Financial Services Sector - Regaining Control of Your Security

The Landscape

The 2024 Verizon Data Breach Report reveals that the Financial Services sector is now among the top four most targeted industries. Phishing remains the leading intrusion technique, responsible for 73% of all attacks, frequently resulting in ransomware. Data exfiltration for extortion has become a standard tactic in the arsenal of cybercriminals. In Canada, the average cost of a data breach surged to $6.9 million in 2023, according to IBC's 2024 Cyber Insurance Report. With all the advancements in the cybersecurity field why does the trend continue to favor the attackers?

The Issue

As the financial services industry continues to adopt more convenient digital offerings for their customers the available attack surface provided to adversaries increases. Phishing and social engineering attacks have become a daily challenge for many institutions. While security awareness programs aim to educate employees and reduce vulnerability, relying on the human element alone is no longer a realistic defense—especially with the rise of generative AI, which makes phishing attacks more convincing and harder to detect. Expecting employees to consistently thwart these increasingly sophisticated threats is unrealistic.

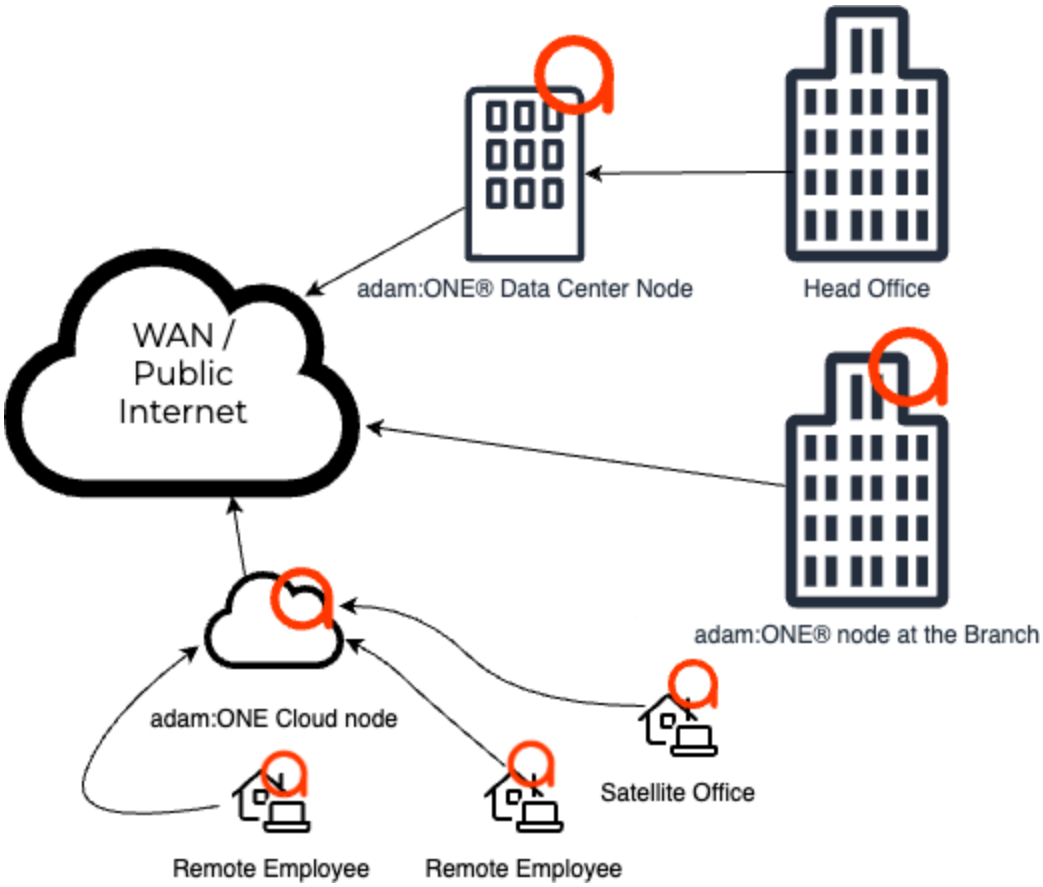
Beyond the loss in productivity, these constant threats place an undue burden on employees, who are left scouring their emails, worried they might be the cause of a critical data breach. Conventional real-time detection and response tools are intended to react quickly, but as we've seen time and time again, they're simply not enough. By the time a threat is detected, the damage is often done, with sensitive client data already exfiltrated.

The Solution

adam:ONE® facilitates a Zero Trust connectivity (ZTc) environment - Where every connection out of the enterprise network is vetted and only verified devices are allowed to connect to known good locations. ZTc allows the enterprise to sculpt the Internet to its needs. "Allow only the good" instead of trying to keep up with the "known bad" becomes the reality. The use of patented Don't Talk to Strangers (DTTS)® technology in combination with Dynamic AI driven allow-listing creates a **non-disruptive** default deny-all state that is virtually invisible to the

user. Utilizing DNS as the root of trust and ensuring all destinations are vetted prior to the connection being allowed, adam:ONE® blocks any connections to both known bad and unknown destinations. DTTS® denies connections to C2 servers and shuts down egress vectors to prevent data exfiltration. Attackers are neutralized by default without the need to know whether the destination is bad or not. Enterprises can finally regain control of their outbound network traffic without disrupting their day to day operations..

ADAMnetworks® Deployment



ADAMnetworks®'s **Smart Rollout** is a guided process designed for Enterprises to move their current network into a **Zero Trust connectivity (ZTc)™** network with a predictable set of resources over a reasonable time period with little to no disruption to the business. **adam:ONE®** provides a flexible edge for the enterprise network and can be deployed on-premise or in the cloud - on bare-metal, virtualized or within a container. **adam:GO™** affords mobile devices the same level of security as if they were on the enterprise network behind **adam:ONE®** including Windows OS, MacOS, iOS, Android, and Chrome OS devices. It is time for a new philosophy. Using reactive security tools causes your organization to have a reactive posture - no matter how proactive you want to be. Instead of relying on detecting threats, and then responding to clean up the mess, security administrators can now move to a true proactive posture to neutralize attackers before they can execute.

Adamnetworks® - Protecting the people and systems you care about.™