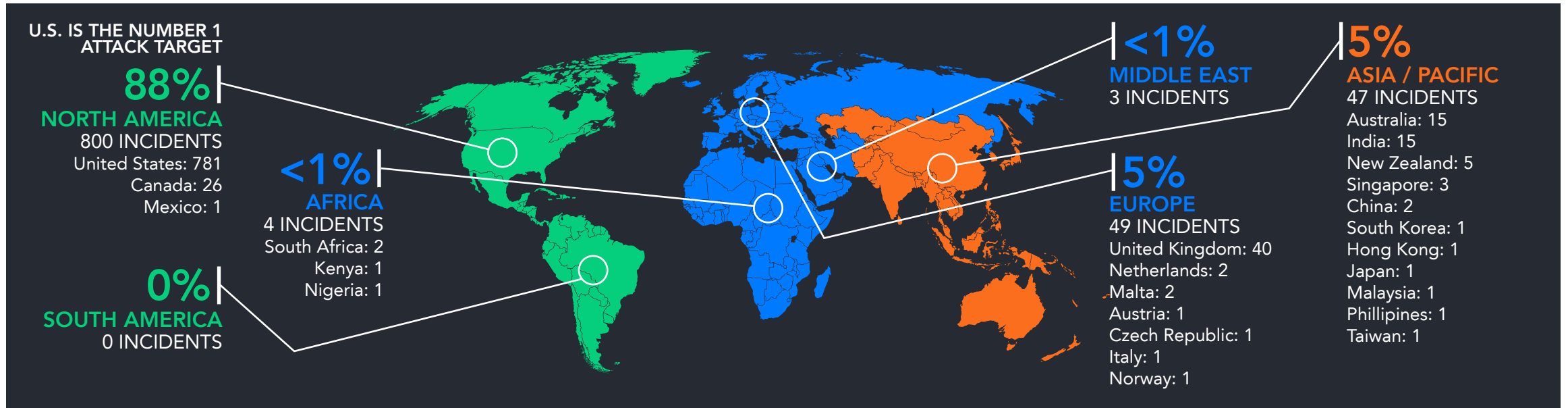
Banks are empowered to focus on ensuring customer satisfaction with their products and services by focusing less on fraud identification and more on how to address customer concerns.



Comprehensive Reporting

Gain access to extensive reports that allow banks to see where potential weaknesses lie and develop best practices on how to address them.

A Look at How Trends Around Fraud & Cyber Are Changing



The banking market continues to evolve through the growing use of digital and mobile devices, as more branch operations aim to enhance convenience and service for the customer. These advancements also create greater opportunities for fraud and loss. Increasingly sophisticated fraud techniques require organizations in these segments to pursue new approaches to preventing and detecting such activities. At the same time, customers demonstrate significant interest in how Big Data analysis and the Internet of Things (IoT) help improve the collection

of data — across bank branches, office locations, and remote sites such as standalone ATMs.

But cyber threats are prevalent in the community banking sector and more institutions are investing in ensuring their brand and assets are protected. But more needs to be done. According to the Cisco cybersecurity report, only 55% of cyber alerts are investigated by financial services organizations. Respondents noted that 28% of the investigated threats are considered legitimate—yet only 43% of those legitimate threats are remediated.

Fraud investigators from credit unions and community banks need to be able to leverage advanced tools to mitigate fraud and potential breaches more efficiently, and reduce the chance for loss — all processes that enhance the overall customer experience. Financial institutions also require solutions to identify suspected transactions before an event occurs and quickly link associated video in a rapid manner. Verint solutions are powerful tools to empower your financial institution to gain the intelligence needed to streamline investigations and centralize fraud mitigation.

Are You Prepared?

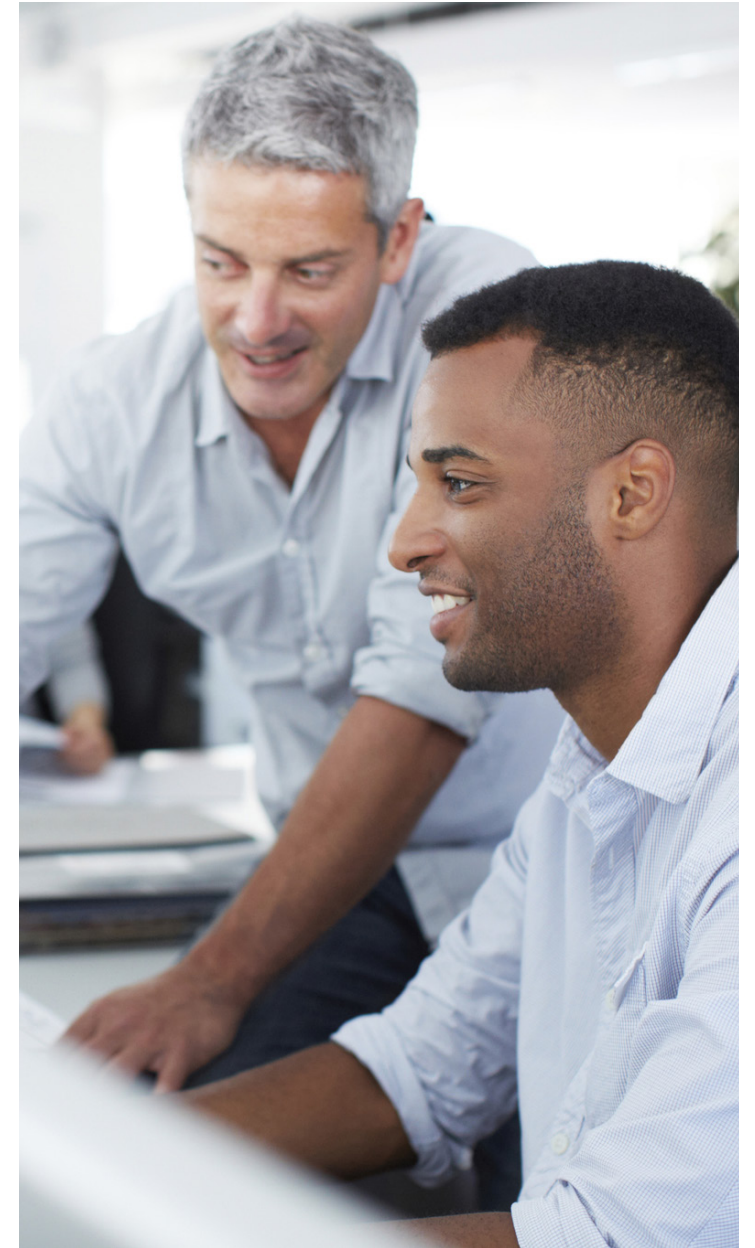
The fact that cyber attacks are becoming more prevalent isn't the only issue; they're also becoming more complex and therefore harder to address. At the same time, physical security risks are still very prevalent. The FBI found that more than 4,000 bank robberies took place in 2016. Emerging technologies, such as the IoT (which also creates many advantages for community banks) also bring increased risk to dangerous threats. Overall, credit unions and community banks are primary targets for hackers. But it's not just the monetary loss that these businesses need to be concerned about — there is also a threat to the brand, customer trust, and employee safety.

“

“Credit unions and community banks are primary targets for hackers”

All of these challenges and complexities open the door to new conversations and risks, including:

- Physical security has historically been viewed as the “black hole” in the organization into which the institution is forced to throw money. Security now needs to be positioned as a benefit to the overall business and security leaders need to know how to demonstrate this to senior leadership.
- Add to this the fact that security professionals need to be making the argument for additional funding. It is essential to speak the language of the financial decision makers within your organization.
- Finally, we discussed the overall impact a network breach can have the organization. The impact of this must be rightly positioned and valued within the organization.





Here are a few things that you can do to ensure your bank and credit union is better equipped to handle threats:

- **Regular Technology Refresh Cycles:**

Although many banks today replace computers and other IT hardware every three to five years, the same cannot be said of their security equipment. Security devices, like other technologies, are changing very fast which means vendors are phasing out certain pieces of equipment quicker and will eventually stop supporting them. Getting buy-in for a technology refresh can be challenging but unlike the days where these systems had to be purchased outright, numerous suppliers now offer leasing programs for their equipment and software, shifting the cost to an operational expenditure and placing the onus for maintenance back onto the vendor and/or integrator.

- **Check and Perform Firmware Updates:**

Manufacturers today are routinely updating their products to ensure they're protected against the latest threats. Unfortunately, many organizations are still woefully lagging when it comes to applying patches to impacted devices.

- **Practice Good Password Hygiene:**

Network security experts have written at length in recent years about the need of organizations and their employees to leverage strong passwords and the same thing can be said with regards to periphery devices, such as cameras and NVRs. Oftentimes, however, the passwords being used on these devices are still the default ones that came with them from the manufacturer or were changed to something simple like "123456" or "password."

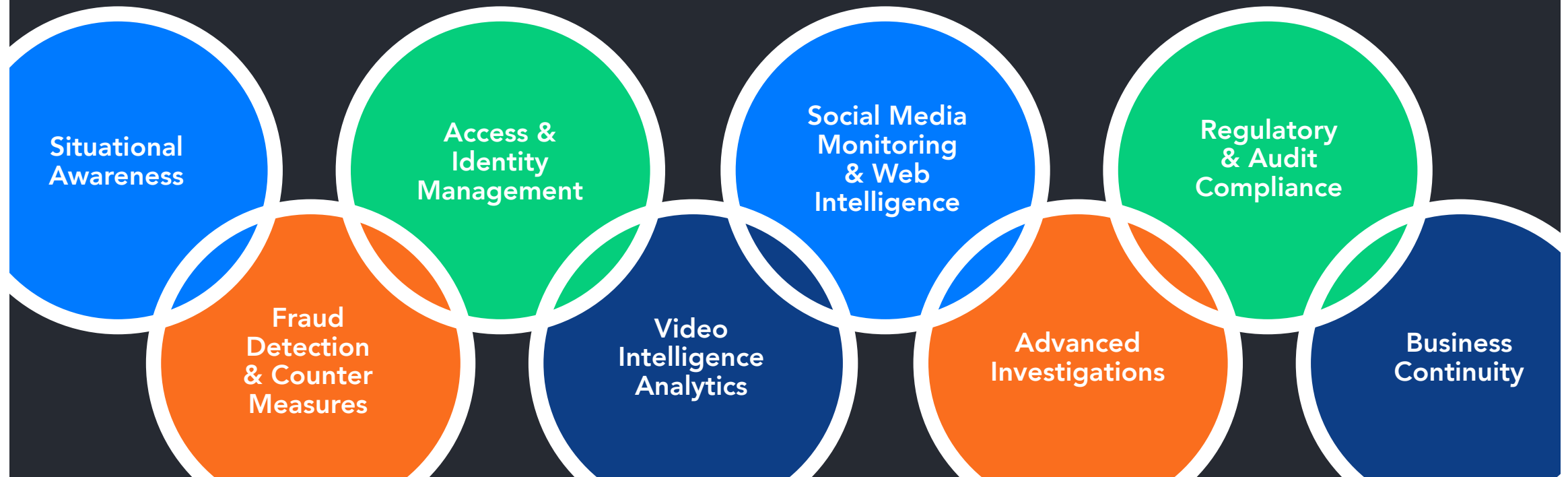
- **Leverage MAC Access Control Lists (ACLs):**

Many people within IT security departments at financial institutions are concerned about the potential of an unauthorized user gaining access to a camera switch at a bank branch, plugging in a laptop and infiltrating the network or introducing a vulnerability to periphery devices themselves. ACLs allow end-users to detect the MAC address of an IP camera and should it be unplugged, subsequently block any other device from connecting to it.

The Technology You Need

At Verint, we understand that you operate in challenging, fast-moving environments in which opportunities, challenges, requirements, and regulations can vary widely, change quickly, and evolve significantly over time. That's why we offer a technology and services portfolio that's among the most extensive in the industry. **Our leadership is proven:** More than 90 percent of the global Fortune 500 companies in the financial market rely on Verint solutions to identify and combat fraud, mitigate risk and ensure compliance. As consumers demand faster, flexible, and more personalized interactions, the financial industry must increase their level of service and convenience while being able to predict and respond in real-time to escalating threats. The Verint financial portfolio provides advanced, unified technology that includes predictive and analytical solutions, data protection, and 24/7 surveillance.

Build a Diverse Technology Platform




In an effort to fully protect your bank, here are a few of the platforms we suggest:



Video Surveillance and Management

Verint EdgeVMS Vid-Center software serves all video functions including DVR/NVR configuration, live and recorded video viewing, event search, system logs, and firmware and license feature updates. Verint EdgeVMS Vid-Center provides instant alerts, surveillance analytics, and is compatible with the entire line of Verint recorders, as well as mobile and legacy installations. This platform eases video searching, streamlines investigations, and provides the tools needed to empower your fraud team to quickly close cases.



Deployment Management

With Verint Evidence Center, Verint redefines the way banks capture transaction data by automatically associating video data with specific transactions. Users can obtain all transactions per location, ATM, and teller window from a central operations center to make decisions based on company-wide data. Fraud investigators can search all sites for data based on customized settings including date, time and transaction number, account number, dollar amount, type of transaction, location, camera name, and terminal and employee ID. This approach also reduces the time to search for fraudulent activity for bank customers, providing them with peace of mind that their accounts and finances are protected.



Surveillance Analytics

Verint Surveillance Analytics helps organizations make sense of vast amounts of security video and data, generating Actionable Intelligence for better decisions and faster, more effective action. This powerful suite of integrated analytic applications can automatically pinpoint potential breaches and significant events and send video alerts to the appropriate people, departments and agencies. Designed to address the specific safety and security requirements across banking environments, this platform helps organizations deliver a proactive approach to threat deterrence and management.



IP Cameras

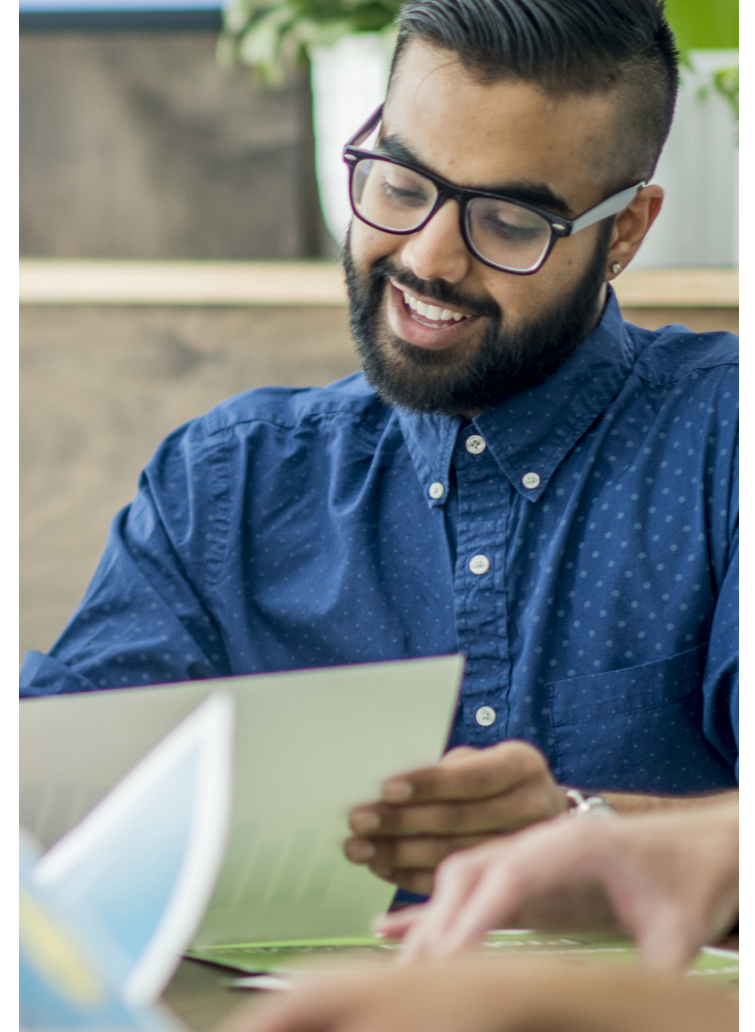
Verint IP cameras deliver high-definition video with ultra-efficient bandwidth management, enabling customized H.264, MPEG-4, or MJPEG compression formats with multi-streaming capabilities. Models come in a variety of forms — from fixed body and pan/tilt/zoom cameras to indoor and all-weather IP domes — to accommodate a wide variety of video surveillance requirements in the community banking market.

Curious if You're Doing Enough? Ask These Questions.

1

Is it best to collaborate to mitigate these threats effectively?

Over the last decade, the emergence of the IoT and a demand for more mobile capabilities has changed the way people and businesses connect. But as the need for connectivity increases, so too does the need for increased security for physical assets, networks, and valuable corporate data. As a result, a dialogue between IT and physical security is necessary to help leaders gain a greater knowledge of how to best collaborate to ensure complete protection. Leaders must communicate closely to drive strategies that help identify vulnerabilities in a more proactive manner. The result of these conversations: a truly comprehensive approach to security intelligence.



2

How can I pinpoint the important data necessary to address cyber threats proactively?

To maintain a high level of security and ensure business continuity around the globe, companies seek solutions that help predict and identify threats in real time. But often, there are too many alerts generated by too many systems, and none of this raw data is actionable. Linking cyber and physical security together transforms alerts into actionable intelligence, which helps users connect the pieces of any situation and present a unified risk scenario to the appropriate analysts and operators. By capturing and analyzing data in real time, enterprise organizations gain a visual representation of risks across the business while accessing information related to the most critical events happening at any given time. Not only does this unified process enable a higher and more proactive level of protection, but it also helps facilitate a plan of action based within a common, unified security operations center. Communicate closely to drive strategies that help identify vulnerabilities in a more proactive manner. The result of these conversations: a truly comprehensive approach to security intelligence.



3

Can we “talk” cybersecurity?

Security leaders in banks need to feel prepared by staying updated, looking at common vulnerabilities, understanding the malware and challenges, and testing the environment. And collaboration is key to mitigation: Traditional security and fraud teams must work in conjunction with cyber teams to effectively handle all aspects of a cyberattack. Additionally, CISOs need to “sell” cybersecurity to CEOs and the board by outlining the importance of protection through emphasizing the impact of a potential cyberattack on the business. Ensure you can verbally address the most critical risks to your senior leadership, including recent botnets, scams, and cyber gangs, to receive the support (and budget) you need to address these threats head on.

4

Is my system secure?

It is critical that you are knowledgeable about the steps you can take to protect your security and network infrastructure from cyberattacks. Changing default passwords should be a first step, as some scams target devices with hard-coded factory defaults. Ensure software and firmware is up to date because updates often include fixes for potential vulnerabilities. These updates keep your devices and network more secure and increase overall system uptime. A firewall is useful to prevent hackers and unauthorized programs from accessing the critical business information and resources on internal networks and computers. Also, minimize potential risk by closing network ports and disabling services you don’t need. With all of these instances, it is best to work closely with your integrator partner and chosen vendor to ensure that your system is as secure as it can possibly be critical risks to your senior leadership, including recent botnets, scams, and cyber gangs, to receive the support (and budget) you need to address these threats head on.

5

What solutions are best to help mitigate risks?

Technology is a great force multiplier. Security — both cyber and physical solutions — helps secure an entire branch footprint, alleviates risk, ensures operational compliance, and improves fraud investigations. Verint’s comprehensive and robust surveillance systems can provide organizations with intelligence and unprecedented protection from fraud, all while enhancing the customer experience.

At Verint, we practice the same concepts outlined here, combining physical and cyber security efforts to realize comprehensive risk intelligence. By bringing various leaders, departments, technologies and strategies together, we can more effectively identify threats, develop trends and quickly access important data to ensure security and safety goals are realized. Our goal is to help financial organizations achieve the same.

Discover How Verint Can Help You

Sophisticated Security Suite for Branch Surveillance and Investigation

Verint's advanced security solutions can help your financial institution identify security threats and vulnerabilities in real time, helping your security personnel mitigate risk, ensure operational compliance, and improve fraud investigations. Verint's comprehensive video surveillance platforms and advanced analytics can provide you with immediate intelligence and unprecedented protection from fraud, enhancing the customer experience while safeguarding assets.

Discover how Verint Security and Compliance solutions for banking can help put security, safety, and compliance at the heart of your customer engagement strategy.

Contact Verint Today to Learn More

Americas

insidesales.brs@verint.com

888-585-7059

Europe, Middle East & Africa

info.emea@verint.com

+44(0) 1932 839500

Asia Pacific

info.apac@verint.com

+(852) 2797 5678



verint.com



twitter.com/verint



facebook.com/verint



blog.verint.com

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited. By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change. Not all functionality is available in all configurations. Please contact Verint for current product features and specifications. All marks referenced herein with the ® or TM symbol are registered trademarks or trademarks of Verint Systems Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners. © 2018 Verint Systems Inc. All Rights Reserved Worldwide. V1180.180323

VERINT®