CyberSecurity - From Big Army to Smart Army

As work expands to use all available space, security threats too expand. Nilesh Gupta, Global Practice Head - Cloud Services at 3i Infotech, reveals how banks can leverage new thinking and new technologies to safeguard themselves:

Ever since covid arrived on the scene and disrupted well established norms, disruption has become the new normal. Many organizations closed offices and had employees work from home. WFH has been recognized as the topmost new word of the year 2020.

Out of the comfort zone of their offices, employees had to start using several new tools and new techniques to continue creating value for their organizations and their customers. Organizations moved quickly to provide new tools such as video conferencing, VPN, etc. Beyond that, employees picked up those tools that were readily available for free such as converting pdf to text or designing a logo or modifying a picture or transferring huge files. And of course, banking specific tools such as forex converters, product comparators, public reviews, new apps, etc. Once people started using such tools and seeing a variety of benefits, including savings in time and effort, there was no stopping them. Since most of such tools are hosted in the cloud, it would surely be correct to say that one part of WFH became Work from Cloud (WFC). WFC may not yet be popular jargon, but it is the new normal for sure.

ACCELERATING INNOVATION

When both employees and their organizations are aligned with the idea of WFC as the preferred environment, a whole lot of things begin to change. The first and foremost is that employees become more innovative. As they explore a variety of offerings in the cloud, they begin to see existing things in new ways. They come up with new product ideas, new product enhancements, new ways to improve CX, new ways to improve the customer journey, new ways to cut costs and much more. All the dream capabilities that an organization wanted in its employees start flowering when employees are exposed to a wide variety of new ideas.


Nilesh Gupta

The second major benefit is that many of these tools are either free or very low cost....another added benefit of WFC.

CONTAINING RISKS

No opportunity comes without a problem – and in this case the problem is cybersecurity. Working outside the organization's perimeter from anywhere, any device, any network and accessing distributed application across cloud and on-premises raises security risks to the bank's business and simply cannot be ignored.

Banks need to ensure that existing security tools are fine-tuned to recognize and control the new risks. Gartner calls this SASE – Secure Access Services Edge. Yet, existing tools may have been designed for an on-prem scenario and cannot simply be reconfigured for a cloud scenario or borderless workforce. SASE directly addresses basic security needs such as encryption and access control, as well as complex compliance needs such as controlling cross-border data flows, restricting access based on geography and other factors, and maintaining detailed access records for forensic investigations.

For a bank, the cloud journey needs a cloud native security setup, preferably one that works seamlessly with on-prem and existing tools. Here comes NuRe Edge, a new age offering from 3i Infotech. NuRe Edge tackles the issue that in a borderless world, people, apps, and data are moving out of the organization's perimeter.

The second big pain that banks face is handling a wide variety of security tools and they do not want WFC to bring in more such tools. The obvious preference is for a single point of control to simplify things. Since there is no perimeter as such and the user can log in from home network, public network, different machines, etc, the need

Hardware Root of Trust (HRoT)

Almost all access control security technologies rely on user identity, but most legacy technologies don't do enough to protect that identity once it is established. Once a user is authenticated, their identity (issued in the form of a digital certificate) needs to be protected. Most legacy security services encrypt and store the certificate on the device where it is vulnerable. The latest technologies including 5G networking and Microsoft's Windows 11 OS go much further by using the Hardware Root of Trust as the foundation of securing the users identity. The HRoT is a unique element in the hardware that cannot be duplicated or replicated by anyone. HRoT benefits the bank as it protects their users when connecting from untrusted networks such as public Wi-Fi and also reduces risk of using non-corporate devices. Hardware security is harder to crack gives more time to take preventive measures if a device is lost or stolen. HRoT also increases adherence to compliance standards such as PCI-DSS.

is to give same level of security and desired assurance that this is indeed happening. Here too, NuRe Edge is designed to bring that assurance with its proven Zero Trust Network Architecture (ZTNA)

USE CASES IN BANKING

Every bank is seriously looking to adopt zero trust base architecture. Banks have invested so heavily in cybersecurity that upgrading to zero trust is a huge challenge. There is where NuRe Edge brings its USP – it works seamlessly with existing cybersecurity controls, platforms and tools to implement Zero Trust Architecture.

NuRe Edge sits as a 2nd layer on top of the existing layers such as Active Directory, and integrate using APIs. Zero trust creates a secure tunnel for users with 'verify and trust' principles, in contrast with antiquated trust principles followed by traditional VPN. Zero trust will build additional walls, allowing only authenticated and authorized users and devices to access applications and data. Further, it also protects those applications and users from advanced threats on the internet.

Whether WFH or WFC, another critical need is clear visibility as to what assets are there in the cloud and who is using which asset. NuRe Edge comes integrated with CASB and helps customer to enforce security, compliance, and governance policies for cloud applications and provides visibility into user activity with sanctioned cloud applications

NuRe Edge incorporates another technology – hardware-based authentication – a unique element in the hardware that cannot be duplicated or replicated by anyone, technically known as Hardware Root of Trust (HRoT). It defeats theft of user credentials, while still allowing flexibility as each user is allowed one Android device, one Windows device, one IOS device, and so on.

UPGRADE THE SECURITY MINDSET

With increased digitalization the banks employees and applications become more and more distributed. Employees can be working from anywhere with a variety of devices and apps can be running in the bank's data centres, in the cloud, or even at other locations such as bank branches. SASE secures this increasingly distributed environment with a set of technologies that secure the identity of users, provide granular access control at the user/device/app level, and tightly control how data/apps can be accessed and stored in the cloud. These technologies are hardware root of trust (HRoT), zero trust network access (ZTNA), and cloud access security broker (CASB). The right security capabilities are essential for both safeguarding the bank's data as well as remaining in compliance with regulatory requirements.

To conclude, to counter the rising threats and increasing attack surface, what banks need is not a big army, but a smart army.

nilesh.gupta@3i-infotech.com

Zero Trust Network Access (ZTNA)

Legacy VPNs place users on the internal network, assuming that they are trusted to have access to anything on the network unless specifically blocked by additional security elements. Zero Trust Network Access flips this paradigm on its head and does not trust any user, device, or service until authenticated. The default policy for ZTNA is to 'Deny All' and only allow that access which is explicitly enabled by security policies. Apart from granular access control, ZTNA also hides internal applications from attackers thereby decreasing the bank's attack surface, without compromising user experience.

ZTNA improves user experience over legacy VPNs because it does not require remote user traffic to be routed through the bank's data centres if the application is also remote. For example, performance sensitive applications like Zoom or VDI can be degraded by the increased latency of routing through the data centre. With ZTNA, the user connects to the ZTNA cloud platform and then directly to the app. This reduces latency, reduces the traffic burden on the bank's internal network, thus delivering a better experience to users.

Cloud Access Security Broker (CASB)

Even with granular access control, there is still the risk of cloud applications being misused to ex-filtrate bank data or to violate other bank policies. A Cloud Access Security Broker (CASB) software sits between the user and cloud apps to make sure that user actions conform with company policies. CASB provides visibility into which cloud apps are being used (thus uncovering shadow IT), helps banks with compliance by enforcing regulatory requirements on how data is used, and protect users from threats such as malware. Most importantly, however, CASBs protect the bank's data by enforcing data loss prevention policies.

Bringing It All Together With SASE

SASE is a key building block for banks adapting to work from anywhere and taking advantage of the cloud to become more agile. It addresses key challenges with protecting data in the cloud through improved security and better adherence to legal and compliance requirements such as national data privacy rules and PCI-DSS. Not all SASE platforms are alike. It is critical to understand which technologies the SASE platform implements and whether it can deliver the security and performance the bank needs. Hardware Root of Trust, Zero Trust Network Access, and Cloud Access Service Broker are each very powerful technologies on stand-alone basis. Integrated into a single, scalable SASE platform their capabilities build on each other and enable the bank to compete head on in our digital-first world.