



INSIDE
BANKING AND
FINANCE IT

Why Effective IT Administration Holds the Key to BFSI's Digital Future

Trend Guide

Complexity as the New Normal in BFSI

The BFSI sector is under constant pressure to innovate while managing a broad and increasingly fragmented IT environment. From hybrid work and AI tools to legacy systems like ATMs and core banking infrastructure, **IT teams are expected to manage it all** – securely, efficiently, and in line with regulatory expectations.

The goal of this report is to equip you with relevant data and actionable insights that help you move from reactive firefighting to proactive innovation. Structured around core trends, this report explores:



**Hybrid work
and BYOD adoption**



**Endpoint
cybersecurity risks**



**Regulatory
compliance
pressures**



**The rise of UEM
and DEX tooling**

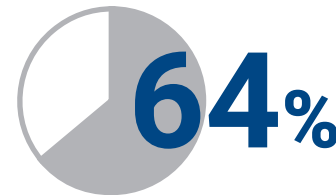
Hybrid Work and IT Fragmentation

The 2020 pandemic has permanently changed BFSI work culture. Hybrid setups are now the standard, with field agents, branch employees, and corporate teams operating from multiple locations. This means IT admins must oversee infrastructures with a growing number of diverse devices across on-premises, remote, mobile and home office locations.

Forrester's 2023 BFSI Digital Operations Brief highlights a **40% increase in endpoint-related IT tickets in banks** that shifted rapidly to hybrid computing without sufficient endpoint monitoring or management automation.



of financial IT teams now support hybrid or fully remote work models (IDC, 2023)



of daily BFSI work occurs in cloud/web-based apps (Forrester, 2023)



of finance employees report increased productivity due to hybrid flexibility (Kyndryl, 2023)

Implications



- Growing demand for centralized device management
- Increased complexity from OS and hardware diversity
- IT must ensure consistent security, updates and support across all endpoints

BYOD: Productivity Driver and Security Risk

BYOD adoption has surged, especially in mobile-first use cases like relationship management, field inspections, and sales. But allowing personal devices onto corporate networks without structured controls invites considerable risk.

According to ISACA's 2023 Banking Security Study, **52% of mid-sized banks** in the EU cite BYOD as their primary endpoint visibility gap and top internal audit concern—particularly in business continuity and fraud prevention contexts.

+

- › Up to 68% productivity gain among users with mobile access (Bitglass, 2022)
- › Cost savings of ~\$250–350 per employee/year (Gartner, 2023)
- › 75%+ of BFSI workers now use personal devices at least occasionally for work (ENISA, 2023)

-

- › 32% of firms have no formal BYOD registration (ENISA, 2023)
- › 17% of users access company data without informing IT (IDC, 2023)
- › Limited or no endpoint visibility increases security and compliance exposure

SOLUTION

- › **Unified Endpoint Management (UEM) tools are essential to: Register and monitor BYOD assets**
- › **Enforce device encryption and app restrictions**
- › **Wipe or lock compromised devices remotely**

Cybersecurity Risks: Endpoints Are the New Frontline

FS-ISAC's 2023 Regional Cyber Resilience Report shows that mid-market institutions now rank endpoint compromise as the **#1 root cause for fraud losses**, ahead of phishing and credential theft. This makes endpoint protection a critical control for fraud prevention teams.

Endpoints remain the top attack vector, with phishing, ransomware, and insider threats targeting user devices directly.



of EU banks and 17% of insurers experienced ransomware in 2023 (ENISA Threat Landscape, 2023)



of BFSI firms still do not encrypt data at rest on endpoints (Jones Walker Financial Services Cybersecurity Survey, 2024)



Only 40% of critical vulnerabilities are patched within 30 days (Qualys Security Report, 2023)

4

of the top five AI-related risks in financial services are data privacy and protection (UK Financial Conduct Authority (FCA), 2025)

GROWING INVESTMENT

- › Cybersecurity budgets now consume **9–10% of BFSI IT** budgets (ENISA, 2024)
- › Endpoint Protection Platform (EPP) adoption is nearly universal, but many mid-market orgs **lack advanced EDR/XDR**



PRIORITY AREAS

- › Full-disk encryption and effective key management
- › Timely, automated patch management
- › Antivirus and malware behavior detection
- › Regular vulnerability scans with actionable insights
- › AI apps and tools - including cybersecurity solutions - with data privacy built-in

Regulatory Pressures Accelerate Modernization

Both EU and US regulators are tightening expectations:

IN THE EU



- **NIS2 Directive (2024):** mandates security and operational resilience across critical sectors, including BFSI
- **DORA (2025):** sets ICT risk requirements covering endpoint hardening, encryption, and response capabilities

IN THE US



- **FFIEC guidance:** calls for risk-based endpoint controls
- **GLBA and SEC regulations:** highlight the need for incident reporting and cyber hygiene

Capgemini's 2023 Financial Services Compliance Outlook shows that **71% of EU-based financial firms are reviewing or re-structuring their endpoint security policies due to DORA**. Similarly, 62% of mid-sized US banks have initiated IT compliance gap analyses ahead of GLBA amendments.

Hence, compliance is shifting from documentation to execution. Regulators expect **auditable security outcomes** – not just policies.

Unified
endpoint
visibility

Policy
enforcement
(e.g., password
rules, remote
wipe)

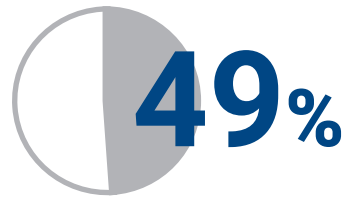
Logging
and alerting
integrations

Ongoing
compliance
validation and
evidence
collection

From Control to Experience: The Rise of DEX

BCG's 2023 Banking Workforce Benchmarking Report found that banks with DEX programs report **2x higher satisfaction** among field employees and relationship managers and **23% lower internal support costs**.

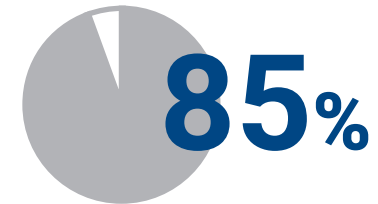
Digital Employee Experience (DEX) solutions close the loop between endpoint operations and user productivity. In BFSI, where time and trust are critical, latency and downtime can be costly.



49% of BFSI firms use DEX tools to monitor endpoint performance and user experience (Forrester, 2023)



76% of teams now dedicate 10–20 hours/week to proactive user support (Auvik, 2024)



85% of insurers prioritize ESG in core functions (PWC, 2023)



57% of BFSI organizations now report DEX metrics to CIOs (Gartner, 2023)

Why it matters

- Resolving endpoint issues before tickets are submitted boosts satisfaction
- DEX insights improve IT budgeting, tool selection, and vendor management
- Employee experience is increasingly linked to business outcomes
- Extending device lifecycles lowers both costs and carbon emissions.

Turn Complexity Into Competitive Advantage

Modern BFSI IT leaders are not just caretakers of legacy systems. They are enablers of innovation, security, and compliance. As complexity grows, IT success depends on choosing the right foundation to meet those needs.

Start turning complexity into clarity – and legacy into leadership

You want to know more?

[> Link](#)

Start your journey to a securely and efficiently managed infrastructure here

Action checklist

- ✓ Consolidate tools with a UEM platform
- ✓ Secure every endpoint (encrypt, patch, protect)
- ✓ Formalize BYOD and mobile security policies
- ✓ Add DEX tooling to optimize operations
- ✓ Map IT controls to regulatory frameworks (DORA, NIS2, GLBA, FFIEC)

Contact

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Deutschland

 + 43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA



baramundi software

baramundi software develops Unified Endpoint Management for the central administration of PCs, mobile devices and servers. It automates software distribution, simplifies patch management and creates transparency in the network. baramundi solutions contribute significantly to IT security and optimize IT resources.

www.baramundi.com