HCLSoftware

Continuous Endpoint Control for the Banking Industry

Reducing Operational Risk Through Scale, Remediation, and Continuous Compliance

HCL **BigFix**

Endpoint Risk Has Become a Banking Resilience Problem

In financial services, **86% of breaches cause operational disruption**, with average breach costs exceeding **USD 5.5 million**[1], and attackers exploit **known but unpatched vulnerabilities**. As banks expand into more branches, ATMs, data centers, cloud infrastructure, and employee endpoints, the attack surface grows faster than traditional device management can keep up.

For CISOs, CIOs, and executive leadership, endpoint risk is no longer an IT issue. It directly affects service availability, audit outcomes, and market confidence. Fragmented tools and episodic compliance checks create blind spots that attackers exploit and regulators question. What was once treated as a technical control issue has become a business continuity and resilience challenge.

This solution brief examines the structural challenges redefining endpoint risk in banking, the resulting business impact, how HCL BigFix addresses these barriers, and what effective endpoint control looks like across the bank.

The Structural Challenges Redefining Endpoint Risk in Banking

A lack of security tools or visibility no longer constrains modern banking environments. Instead, risk accumulates when high-priority vulnerabilities, especially those most likely to be exploited by hackers, remain unpatched. This happens when controls are not enforced continuously, remediation cannot keep pace with exposure, and human-driven processes fail at scale. We see some of these challenges across organizations, like:

Configuration drift increases audit risk

Banks face a growing gap between the speed at which vulnerabilities emerge and the speed at which they are remediated. According to the IBM Cost of a Data Breach Report 2025, **86% of financial services breaches result in operational disruption**, with an average cost exceeding **USD 5.5 million**. At the same time, the Verizon 2025 Data Breach Investigations Report shows that **vulnerability exploitation accounts for 20% of initial breach vectors**, yet only **54% of vulnerabilities are fully remediated**, with a **median remediation time of 32 days.**[2]

This gap between exploitation and remediation allows known weaknesses to remain exposed long enough to translate into real operational and financial impact.

Human-centric security operations fail at banking scale

The scale of modern banking infrastructure has outgrown manual enforcement and response models. Banks manage millions of endpoints across branches, data centers, cloud platforms, and employee devices, while security and IT teams remain lean. IBM reports that **48% of organizations experience a high security skills shortage**, and those organizations incur significantly higher breach costs, averaging **USD 5.22 million compared to USD 3.65 million** where shortages are minimal.[3]

Compounding this challenge, the Microsoft Digital Defense Report indicates that **80–90% of ransomware incidents originate from unmanaged or weakly managed devices**[4], highlighting that the core issue is not awareness but the inability to act consistently and quickly at scale.

Compliance remains episodic rather than sustained

In many banking environments, compliance is still treated as a point-in-time exercise rather than an enforced state. IBM findings show that the average breach cost of **noncompliance with regulations is approximately USD 5 Million**[5], underscoring the heavy penalty cost coupled with the material impact of control gaps. Periodic assessments and audit-driven checks fail to capture day-to-day configuration drift, allowing compliance posture to degrade silently between audit cycles.

As a result, banks often discover gaps only during audits or after incidents, when remediation is most disruptive.

How Structural Challenges Translate Into Banking Risk

These challenges do not exist independently. They reinforce one another, creating systemic weaknesses that surface as persistent operational, security, and regulatory issues across banking environments.

Breaches cause operational disruption

When exposure grows faster than remediation, security incidents rarely remain isolated. Breaches cascade into downtime, degraded services, delayed transactions, and costly incident response efforts, directly affecting customer trust and business continuity.

Known weaknesses enable modern attacks

Unpatched risks and misconfigurations continue to serve as reliable entry points for attackers. Without consistent enforcement, these known issues evolve into service disruptions and ransomware events rather than remaining theoretical risks.

Scale overwhelms security and IT capacity

As endpoint estates expand, manual processes struggle to keep pace. The result is slower decision-making, delayed response, and uneven execution across environments, particularly during high-pressure incidents.

Control breaks across heterogeneous environments

Diverse operating systems, platforms, and deployment models make consistent policy enforcement difficult. Gaps emerge when controls cannot be applied uniformly across servers, workstations, cloud workloads, and remote endpoints.

Compliance gaps surface between audit cycles

Without continuous enforcement, configuration drift accumulates between audits. Banks are left exposed to regulatory findings and operational risk long before formal assessments bring issues to light.

How HCL BigFix Addresses Banking Industry Challenges

HCL BigFix enables banks to move from reactive, point-in-time control to continuous enforcement across the endpoint lifecycle.

Delivers reliable and prioritized remediation without disruption

HCL BigFix achieves over **98% first-pass patch success**, cutting remediation cycles from weeks to hours. Backed by a continuously maintained library of **500k+ remediations across 100+ OSs and 400+ Software titles**, HCL BigFix executes remediation with prioritization, consistency, and validation across complex banking environments.

Banks can achieve significant savings, potentially millions, by preventing security breaches. They can concentrate their efforts on the highest-risk exposures and remediate them proactively, eliminating threats to the security ecosystem before they can materialize.

Scales to banking environments

HCL BigFix manages **155M+ endpoints globally** and supports over **300,000 endpoints per server**, enabling banks to operate at massive scale across a diverse set of endpoints, including laptops, mobile devices, ATMs, kiosks, and more. While maintaining centralized control and visibility, HCL BigFix replaces an average of six tools with one unified and cohesive solution. This can enable banks to autonomously execute security solutions across a wide variety of devices and tools, significantly reducing the time required.

Makes compliance continuous

HCL BigFix continuously enforces security solutions using **50,000+ out-of-the-box compliance** checks across **PCI-DSS, DISA-STIG, CIS, and NIS2 frameworks**, helping organizations maintain **more than 99% compliant endpoints** at all times. The solution enables the customization and enforcement of policies tailored to the bank's environment. Banks can significantly reduce the time required for compliance response, from **weeks to minutes**, by leveraging the solution's ability to generate audit evidence and historical reporting on demand. Furthermore,

What Endpoint Control Looks Like with HCL BigFix

Security and risk leadership

(CISO, Head of Cybersecurity, Security Operations)

Reduce financial loss and operational disruption from breaches

Banks can continuously discover endpoint state and validate that patching and remediation have been applied across critical systems, significantly shrinking exposure windows before vulnerabilities turn into incidents and cause downtime.

Protect revenue-generating systems from ransomware and targeted attacks

HCL BigFix enables security teams to prioritize and remediate vulnerabilities autonomously across large, distributed endpoint estates, focusing on weaknesses most likely to be exploited. This shifts effort onto real attack paths and materially reduces exposure, response time, and breach-driven disruption.

IT operations and infrastructure

(IT Operations Head, Endpoint and Infrastructure Teams)

Accelerate risk response with near real-time endpoint visibility

A single source of truth for servers, workstations, and mobile devices, which gives IT teams an accurate, current view of what exists, what changed, and what needs action across the endpoint lifecycle.

Simplify endpoint operations by consolidating fragmented tools

Discovery, patching, remediation, asset management, and compliance are executed through a single cohesive solution, reducing operational friction, manual data reconciliation, and execution delays caused by tool sprawl.

Compliance, risk and audit

(Chief Risk Officer, Compliance Head, Internal Audit)

Audit-ready compliance without audit-time fire drills

Give compliance leaders continuous visibility into policy enforcement across endpoints, ensuring audit-ready evidence is always available and eliminating the hassle of last-minute remediation.

Environment-specific compliance with historical reporting

Enable customization of compliance checklists based on the environment and continuously enforce them across endpoints. Historical reports provide clear evidence of compliance posture over time, not just at audit checkpoints.

Executive and scale owners

(CIO, COO, CEO)

Enable secure scale without increasing headcount or complexity

Large, distributed banking environments are managed through automation across the lifecycle, patching, and remediation, allowing growth without adding tools or operational staff.

Preserve uptime across always-on banking systems during remediation

Patches and configuration changes are executed with high first-pass success, ensuring critical services such as payments, trading, and branch systems remain stable while reducing security risk.

HCL BigFix – Built for Banking Scale and Regulatory Confidence

HCL BigFix provides a single, trusted foundation for endpoint lifecycle management, remediation, and continuous compliance. It enables banks to reduce risk, stabilize operations, and meet regulatory expectations while maintaining the availability and trust the industry demands.

Explore how HCL BigFix can support your banking operations at scale and help keep them secure and compliant.

Visit the **HCL BigFix Banking Solutions.**

Ready to assess your endpoint risk posture?

Contact us to speak with an HCL BigFix expert.

Sources:

1 https://www.ibm.com/reports/data-breach
2 Verizon 2025 Data Breach Investigations Report
3 https://www.ibm.com/reports/data-breach
4 Microsoft Digital Defense Report
5 https://www.ibm.com/reports/data-breach