Upgrading for Safety:

The Importance of Firmware Updates

Banks and other financial organizations face a constantly changing risk landscape that includes cyber and physical threats such as ATM skimming, identity theft, data breaches, robberies, phishing and hackers. The average cost of a data breach in 2020 is estimated to exceed $150 million, according to Juniper Research. Outdated technology cannot fight the continuing battle, and for financial institutions, there's more to lose than just money, a bank's reputation and brand's trust could be at stake.

Therefore, financial institutions must now approach security from a holistic point of view, opting to deploy end-to-end technology solutions that can help identify various kinds of threats and streamline investigations for a quicker resolution. However, while these types of deployments are the safest and healthiest security technology strategy, they can be vulnerable if they aren't frequently updated and appropriately upgraded.

The process of firmware updates is essential when it comes to the data that security systems collect, through tools such as surveillance cameras, analytics or networked video recorders. Video now provides so much more information than merely visual footage; it can help banks identify the intelligence most vital to them. Advanced solutions, such as facial recognition technology and ATM loitering detection, provide elevated insight to help businesses become more efficient in both their security and business operations.

Considering the value of an end-to-end security solution, can businesses afford a system error, or worse, a system failure? The answer is no, and there are four substantial reasons why keeping security systems updated and upgraded to the latest version levels is essential:

1 **Cybersecurity**

2 **New Functions & Features**

3 **Support**

4 **Compliance**

The average cost of a data breach in 2020 is estimated to exceed

$150 million

25% of all malware targets financial service providers

Ignoring firmware fixes can result in **data loss, breaches** and other **crippling scenarios.**

VERINT®

1

Cybersecurity

Financial institutions are prime targets for cybercriminals. According to a report by Intsights, 25% of all malware targets financial service providers. Therefore, the banking industry cannot allow security failures to occur due to a lack of technology maintenance. As vendors release new technologies, they are also continually improving their firmware and software, fixing security bugs, patching holes in systems, and striving to create the best and safest version of its solutions. However, those fixes are only relevant if the organization upgrades the system when the update is released. Ignoring firmware fixes can result in data loss, breaches and other crippling scenarios.

3

Support

Support is a critical component of advanced technology solutions and Verint is here to help troubleshoot and handle any concerns that may arise. For example, a Verint system can be accessed remotely, solving the issue at hand effectively and efficiently, and then pushed through the entire network from Op-Center health and management solution, making the whole process seamless and relatively effortless. However, as with Verint's Op-Center, outdated systems make supporting the customer much more difficult, increasing the time and effort to solve the issue. Ensuring the newest software is being used enables manufacturers to assist when needed to keep the solution running properly.

2

New Functions & Features

Just as manufacturers continue to improve their security measures, they are also adding new functions and features to the technology. Modern security technology, including video, continues to progress at a rapid rate and creates numerous opportunities in software while still using the same hardware. High-end cameras, such as Verint's 4k cameras in conjunction with Verint's EdgeVMS, have the functionality to not only record video but also can include fraud detection, facial detection and much more. Artificial intelligence (AI) and the Internet of Things (IoT) have changed the way security solutions work, leading to a dramatic increase in functionalities and innovation. Taking advantage of new firmware releases is one of the best ways to maximize your technology investments.

4

Compliance

Because of the high risk, valuable assets and massive amounts of personal data involved with the financial industry, these organizations face some of the most stringent compliance guidelines and regulations of any industry, facing hefty fines and penalties if found to violate compliance. Although there's an incredibly long list of the various guidelines to comply with, one of the largest governing bodies is the Federal Financial Institutions Examination Council's (FFIEC). The FFIEC is a formal interagency that is "empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions." Complying with the FFIEC and other regulations requires that best practices simplify, automate and modernize processes among a variety of areas, including IT/cybersecurity. One element of their best practices requires a patch management strategy. Successful patch management is critical, but it can only be executed by keeping the security platform updated, as patches are only available via updates and upgrades.

While there are numerous reasons to update infrastructure regularly, why is it that some financial institutions fall behind? After all, in our technology-focused society, people are used to updating and upgrading their technology regularly, including cell phones, computers, cable boxes and more. **What's different? Two factors:**

Cost

High-tech, end-to-end security solutions can be more complicated to update than a smartphone. But much like upgrading a computer's operating system, it takes time, just on a much larger scale. To deploy an upgrade, many companies might fear the need for additional workforce, adding unexpected costs. However, using a solution such as Verint Op-Center facilitates a seamless and secure deployment, all from one location, saving time, effort, and cost.

Awareness

On many personal technology devices, a glaring red bubble on an app and constant popups are visual reminders for upgrades and updates. Without these indications, customers may not be aware that maintenance is needed. Verint customers can find update information in monthly newsletters and the Verint Community portal, and customers can reach out to integrator partners as well as Verint's sales and support network. As a customer engagement company, Verint is always available to help make sure customers are getting the best experience with their investment.

Best Practices

To make sure that your system is operating at its top capacity, firmware and software updates must be deployed as soon as they're available, which can be achieved by following a few best practices:

Create a Schedule

Set a date at least once each year — but preferably every six months — to investigate potential firmware upgrades. Make sure key decision-makers and participating departments, such as IT, are aware of this date and involved in the deployment to assure a seamless process.

Have a Process in Place

Making a schedule creates a regular calendar appointment for maintenance, but you should also have a process in place to complete emergency upgrades. Most likely, this involves multiple departments, meaning that this plan should be agreed upon by all important decision-makers so that the deployments are executed quickly and efficiently when needed.

Security Technology is a Critical Asset for Financial Institutions.

It increases efficiency in business operations, helps ensure compliance, and protects assets from fraud and theft. But as with any technology investment, maintenance is key to a successful long-term deployment. Verint's end-to-end solutions and customer support make it easy to implement these upgrades so that customers can get the most out of the technology investment.

The Customer Engagement Company™

Americas

info@verint.com

1-800-4VERINT

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. V1490.200103

VERINT®