WHITE PAPER

Q2

5 Things Every CISO Should Know: Securing the Digital Banking Channel in 2022 and Beyond

Financial institutions looking to meet the needs of today's customers must deploy robust security measures to help ensure that their data and networks are protected from cyber threats. Malicious actors both inside and outside organizations present a grave threat, as do inside employees who may, through no fault of their own, fall victim to an email-based phishing attack or other attempt to compromise access credentials. In a digital-first banking world, every financial institution must deploy solutions that are both robust and future-proof as new threats emerge and the stakes associated with losses grow higher.

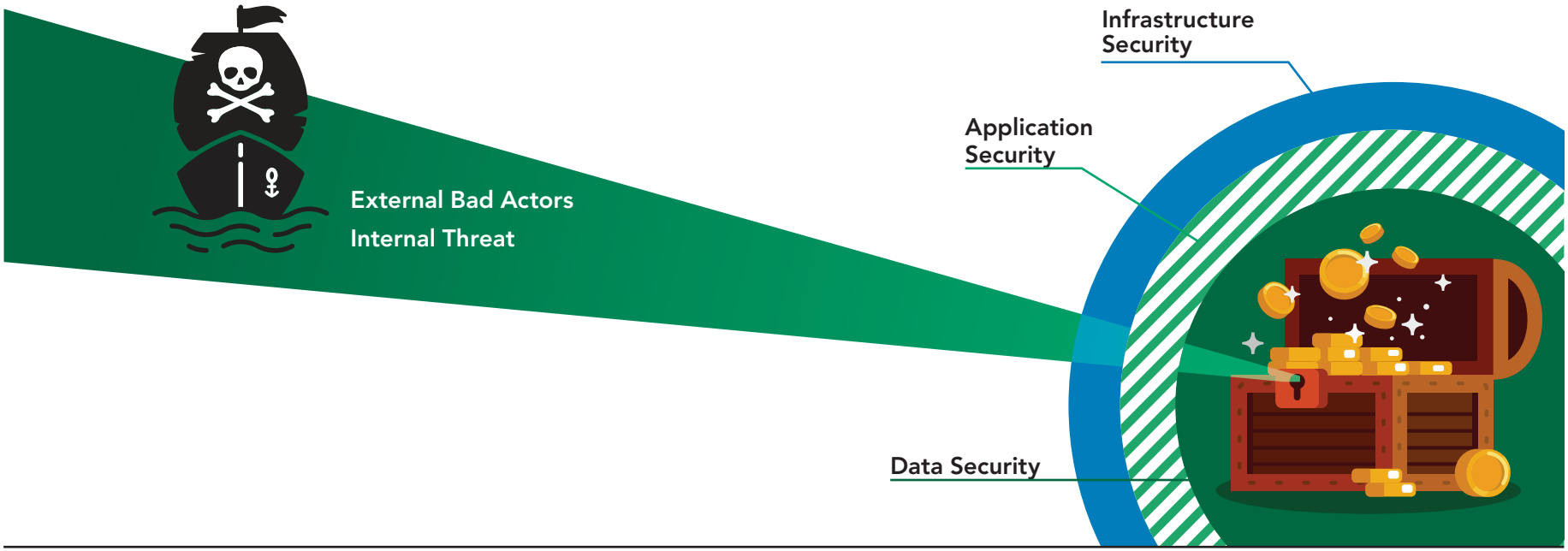
The increase in cyber threats to the financial services industry continues to snowball. As just one example, the FBI stated in 2020 that "ransomware has become one of the most costly and destructive threats to businesses and governments." The FBI reported a 20% increase in "reported ransomware incidents" — outside attacks that shut off access to a company's data until a ransom is paid — "and a 225% increase in ransom amounts."[1] In June 2020 testimony to the U.S. House of Representatives, one industry leader noted that in the first five months of that year, digital crime incidents in the financial industry had increased by a whopping 238%.[2] A March 2021 Harvard Business Review study put it succinctly: "Cyberattacks are inevitable."[3]

The financial services industry is particularly vulnerable. A Boston Consulting Group study indicated that "financial services firms are 300 times as likely as other companies to be targeted by a cyberattack" and that "dealing with those attacks and their aftermath carries a higher cost for banks and wealth managers than for any other sector."[4] To protect against bad actors, particularly in an industry as highly regulated as financial services, financial professionals must take steps to protect both every potential attack surface — from edge devices to data centers — as well as every potential attack timepoint, from Zero Day vulnerability discoveries (that is, the rapid exploitation of a recently discovered vulnerability by a malicious actor) to long-term breaches discovered only weeks or months after a system has been infiltrated. This whitepaper outlines recommended best practices for financial institutions to fully secure their infrastructure, applications, and data from cyber threats both inside and outside their organizations.

Identifying and securing all potential attack surfaces

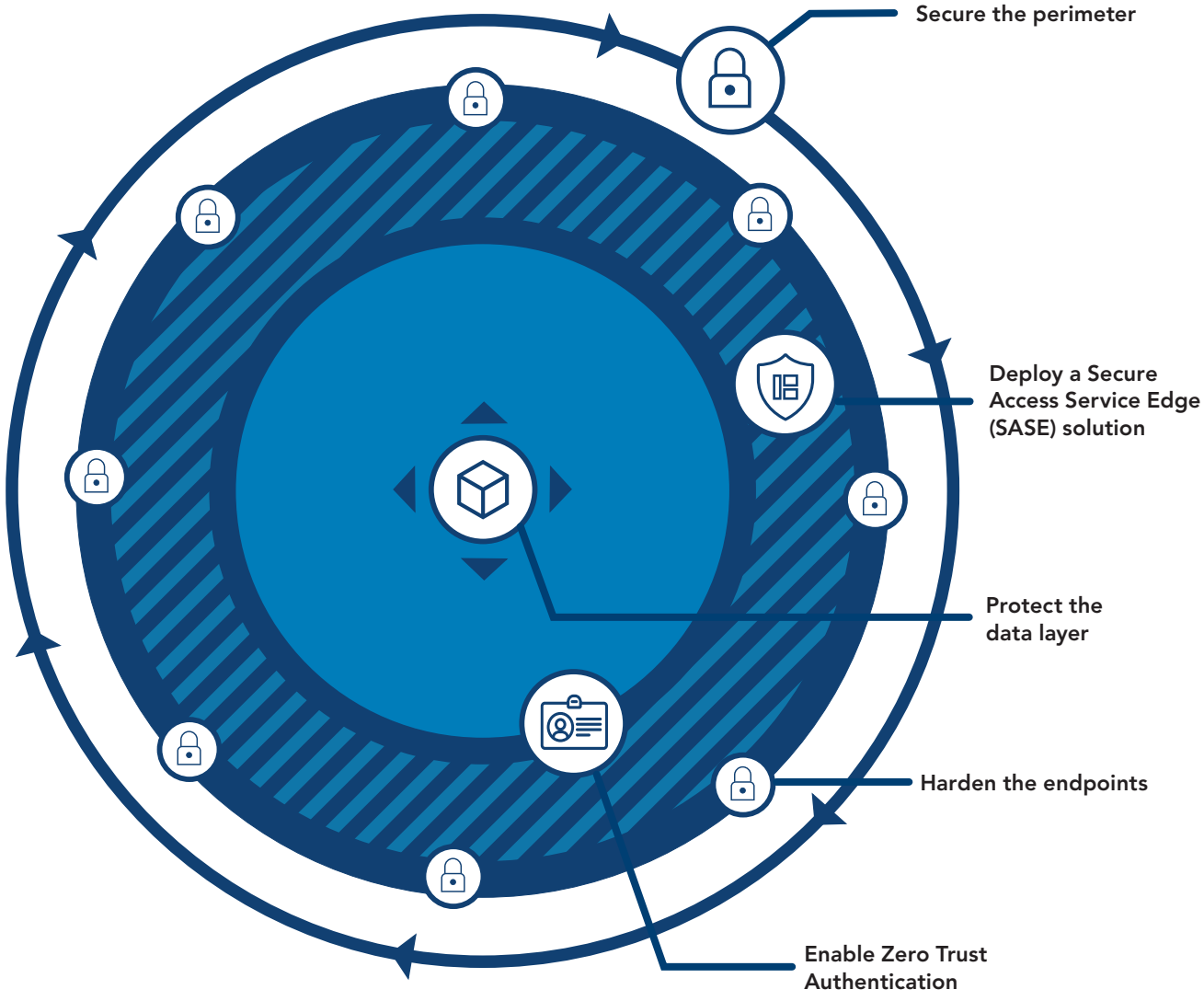
To build a robust security posture to secure digital assets, organizations should begin by identifying every layer of vulnerability in their organizations' networks and infrastructure. Consider a "bull's-eye" model of potential vulnerability, from the edge of your network to the center, where your critical data is stored. By mapping out the structure of your entire network, your organization will gain a full understanding of how end users (including customers and your own employees) gain access to your networks, infrastructure, and data. This in turn will create a roadmap for structuring security measures that protect each layer of your environment from threats both inside and outside your organization.

Consider the diagram pictured above. The perimeter of the network is where external traffic meets your network: the place where desired actors are granted access (such as employees and customers). This desired traffic must first enter through the network layer: gaining access to the physical hardware (cloud data centers, third-party data centers, and on-premises networks) that together comprise your infrastructure. From there, traffic gains access to the applications: the code that powers your intellectual property. Finally, desired traffic can gain access to the data layer: the data lakes and databases holding the critical data without which your organization would not be able to recover from a breach. With most organizations today storing data in multiple locations, every location, both on-premises and in cloud or third-party data centers, must be secured to prevent cyber attacks that could cripple your systems.



A robust security posture demands that every layer of potential vulnerability is met with a multi-pronged response that anticipates both the threats known today, and those that have not yet been imagined. Once you have mapped out your organization's infrastructure, apply the following best practices to develop a security posture that provides protection for every attack surface, at every timepoint in your organization's data lifecycle:

The following sections explain each of these practices in detail.



Secure the perimeter

When it comes to cyber security, the best defense is to prevent bad actors from ever accessing your internal systems. To harden your external security posture (that is, between your network and the public, global Internet traffic attempting to infiltrate your environment 24/7), it is imperative to choose the strongest possible defense for your organization's perimeter.

In data security, the term perimeter layer refers to the technology nested between the Internet and the application. All Internet traffic that attempts to enter the network through the perimeter layer must be analyzed prior to entering your secure network to ensure that it is free from malware or other threats. In other words, perimeter defense is about protecting the outside environment from where end users will attempt to enter your systems.

This practice involves configuring the physical networks within which your applications and data reside, including cloud service providers, on-premises data centers, or private data centers operated by third parties. When designing your perimeter-layer security, consider solutions that allow you to analyze all external traffic coming from the public Internet before it is ever allowed to enter your systems. Engage partners who have created global networks that can analyze traffic before it encounters your organization's infrastructure using tactics such as DDoS (distributed denial of service) mitigation services. Such partners must have the network capacity to defend against the largest possible attacks coming from anywhere in the world.

Further, it is imperative to ensure any public cloud platform utilized by your organization's network is configured properly to restrict access from the public Internet. This can include physical networks and next-generation firewalls. Mature public cloud offerings such as Azure and Amazon Web Services utilize advance threat feeds from credible sources including the Financial Services Information Sharing and Analysis Center (FS-ISAC) from the U.S. Department of Homeland Security to stay abreast of emerging threats: a critical step in future-proofing your organization's security posture.

Enable Zero Trust authentication

The practice of Zero Trust authentication ensures that your network is constantly re-examining the credentials of any outside actor who attempts to access your internal systems. When utilized properly, it is a feature of the perimeter, the network layer, and the data layer: the entirety of the hosting environment in which your applications live.

A Zero Trust authentication model embraces three principles. First, it requires that you verify a user's right to access the network explicitly, by continuously authenticating and authorizing access to your network and systems. Secondly, it requires using least-privileged policies to limit user access with just-in-time and just-enough access. Finally, it requires that you assume that a breach is occurring at any time, by any user. This approach allows you to minimize actual breaches by segmenting access by network, user, device, and application awareness.

This authentication model adds on to the defenses offered via a perimeter-based strategy. While the perimeter solution protects bad actors from entering the network layer in the first place, the Zero Trust authentication model builds on that defense by assuming that at least some bad actors will get into your system no matter how sophisticated your perimeter-based defenses may be. Zero trust protects the assets located inside the perimeter by utilizing strong authentication and security standards that minimize privileged access to the network, offering users access only to those applications and data sources that are required for them to perform the tasks they are inside the system to perform.

When designing your organization's Zero Trust posture, consider building in a Zero Trust Network Access (ZTNA) service. This type of offering creates "an identity and context-based, logical access boundary around an application or set of applications." A well-designed ZTNA requires that access credentials must be re-authorized throughout the time period in which any user has access to internal systems, whether it is an employee who requires some access to secure data, or outside customers who may have entirely different application and data access requirements. The result is a network in which the attack surface is minimized as fewer application assets are visible to public traffic.

Adding Privileged Access Management (PAM) solutions to your Zero Trust posture creates an additional layer of security for your organization's privileged accounts: those that "provide administrative or specialized levels of access to enterprise systems and sensitive data." Finally, create an additional level of security by adding tools that ensure sensitive data can never be directly downloaded if a cyber attack succeeds in breaching the data layer. Simply put, the best Zero Trust models ensure that even if an attacker beats all other layers of security, there will be no data for them to find inside your perimeter if it has been removed via blockchain technology.

Deploy a Secure Access Service Edge (SASE)

The concept of a Secure Access Service Edge (SASE) emerged in late 2019 as Gartner noted that more organizations were moving to security frameworks that packaged existing technologies together to "identify sensitive data or malware" and to offer "continuous monitoring of sessions for risk and trust levels." Gartner defined SASE offerings as those which packaged together a wide variety of security solutions, including software-defined wide area networks (SD-WAN), secure web gateways (SWG), cloud access security brokers (CASB), Zero Trust network authentication (ZTNA, described earlier in this paper), and firewall-as-a-service (FWaaS) offerings.

Together, the SASE environment extends the security posture of your organization's hosting environment all the way to the customer site. For financial services organizations, this means securing the traffic between your organization and the digital banking technologies you utilize from partner organizations to provide value to your end users. A well-deployed SASE leverages technologies including machine learning to constantly analyze traffic to identify abnormal or unexpected behaviors. These could indicate the presence of a malicious actor attempting to gain access via the connection between the financial organization and the digital banking partner.

A SASE solution essentially comprises both a Network-as-a-Service model and a Security-as-a-Service offering layered onto the network, extending to the endpoints in a customer's own environment. Firewalls, WAFs, and SIEM tools can be deployed seamlessly onto these endpoints, no matter where they are located in the network. When considering a SASE solution for your organization's security, ensure that your solution can allow for both the ease of deployment and configuration found in modern SD-WAN solutions as well as the agility required to deploy that security posture across the entire network.

Harden the endpoints

In cyber security parlance, "endpoints" and "perimeters" appear to perform the same task as physical borders that create a secure bubble around your network, applications, and data. However, when we speak of hardening endpoints specifically, we are looking at the entry points through which accepted traffic is allowed to enter your environment, such as customers, trusted partners, and even your own employees. The COVID-19 pandemic moved hundreds of thousands of technology workers to virtual status, requiring them to access sensitive systems and data from remote workstations and from millions of endpoint devices, including laptops, tablets, and mobile phones. Every edge device creates its own set of security challenges. Even a well-meaning employee could unwittingly open a phishing email or access data via an unsecured network, potentially compromising company credentials. These risks are far more than theoretical: a full 42% of financial institutions reported in April 2021 that "the remote working model due to COVID-19 makes them feel less secure."

Hardening the endpoints allows you to control access to your environment no matter how many employees are working remotely, and no matter the security level of the public Internet systems they are utilizing to access your network. An EDR (endpoint detection and response) solution backed by a 24x7 security operations center (SOC) that responds quickly to alerts, as well as third-party validation via monthly endpoint security posture reviews, provides a solution for allowing desired traffic to enter a network remotely. Robust endpoint hardening solutions also include the deployment of static and behavioral AI/ML tools to detect unusual activity, as well as active threat hunting and response and a range of other proactive threat prevention services that focus on preventing bad traffic from entering where trusted users can gain access to the system.

These risks are far more than theoretical: a full 42% of financial institutions reported in April 2021 that "**the remote working model due to COVID-19 makes them feel less secure.**"

Protect the data

The reality of cyber security today is that no matter how robust your posture, eventually you will suffer a breach. What matters most when a bad actor has gained access to your internal systems is implementing steps to protect the critical data, such as personally identifiable information, passwords, and financial details, that are extremely valuable assets to cyber criminals.

This leads to our final best practice in building a robust security posture for financial services organizations: Protect the data. By assuming a bad actor will eventually beat your external systems and infiltrate your network, you can take the steps necessary to ensure that even if that attack finds your data, whether at rest, in use, or in transit, there will literally be nothing there for them to steal.

Consider a data governance and protection solution with the ability to tokenize data using blockchain technologies. Such technologies ensure that data is de-identified using complicated algorithms that make it essentially useless to outside actors who do not have access to the tokens necessary to "re-hydrate" the data. This practice renders data virtually inaccessible to bad actors and provides the highest level of protection for financial institutions and their end users. In summary: when all else fails, use the data to protect the data.

Conclusion

Financial services organizations are in a unique position in today's technology landscape: a highly-regulated industry heavily targeted by cyber criminals, and an industry in which customer trust plays an outsized role in the success of the entire organization. Earning that trust requires deploying the most robust possible security solutions at every stage of the data lifecycle, and from every location where data, applications, and networks risk compromise from bad actors.

Engaging a digital banking partner with industry expertise in cyber security can help financial institutions focus on the work they do best: meeting the needs of a digital-first customer base in a world of increasing threats. Partners with the ability to build out fully-realized security solutions integrated throughout the digital banking platform can help financial services organizations realize the full value of their digital offerings, creating compelling differentiators that help to attract and retain customers. Using this whitepaper as a guideline for evaluating potential partners will help financial organizations identify the partners most able to deliver on both the technology and security solutions required to support the growth and the ongoing health of the organization.

About Q2

Q2 combines two decades of expertise in both financial services and cyber security to offer the best of both worlds for financial institutions of all sizes: a mature security posture backed by deep industry expertise and an ironclad commitment to security as the first goal of the organization. Q2 utilizes a robust portfolio of security solutions to protect customer data. Our technology partners include Cloudflare (edge security), Trustgrid (Secure Access Service Edge), ALTR (blockchain for secure data storage), SentinelOne (behavioral fraud prevention) and many others with decades of industry experience securing the world's largest and most complex technology networks. In combination with our internally developed security solutions including Q2 Trustview, Q2 secures over 20 million end users and over 450 financial institutions moving trillions of dollars annually. For this ongoing commitment to data security, we've been recognized with industry awards from CSO Magazine in both 2019 and 2020.

Sources

[1] America Under Cyber Siege: Preventing and Responding to Ransomware Attacks — FBI

[2] Cybercrime Up 75% During COVID-19, Congressional Hearing Details (cointelegraph.com)

[3] Cyberattacks Are Inevitable. Is Your Company Prepared? (hbr.org)

[4] 10 Statistics that Summarize the State of Cybersecurity in Financial Services (bricata.com)

[5] Definition of Zero Trust Network Access (ZTNA) - Gartner Information Technology Glossary

[6] Privileged Access Management: A Professional Intro to PAM (thycotic.com)

[7] Say Hello to SASE (Secure Access Service Edge)|Gartner Blog Network

[8] COVID Cyber Crime: 74% of Financial Institutions Experience Significant Spike in Threats Linked To COVID-19 | Business Wire

Learn more

Schedule a conversation today to learn how Q2 can help your financial institution create compelling digital banking services backed by industry-leading cyber security solutions.

Q2