Is your financial institution future-ready? Modernizing endpoints for success

Financial services (FinServ) is one of the most highly regulated industries in the world due to the need to protect consumers' sensitive, personal and financial data from threat actors. Like almost every major industry in recent years, FinServ has undergone widespread digital transformation to support new customer offerings and modernize the employee experience. In fact, most financial institutions now manage **100,000 or more endpoints**, and **at least 90%** of FinServ organizations maintain some data, applications or operations in the cloud.

Meanwhile, **more than two-thirds of banks** now offer workers full or partial hybrid work arrangements, and many financial institutions have adopted virtualized desktop infrastructure (VDI) to provide secure, remote access to files and systems. Banking, financial services and insurance sectors are among the **top two consumers of VDI**, behind IT and telecom and ahead of healthcare. In addition, FinServ desktop virtualization is expected to grow at a CAGR of **50.55% through 2028**.

This movement toward virtualization has opened up a new world of opportunities for FinServ IT teams, while also creating a few distinct challenges. In this paper, we'll outline how a modern endpoint strategy can help financial institutions address key challenges they face now — including bolstering cybersecurity, streamlining the employee user experience and reducing IT complexity — while preparing for what's coming next.

Three challenges facing today's FinServ IT teams

Financial institutions are under pressure to be proactive as both digital demands and threats grow in scope. Some of the most pressing needs relate to FinServ organizations' many endpoints, including:

1 Bolstering cybersecurity at the endpoint

To securely support remote work, IT teams must reduce threat exposure at the endpoint.

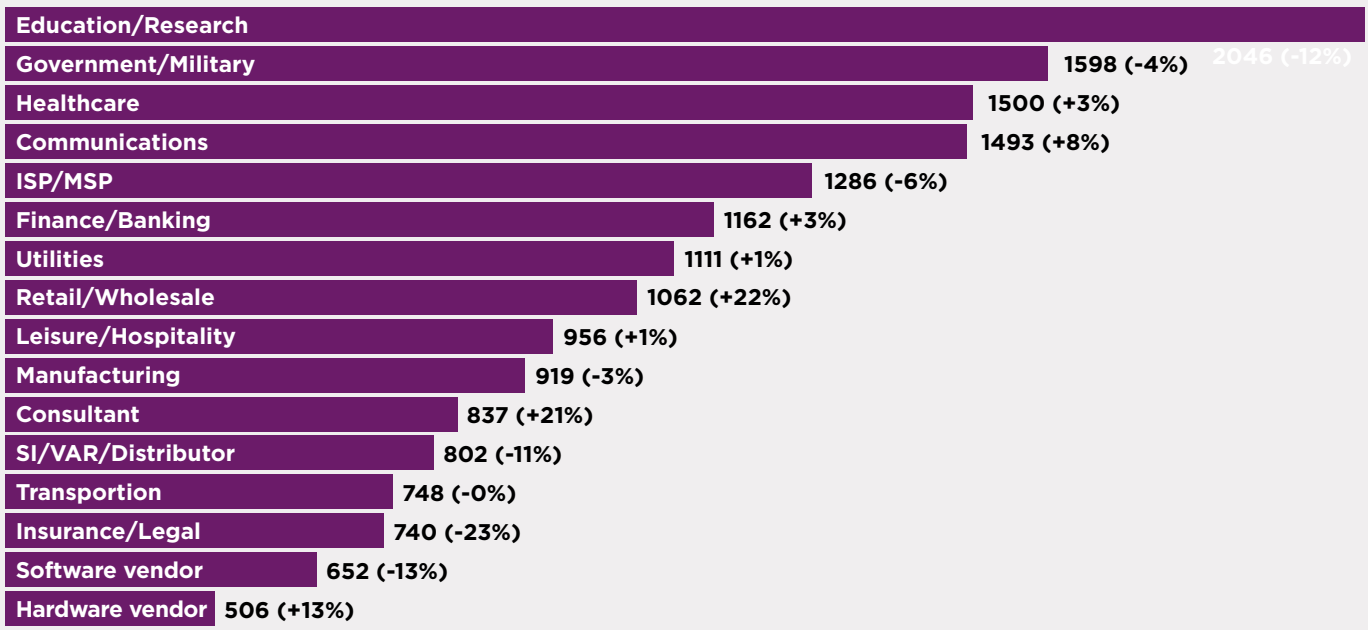
For decades, the financial industry's rigorous standards and regulations have compelled FinServ institutions to follow strict cybersecurity protocols. As a result of these defenses, banking and credit union systems have historically been difficult to breach, driving many cyber attackers to focus their energy elsewhere. But now, as financial institutions support remote work with virtualization and cloud connectivity, attackers have developed a renewed interest in finding and exploiting vulnerabilities in bank and credit union cyber defenses by attacking employees' devices.

Among enterprises across industries, **70% of today's breaches** originate at the endpoint. As workers connect to their home networks, they expose company systems to a wide range of cyber threats, including ransomware and other malware that may have been acquired by other users on the network.

Threat actors have been quick to exploit this increased exposure. In 2021, weekly attacks against financial institutions increased by 53%, with the average institution fielding 703 attacks per week. By 2023, that number reached **1,162 attacks per week**. When a breach succeeds, it costs the institution an average of **$5.72 million per incident** and takes an **average of 233 days** to detect and contain.

Global average of weekly attacks per organization by industry in 2023

(% of change from 2022)



Source: **CHECK POINT RESEARCH. 2024 Cyber Security Report.**

Regulators are working to update requirements to improve security across the FinServ organization, including at the endpoint. In addition to the vulnerabilities that come with network connectivity, risks exist along the entire chain of custody of the physical device, starting with the manufacturing and shipment of each intelligent component to the device maker. To ensure security, device makers must enact zero trust policies across their entire supply chain, thoroughly evaluating each supplier's development and manufacturing process to help identify and mitigate security risks.

In June 2023, three regulatory agencies — the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (FDIC) — announced they would **now include supply chain risk** when assessing third-party risk and vendor management, which extends to device manufacturers.

Banks know they need more defenses in place — **43% of senior bank executives** admit their bank is not adequately equipped to protect customer data, privacy and assets from a cyberattack. But for many, the optimal approach to endpoint security has proved elusive.

2 Streamlining employee UX

FinServ institutions must create a consistent employee experience on top of fragmented technology.

As of 2021, despite being in the midst of a digital transformation, only **5% of banks** said their technological framework was cutting-edge. More often, financial institutions have modernized by implementing new technology alongside their legacy systems, leaving many organizations with a mix of disjointed hardware and applications and creating an inconsistent employee user experience.

In addition, banking merger and acquisition (M&A) activity **ramped up between 2017 and 2021**, giving banks an influx of disparate technologies. McKinsey & Company **tracks activity associated with banking M&As** and has found that, while technology integration strategies would be most impactful during the first 100 days after closing, many banks miss the opportunity to get ahead of integration needs and then become stuck with divergent technology. Although M&A activity has slowed, many financial institutions are still figuring out how to streamline the fragmented technology they have acquired over the years.

For these reasons, it is not unusual for FinServ employees at the same company to be working on different devices and sometimes even using different software. When one employee has a fast interface while another struggles with an outdated device or connection, this inconsistency can lead to reduced productivity and employee dissatisfaction. Employees may even attempt to find a "fix" for these inconsistencies on their own, leading them to follow online help articles that, if incorrect or compromised with malware, can create further opportunity for exploitation.

3 Reducing IT complexity

IT teams need to streamline the management of their increasingly complex environments.

This diversity of endpoints and systems not only affects the average employee's experience, it also significantly increases the IT management burden for FinServ tech teams. **More than a third of banks** name complex systems as one of their top challenges. For example, McKinsey & Company found that the number of applications in a financial institution's environment is a **good measure of that organization's IT complexity**. Interestingly, as banks increase in size, they never achieve economies of scale — their environments simply become more complex.

One reason this complexity is cause for concern is that financial institutions are experiencing a shortage of IT talent to manage their environments. In recent years, the Global Workforce Intelligence Project found that **four out of ten tech jobs for banks** would not be filled by tech professionals with industry experience — and that gap has only grown.

Patch management can be one of the hardest tasks for busy IT teams to stay on top of, especially when managing updates and patches for hundreds of thousands of institutional endpoints. It takes financial institutions **an average of 54 days** to patch known vulnerabilities, exposing their data and systems to threat risks.

Streamlining endpoint management can make these types of tasks significantly easier, even for less-experienced IT teams. For example, teams can rapidly respond to exposed cyber threats with a unified endpoint strategy, rolling out the same mitigation measures across all endpoints at once.

Top five IT challenges on the road to digital transformation

Conflicting priorities

Nearly 80% of IT staff in banks spend the majority of their time on recurring tasks.

Complex systems

36% of banks name complex systems as a top challenge faced by organizations.

New technologies

Only 5% of banks would consider their technological framework to be cutting-edge.

Budget constraints

57% see the lack of budget allocation as a concern for innovation.

Lack of talent

40% of banks are getting by without a consistent technology experience.

Cloud-client computing + purpose-built hardware: An endpoint strategy for what's now and next

These pressing FinServ IT challenges at the endpoint can be solved by leveraging a modern cloud-client computing model — deployed on standard PCs — using a next-gen operating system (OS) purpose-built for the cloud.

As a highly regulated industry, the FinServ space was one of the early users of cloud-client computing. However, many IT teams may not be aware how this endpoint model has evolved to fit modern use cases.

What is cloud-client computing?

Cloud-client computing is a cloud-first model in which an organization's mission-critical data and applications are stored in the cloud, and employees access those systems through a secure, virtual desktop environment. This model enables FinServ employees to work from anywhere while theoretically limiting the amount of company data they need to store on their devices.

However, if those employees are still using PCs with a consumer operating system (OS) installed, their ability to store information is not inherently limited. In other words, they can still potentially download sensitive information — or malware — exposing the rest of the organization and its customers to threat activity. In addition, they will able to configure and customize their devices, sometimes accidentally introducing vulnerability in the process.

Historically, this is why organizations employing a cloud-client computing approach used thin or zero clients — read-only devices with limited or no connectivity and restricted use cases focused on task-based workloads.

Today, financial institutions can achieve the full benefits of cloud-client computing on their existing fleet of PCs by installing a next-generation, read-only endpoint OS.

The secure endpoint OS is purpose built to connect users to cloud-based applications, virtual desktops and company data centers. It supports not only commonly used peripherals, like scanners, check printers, readers, webcams and headsets, but also virtual desktop infrastructure (VDI) agents, cloud storage and the cloud-client computing model — giving IT teams the ability to instantly turn any endpoint into a workstation of the future.

What is purpose-built hardware?

While financial institutions can deploy cloud-client computing on their existing fleet of devices, as they begin to replace those endpoints over time, they can further extend the benefits of this model by selecting purpose-built hardware. That means choosing devices that are built for reparability, longevity and reliability, all on a secure framework.

With the new regulatory focus on third-party supply chains, it is also important that new hardware be manufactured and delivered using a Zero Trust secure supply chain.

What's now

Shifting to a cloud-client computing model by deploying a secure endpoint OS can help FinServ organizations solve their most pressing endpoint challenges in an approachable and cost-effective way. This approach unlocks a few key benefits:

Reduces threat exposure at the endpoint and supports Zero Trust architecture.

By deploying a secure endpoint OS, financial institutions can benefit from increased security measures that protect against an employee's accidental or malicious downloading of malware. The OS's read-only design reduces its vulnerability to attacks and unauthorized modifications, making it highly resistant to tampering and malware. Moreover, the modular nature of the modern OS means that only the resources and tools required for the user's task need to be installed. This results in a strong security posture that helps to narrow the threat opportunity and protect sensitive information.

In addition, implementing a read-only OS allows organizations to simplify their security infrastructure by reducing the need for multiple third-party solutions and agents. This consolidation streamlines security operations and minimizes potential vulnerabilities that can arise from managing multiple software components.

Provides a consistent employee experience across endpoints.

The secure endpoint OS can be installed on most devices, including older x86 pc hardware, giving financial institutions a simple way to unify the endpoint experience across employee devices. All employees will see the same interface upon signing in and enjoy the same streamlined cloud and server connectivity, reliability, uptime and speed.

Nearly **80% of workers** use collaboration tools today to conduct meetings and customer service, including many financial institution employees. The GPU requirements to run these productivity applications are high, creating special considerations for IT teams who want to ensure employees have a seamless experience when using these applications in the cloud.

On certain purpose-built devices, the secure endpoint OS can also be elastic, meaning it can support existing remote display protocols from the key vendors in the virtualization space, but also purpose-built agents that intelligently redirect how and where to render the application or even redirect what peripherals to use locally on the endpoint. It can ensure that resource-intensive applications running in the cloud offload the heavy processing load to the local endpoint, relieving the cloud host of that burden so more virtual desktops can reside on it. This has the added benefit of increasing the host density and can decrease the cost of each virtual desktop..

A secure endpoint OS can also use protocol optimizations to avoid sending call or video data back and forth to the cloud — an undesirable process called hairpinning that affects network traffic. Instead, it will redirect audio and video directly to the intended recipient, reducing unnecessary network traffic.

Moreover, the secure endpoint OS can speed up the onboarding process for refreshed devices and new hires. Financial institutions can order new devices with the secure endpoint OS pre-installed, enabling the factory to ship the device directly to the employee, who enters their password to log in to their virtual workspace. This streamlines the onboarding process by surpassing the need for FinServ IT teams to set up new devices, download the right applications for each user's role, ship the devices to the users, and work with the user to connect to the appropriate virtual environments. With a secure endpoint OS, onboarding takes as little as one day instead of weeks.

Streamlines IT management

In addition to reducing threat exposure at the endpoint and unifying the employee experience — both of which save IT time and resources — the secure endpoint OS can reduce IT management challenges.

Patch management can be one of the hardest tasks for busy IT teams to stay on top of, especially when they must manage updates and patches for hundreds of thousands of institutional endpoints. However, when a financial institution is using a secure endpoint OS, IT teams can patch and update one centrally managed, cloud-based Windows implementation.

IT teams can also update the next-gen endpoint OS and its applications seamlessly from a central location without the need for additional software like a virtual private network (VPN). The secure endpoint OS acts as a virtual tunnel, supporting secure and encrypted two-way communications based on open communication standards like TLS/SSL encryption and WebSocket protocol.

What's next

Of course, as financial institutions solve the challenges of today, they also must think long-term, future proofing their endpoints without knowing exactly what challenges lie ahead.

The secure endpoint OS and purpose-built hardware provide an adaptable solution that can help FinServ IT teams meet future challenges and maximize opportunities as they arise, including:

The rise of AI personas

In the future, financial institutions will use AI personas to support decision making and enhance security. For example, when an employee's behavior or actions are not consistent with their job roles or functions, AI will be able to observe these unexpected behaviors and respond according to the organization's protocols. This pro-active AI behavior will provide real-time response to active threats.

The secure endpoint OS will be poised to support the use of AI personas by enabling financial institutions to roll out AI modules over the entire environment, regardless of device or location.

Using the OS on purpose-built hardware further enhances these capabilities by enabling intelligent threading and routing of AI workloads to devices or servers with the capacity to handle them.

Compliance changes

In a highly regulated and dynamic space like FinServ, compliance requirements change frequently. The secure endpoint OS is not only read-only, inherently enhancing security and compliance, it is also modular. IT teams can add, remove, modify or distribute applications. For example, if regulations change to require more characters in an employee password, IT teams can make those updates and distribute that instruction set across the entire environment.

Purpose-built hardware is also designed to meet upcoming compliance requirements. For example, today's future-proof devices should be built to accommodate generation 10 of TCO Certified sustainability criteria, knowing that requirement will go into effect in 2026.

AI may further help financial institutions to adhere to regulatory changes by automatically monitoring compliance-related tasks and guiding the organization to implement changes as they are needed.

Scalability needs

As financial institutions continue to grow their footprint through M&A activity, the secure endpoint OS will enable them to scale their fleet more quickly. This uniform OS works regardless of the generation of devices in use and can maintain a consistent employee UX across any number of devices.

The flexibility of this solution enables FinServ organizations to keep endpoint management streamlined and simple as the organization scales up or down, while also enabling faster employee onboarding.

Implementing your now and next endpoint strategy with IGEL and Lenovo

Getting started with a cloud-client computing strategy is much faster and easier with the right partners. Lenovo has teamed up with IGEL OS to provide financial institutions the ultimate cloud-connected device. Designed for the cloud, IGEL OS solves many of today's most pressing FinServ IT challenges. It delivers:

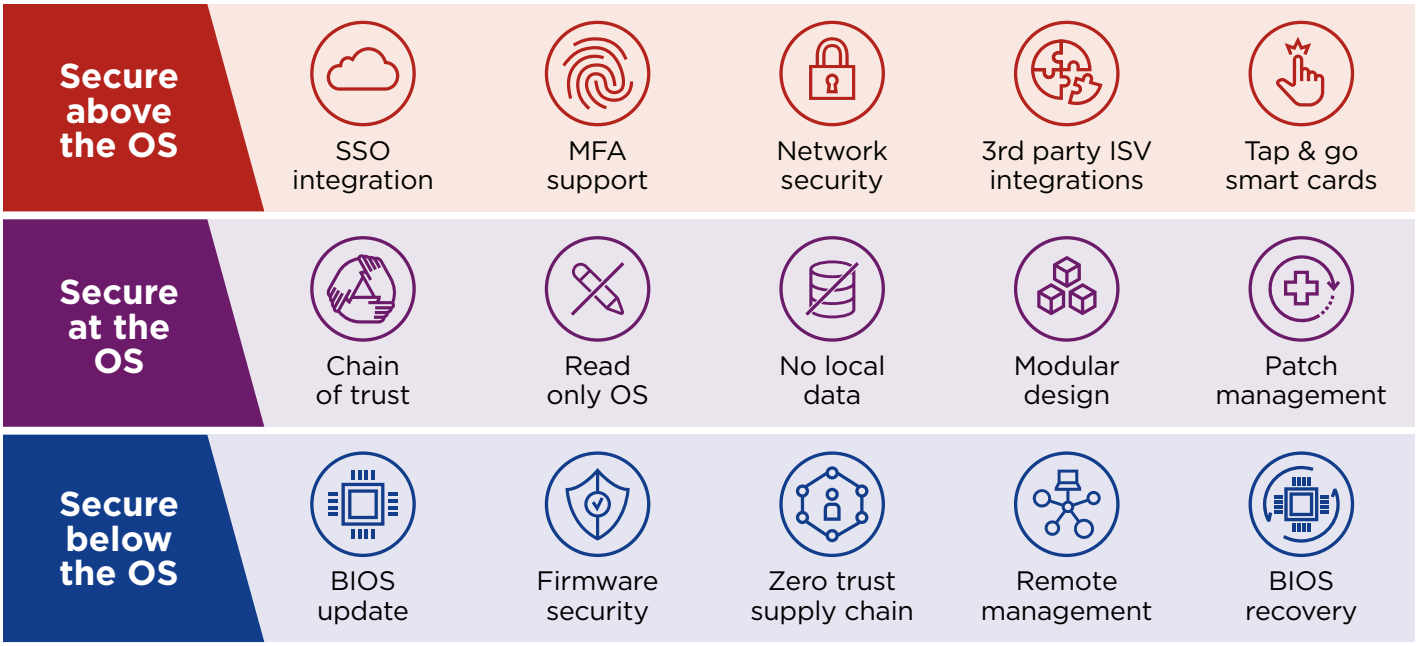
1. **Intrinsic endpoint security enhancements** — The read-only format automatically reduces threat exposure at the endpoint, regardless of the network being used to connect to company systems.

2. **Consistent employee experience** — IGEL OS can be installed on virtually any endpoint, overcoming the inconsistent internal UX that can result from M&A activity and maintaining legacy system investments.

3. **Ease of management** — IT teams can streamline patching and updates across their endpoints without needing expensive VPNs.

4. **Future-proof adaptability** — IGEL OS is designed to meet the needs of today and adapt to whatever the future holds for financial institutions.

By using IGEL OS to run purpose-built Lenovo devices, financial institutions unlock the ultimate cloud-connected device. IGEL and Lenovo, powered by Intel, work together to provide multiple layers of preventative to security to help keep customers' sensitive data safer from cybercriminals and other threats.



Today's FinServ IT challenges are simple to address for teams who are willing to shift to a modern cloud-client computing model using a secure endpoint OS. Behind every challenge for IT teams is an opportunity to enhance security, improve employee experience and streamline technology management.

Having the right partners in your corner can make any technology transition easier. To learn more about working with Lenovo and IGEL, **contact us**.

About Lenovo

Lenovo (HKSE: 992) (ADR: LNVGY) is a global technology powerhouse serving millions of customers every day in 180 markets. Focused on a bold vision to deliver smarter technology for all, Lenovo has built on its success as the world's largest PC company by further expanding into growth areas including software. Whether it's supporting hybrid work environments, enabling smart homes, empowering small and medium-sized businesses, revolutionizing AI gaming experiences, or enhancing digital learning, Lenovo Cloud and Software's portfolio of innovative solutions empower our customers to thrive in the ever-evolving digital landscape. Lenovo's world-changing innovation is building a more inclusive, trustworthy and smarter future for everyone, everywhere. To find out more, **visit our website**.

About IGEL

Today, the world of work is hybrid. Multiple clouds can deliver applications sourced from anywhere to a widely distributed workforce using all types of devices. Right at the moment when the world of work needs it most, IGEL has the solution for fully managed, secure endpoint access to any digital workspace that gives IT teams strong control and end-users the freedom to work as they wish in a hybrid world. Enabling choice of any cloud, from any device, anywhere, IGEL unlocks a collaborative and productive end user computing experience while solving the common security and management challenges required to compete and win in today's world of hybrid work. With a growing ecosystem of more than 100 IGEL Ready technology partners, IGEL has offices in Europe and the United States and is represented by partners in over 50 countries. For more information on IGEL, visit **IGEL.com**.