IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ISM/2025/4646625/
Vol. 2025 (29), Article ID 4646625

Designing a Low-Budget Secure Network for SMEs: Threat Landscape, Virtualization and Data Storage*

Mateusz KRAUZE and Mariusz ZAL

Poznan University of Technology, Chair of Communication and Computer Networks, Poznań, Poland,

Correspondence should be addressed to: Mariusz ZAL, mariusz.zal@put.poznan.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

Small and medium-sized enterprises (SMEs) remain highly exposed to advanced cyber threats despite their growing dependence on digital services. This study is motivated by the persistent resource gap between SMEs and large organisations, which prevents smaller entities from adopting resilient, security-by-design infrastructures. Although numerous guidelines and frameworks for SME cybersecurity exist, the literature lacks a unified, practical, and empirically grounded architectural blueprint that integrates low-cost virtualization, modern storage systems, and selective cloud services into a coherent, security-enhancing environment. To address this gap, the study conducts a comparative analysis of key infrastructure technologies relevant to SME cybersecurity. The methodology combines feature-based evaluation of widely used virtualization platforms (KVM, Proxmox VE, Hyper-V, VMware vSphere), assessment of data storage solutions (NAS, SAN, and Software-Defined Storage), and examination of selected IaaS/PaaS cloud services suitable for low-budget deployments. The analysis emphasises cost structure, security capabilities, manageability, and failure-resilience characteristics. The findings demonstrate that SMEs can significantly strengthen their cyber resilience by adopting an open-source-centric, hybrid architecture that leverages commodity hardware for on-premise virtualization and storage while offloading selected functions to cloud services. The proposed reference architecture provides improved redundancy, streamlined management, and enhanced protection against common threats such as ransomware, credential compromise, and service downtime. The study contributes a practical, implementable model that allows SMEs to transition from fragmented and vulnerable infrastructures toward robust, corporate-class environments that meaningfully support business continuity and cybersecurity.

Keywords: SME, cybersecurity, IT infrastructure, virtualization, data storage, cloud computing, low-budget corporate-class architecture

Introduction

Small and medium-sized enterprises (SMEs) are a critical part of the modern economy, yet they are increasingly exposed to the same advanced cyberattacks that target large corporations-without having comparable budgets, redundant systems, or specialised security teams. At the same time, market pressure forces them to digitalize, making core business processes dependent on IT infrastructures that are often fragile and difficult to manage. This imbalance between high exposure and limited defensive capacity creates a particularly challenging environment for cybersecurity in SMEs.

Despite their internal diversity, SMEs typically operate under strong cost pressure and limited investment capacity, and they often treat IT as a supporting utility rather than a strategic asset [1]. Many rely on basic tools such as e-mail, office suites and simple communication platforms, run mainly on Windows-based desktops and

Cite this Article as: Mateusz KRAUZE and Mariusz ZAL, Vol. 2025 (29) "Designing a Low-Budget Secure Network for SMEs: Threat Landscape, Virtualization and Data Storage " Communications of International Proceedings, Vol. 2025 (29), Article ID 4646625, https://doi.org/10.5171/2025.4646625

laptops, with NAS devices and Gigabit Ethernet forming the backbone of storage and networking. More advanced components-virtualization platforms, central monitoring, or structured backup and recovery-are less common or implemented in an ad hoc way [2]. IT and security are frequently handled by non-specialist staff, and budgets are focused on visible hardware rather than security systems, monitoring, or skills development, resulting in infrastructures that work in normal conditions but lack resilience, redundancy, and security-by-design features [3].

At the same time, SMEs face an increasingly hostile threat landscape. Industry reports show that typical initial access vectors include software vulnerabilities, compromised credentials and social engineering. Ransomware is the most disruptive attack type, often combined with data theft, while Trojans, spyware, viruses and worms further degrade performance and reliability [4,5,6]. A substantial share of incidents is linked to human error-misconfigurations, accidental disclosures and susceptibility to phishing-demonstrating that users are an integral part of the attack surface and that technical controls alone are insufficient [7, 8, 9].

These conditions highlight the need for practical, cost-conscious approaches that can raise SME cyber resilience without enterprise-level resources. One promising direction is the design of a low-budget, corporate-class network architecture based on widely available technologies but incorporating security, redundancy and manageability from the outset. The aim of this paper is to present such a concept, tailored to SME constraints. As a first step, it provides a systematic analysis of available tools and technologies-covering network and security devices (e.g. next-generation firewalls, NAS, virtualization and monitoring solutions) and supporting mechanisms for patch management, access control and incident detection. On this basis, the paper proposes and evaluates a reference architecture that helps SMEs move from vulnerable, ad hoc infrastructures towards resilient, well-structured network environments.

The Importance of Virtualization for SMEs

Virtualization is a key technology for ensuring flexibility, high availability, and efficiency of IT infrastructures, including those of small and medium-sized enterprises (SMEs) [10]. It enables multiple operating environments to run on a single physical machine, improving hardware utilization and simplifying management-without sacrificing performance and in some cases even enhancing it. This makes virtualization particularly attractive for SMEs, which usually operate with limited resources.

Instead of maintaining many physical servers, a single well-designed, secure, and efficient virtualization cluster can host most or all services, generating substantial cost savings. Server consolidation and reduced reliance on physical hardware lower expenditure on equipment, maintenance, power, and cooling, while also reducing space requirements. A properly configured host provides a stable platform for virtual machines, and the ability to flexibly create, remove, and adjust VM resources allows IT staff to respond quickly to changing business needs. Scaling server resources often requires only configuration changes, which minimizes or even eliminates service downtime.

Virtualization also supports high availability. Operating systems hosting services are stored as files rather than tied to specific physical disks, which greatly simplifies backups and even allows them to be performed while a virtual machine is running [11]. Recovery is likewise faster and more straightforward, improving business continuity in case of failures.

According to a 2023 report in the International Journal of Education and Management Engineering [10], virtualization in SMEs brings significant economic and operational benefits: hardware procurement costs can be reduced by 40–60%, while lower energy use and smaller space requirements cut building operating costs for server rooms by 30–50%. Virtualized systems reach availability levels above 99.5%, and the flexibility of managing virtual resources shortens IT response times by around 35%. These figures confirm that virtualization effectively optimizes infrastructure and strengthens the strategic efficiency of SME operations.

Review of Selected Virtualization Solutions Used in SMEs: Functionality, Licensing Models and Operational Costs

Virtualization is becoming an indispensable element of IT strategy, especially for companies seeking greater competitiveness. In practice, platform choice should be based on concrete, widely used solutions, whose functionality, availability, licensing model, and costs determine whether they fit SME requirements [10]. With a suitable platform, enterprises can optimize resource usage and gain flexibility in adapting to changing technological needs.

Kernel-based Virtual Machine (KVM) is an open-source full virtualization technology integrated into the Linux kernel, turning it into a hypervisor [11]. It uses QEMU to emulate hardware and supports full and paravirtualization. Key features include snapshots (quick rollback to a previous VM state) and live migration between physical hosts without downtime. Management can be handled via tools such as Libvirt or Virt-Manager, and KVM enables building high-availability clusters. Its major advantage is licensing under the GNU GPL, which allows free commercial use, at the cost of higher implementation complexity and the need for specialist knowledge.

Proxmox Virtual Environment (Proxmox VE) is also open-source but easier to deploy [12]. It combines full virtualization with Linux Containers (LXC), which provide isolated environments sharing the same kernel and consuming fewer resources than VMs. A web-based GUI and exposed API support both convenient daily administration and automation. Proxmox VE offers high-availability clusters, snapshots, live migration, and automated backups. The platform is free, with optional paid subscriptions for support and access to enterprise repositories, making it attractive for SMEs that may later scale up.

Microsoft Hyper-V is a paid but often reasonable alternative tightly integrated with the Windows ecosystem [13]. A limited version is built into Windows 10/11, while full functionality is available with Windows Server. Hyper-V supports snapshots, live migration, replication, virtual networking, high availability, and dynamic resource allocation. The cost is tied to Windows Server editions (Standard vs. Datacenter) and per-core licensing, plus Client Access Licences, which makes it suitable for SMEs already invested in Microsoft infrastructure.

VMware vSphere is a corporate-grade platform offering all the above capabilities and more, but with a higher total cost of ownership [14]. Its ESXi hypervisor runs directly on bare metal, managed centrally via vCenter Server. Advanced features such as vSphere Fault Tolerance eliminate downtime by maintaining real-time VM replicas across nodes. Licences are subscription-based and priced per core, which may be prohibitive for many SMEs, but vSphere remains a benchmark for reliability, manageability, and integration in professional virtualized environments.

The cloud is not a solution for every company; even if its other drawbacks are acceptable, for many organisations maintaining their own infrastructure will be more cost-effective. In each case, the cost calculation must be carried out individually, but as an example, a single virtual machine with 2 virtual CPU cores, 8 GB of RAM, 256 GiB of SSD storage and Windows Server costs 1,067.88 USD per year according to the official Azure pricing calculator.

From the perspective of the SME sector, each of the solutions presented may be reasonable depending on specific needs. Table 1 compares all technologies against the parameters most important for SMEs. Entities with a small budget and high requirements should choose Proxmox VE, whereas more modest needs can be fully covered by KVM. With a larger budget, the choice will typically be between Hyper-V and vSphere. By contrast, a company with staff distributed outside the main headquarters will benefit more quickly from cloud solutions, due to the fact that cloud services are accessible from any location with an Internet connection.

Table 1. Comparison of hypervisors

Technology	Type	Licensing	Snapshots	Cluster (High Availability)	Initial Costs	Ease of Management
KVM	Local	GNU GPL	Yes	Yes (with add-ons)	Low	Low
Proxmox VE	Local	GNU GPL	Yes	Yes	Low	High
Microsoft Hyper-V	Local	Built into Windows Server (paid)	Yes	Yes	Medium	Medium
VMware vSphere	Local	Subscription model	Yes	Yes	High	High
Microsoft Azure	Public cloud	Subscription model	Yes	Yes (distributed data centers, regions)	None (grow over time)	High

Data Storage Systems in Virtualized Environments in the SME Sector

Every hypervisor requires a well-designed data storage system; storing virtual machine files on the same physical disk as the host OS is highly inadvisable. This is especially true in clustered setups, where storage must be fast enough for all VMs and accessible from every node. On the market, common options include NAS appliances (hardware or virtual), block-based Storage Area Networks (SAN), and software-defined storage (SDS) [15], [16]. Scalability, stability and fault tolerance make storage choice no less important than the choice of virtualization technology itself.

Given limited resources, NAS is often the natural choice for SMEs. It offers a favourable price–performance ratio and low initial cost [17]. As an independent file server, a NAS can share data over LAN and WAN using protocols such as NFS and SMB/CIFS. Because it operates on files, integration with other systems is simpler than with SAN. Besides classic standalone systems, NAS gateways can present a file interface to applications while using a block-based SAN backend. Popular hardware platforms include QNAP arrays, which support snapshots, replication, deduplication, encryption, iSCSI targets and backup integration [18]. A comparable, largely open-source alternative is TrueNAS from iXsystems, which can turn almost any server into a fully fledged NAS with enterprise-class features, with payment limited to optional support [19].

SAN represents a different model, delivering higher performance and lower latency than NAS – key in environments requiring very high availability and scalability. Traditional SAN deployments rely on Fibre Channel (FC), separated from the LAN to guarantee quality of service [17]. Vendors such as IBM offer storage virtualisation, non-disruptive data migration, real-time replication and snapshots tightly integrated with virtualisation platforms [20]. However, such environments are expensive, and SME use cases rarely justify full SAN deployments. As a compromise, iSCSI over IP can provide block storage without FC, but even then costs may remain significant compared to NAS.

SDS is an evolution that reduces dependence on proprietary hardware. Here, software acts as the storage controller and can use local disks in multiple nodes to provide high availability and scalability [16]. This makes SDS suitable both for cost-sensitive SME deployments and for large data centres. TrueNAS is one such SDS-capable system, while Ceph is a prominent open-source, distributed solution supporting block, file and object storage [19], [21]. Ceph clusters replicate and distribute data across nodes without requiring FC, and are recognised as mature enough even for SME environments, largely thanks to long-term development by major IT vendors such as Red Hat.

Protecting organisational data is essential for maintaining operational capability, and a carefully selected storage technology is one of the simplest ways to achieve this. As summarised in Table 2, the characteristics of the main storage options indicate that SAN is usually not justified in the SME sector. Under typical financial and staffing constraints, NAS arrays are the most practical choice in simpler environments, while SDS solutions are better suited to more demanding SME deployments.

Table 2. Comparison of data storage technologies

Feature	NAS	SAN	SDS
Initial cost	Medium	High	Medium/Low
Performance	Medium	High	Variable
Scalability	Limited	Very good	Very good
Management	Simple	Requires expertise	Variable
Vendor dependence	High	High	Low

Conclusions

The analysis shows that small and medium-sized enterprises are increasingly exposed to advanced cyber threats while lacking enterprise-grade budgets, redundant infrastructure and dedicated security teams. At the same time, digitalization makes their IT – especially network, virtualization and storage layers – critical for both business continuity and cybersecurity. Ad hoc, minimally protected infrastructures are no longer sufficient in this context.

The review of technologies demonstrates that a low-budget, corporate-class environment is feasible using widely available components. Open-source platforms such as KVM and particularly Proxmox VE, combined with NAS or software-defined storage (e.g. TrueNAS, Ceph), provide a flexible and cost-effective basis for consolidating

services, improving availability and simplifying management. Commercial hypervisors (Hyper-V, VMware vSphere) and public cloud services (IaaS/PaaS) remain valuable options, but their total cost and operational characteristics require careful, case-by-case evaluation in SMEs.

For typical SMEs, the most realistic direction is a pragmatic, hybrid architecture that relies primarily on open-source or commodity on-premises solutions, complemented by next-generation firewalls, robust backup mechanisms and selective use of cloud services. Crucially, technical measures must be supported by basic security governance, systematic patch management and user awareness. With such deliberate design, SMEs can move from fragmented, vulnerable setups towards more resilient, well-structured infrastructures that better support operational continuity and cyber resilience.

Acknowledgement

This research was funded by the Polish Ministry of Science and Higher Education (No. 0313/SBAD/1311).

Bibliography

- European Commission, *Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty Text with EEA relevance*, 2014. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/651/oj, [Accessed: 20.11.2025]
- M. Urbanek, "Małe firmy w świecie wielkich danych," CRN Polska, Sep. 30, 2019. [Online]. Available: https://crn.pl/artykuly/male-firmy-w-swiecie-wielkich-danych/. [Accessed: 20.11.2025]
- Grand View Research. (2024). *Next-generation Firewall Market Size, Share & Trends Analysis Report, 2022–2030*. San Francisco, CA: Grand View Research. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/next-generation-firewall-market-report [Accessed: 20.11.2025]
- Sophos, *The State of Ransomware 2024*, Oxford, UK, 2024. [Online]. Available: https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/ [Accessed: 20.11.2025]
- Check Point, Ransomware Attack – What Is It and How Does It Work? (section: "Why Are Ransomware Attacks Emerging?"), 2025. [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ [Accessed: 20.11.2025]
- Elsevier, "Computer Worms – an overview," in ScienceDirect Topics: Computer Science, 2025. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/computer-worms. [Accessed: 20.11.2025]
- Verizon, 2024 Data Breach Investigations Report (DBIR), 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf [Accessed: 20.11.2025]
- A. A. Abubaker, D. Eleyan, A. Eleyan, T. Bejaoui, N. Katuk and M. Al-Khalidi, "Social Engineering in Social Network: A Systematic Literature Review," 2023 International Symposium on Networks, Computers and Communications (ISNCC), Doha, Qatar, 2023, pp. 1-7, doi: 10.1109/ISNCC58260.2023.10323826.
- C. Lekati, "Psychological Exploitation of Social Engineering Attacks," Cyber Risk GmbH, [Online]. Available: https://www.cyber-risk-gmbh.com/Psychological_Exploitation_of_Social_Engineering_Attacks.html. [Accessed: 20.11.2025]
- S. Kushwaha, A. K. Yadav i H. N. Verma, „Desktop Virtualization: Benefits, Challenges, and Future Trends," I. J. Education and Management Engineering, tom 6, pp. 14-24, 2023.
- The KVM Project, „KVM - Kernel-based Virtual Machine," Linux Kernel Virtualization, [Online]. Available: https://linux-kvm.org/. [Accessed: 20.11.2025]
- Proxmox Server Solutions GmbH, „Proxmox Virtual Environment," Proxmox Server Solutions GmbH, [Online]. Available: https://www.proxmox.com/proxmox-ve. [Accessed: 20.11.2025]

- Microsoft Corporation, „Microsoft Learn," Microsoft Corporation, [Online]. Available: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-vtechnology-overview. [Accessed: 20.11.2025]
- VMware, Inc., „ VMware Products, " VMware, Inc., [Online]. Available: https://www.vmware.com/products/cloud-infrastructure/vsphere. [Accessed: 20.11.2025]
- R. Kumar, A. Nagaraj, B. Paul i S. P. Dixit, „Network-Attached Storage: Data Storage Applications," Turkish Journal of Computer and Mathematics Education, tom 12, nr 12, pp. 2385-2396, 2021.
- M. Carlson, A. Yoder, L. Schoeb, D. Deel, C. Pratt, C. Lionetti i D. Voigt, „Software Defined Storage, " Storage Networking Industry Association, 2015.
- M. Blunden, M. Berx-Debeys i D. Sim, Storage Networking Virtualization: What's it all about?, San Jose, California, USA: 1st ed., International Technical Support Organization, IBM Corporation, 2000.
- QNAP Systems, „QNAP," QNAP Systems, Inc., [Online]. Available:https://www.qnap.com/pl-pl. [Accessed: 20.11.2025]
- iXsystems, Inc., „TrueNAS - Open Enterprise Storage," iXsystems, Inc., [Online]. Available: https://www.truenas.com/. [Accessed: 20.11.2025]
- IBM Corporation, „IBM - Storage Area Network," IBM Corporation, [Online]. Available: https://www.ibm.com/storage-area-network. [Accessed: 20.11.2025]
- Ceph Foundation, „Ceph," Ceph Foundation, [Online]. Available: https://ceph.io/en/. [Accessed: 20.11.2025]