

# Single Stack Network Security, Cybersecurity, Email Security and SIEM for Affordable, Easy to Implement Enterprise Protection for SMBs

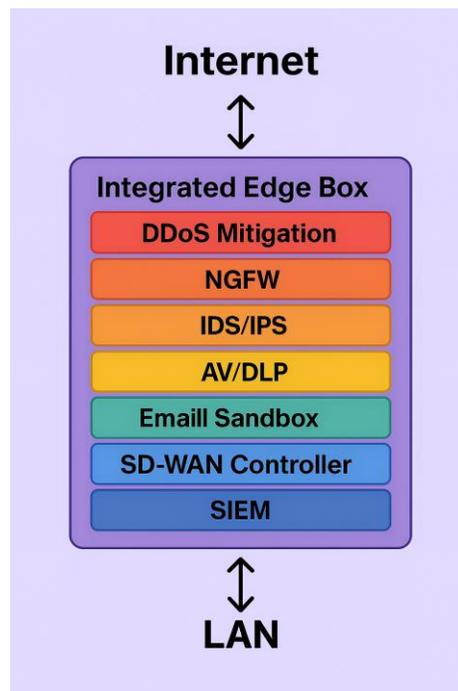
*Cutting Edge Innovative Integrated security Solution for Low Cost Enterprise Protection.*

Small and mid-sized businesses (SMBs) are confronted with a bewildering array of cloud service providers, each requiring specialized cybersecurity knowledge. To achieve full protection, many organizations end up purchasing multiple services from different vendors — a fragmented approach that drives up both complexity and cost.

FatPipe has recognized this challenge and developed a **single-stack solution** that integrates SD-WAN, Network Edge Security, Cybersecurity, and SIEM, with **locally stored SIEM data** to meet data security and GDPR requirements. All information is visible through a **single-pane-of-glass interface**, simplifying management for resource-constrained IT teams.

**FatPipe Total Security 360** is a comprehensive perimeter security appliance that combines NGFW, IDS/IPS, antivirus, DLP, proxy inspection, SD-WAN control, and DDoS protection into one platform. By embedding these capabilities at the network edge, SMBs gain not only performance but also resilience. On-premises deployment eliminates expensive cloud hosting fees, reduces bandwidth costs, avoids cloud egress charges, and cuts storage expenses. It also mitigates the latency, jitter, and VPN authentication delays common with cloud-based inspection — issues that are especially problematic over Wi-Fi, LTE, or satellite links where instability can cause VPN sessions to drop.

In addition, **FatPipe SIEM** securely stores the compliance data required by customers in regulated industries, supporting frameworks such as **HIPAA, NIST, PCI, and MITRE ATT&CK**.



The economics of a single stack solution are equally compelling. A single-stack solution simplifies vendor management, eliminates multiple license fees, reduces hardware sprawl, simplifies and combines network and cybersecurity monitoring, lowering integration costs. Compared to fragmented add-ons, lifecycle costs are consistently lower, while resilience and uptime are consistently higher. For SMBs, the ROI is clear: better protection at a lower, predictable cost.

Aspect	On-Premises Single-Stack Solution	Cloud-Hosted / Add-Ons
Licensing Fees	✔ One integrated license; predictable	✘ Multiple subscriptions, per-user or per-GB fees
Hosting Costs	✔ No recurring cloud hosting costs	✘ Recurring hosting charges from provider
Bandwidth Consumption	✔ Local inspection; no forced backhaul	✘ Higher bandwidth required to route traffic to cloud
Data Egress Fees	✔ No egress costs (local storage/logs)	✘ Charged for downloading / moving data out of cloud
Storage Costs	✔ Logs/quarantine stored locally; predictable	✘ Ongoing cloud storage fees that scale up
Integration	✔ Built-in, policy-consistent	✘ Manual integration needed across vendors
Vendor Management	✔ Streamlined, one vendor	✘ Multiple vendors, more complexity
Administration	✔ Simplified with single-pane view	✘ Time-consuming, fragmented dashboards
Compatibility Issues	✔ Minimized	✘ Higher risk of interoperability problems
Network Latency & Jitter	✔ Local inspection; stable VPNs, fast transfers	✘ Added latency from cloud hops; VPN logins and large files slower
Impact of Wi-Fi/LTE/Satellite	✔ Minimal; local edge processing absorbs instability	✘ Performance degradation worsens over unstable links
Lifecycle Costs	✔ Lower, predictable	✘ Higher overall, often hidden costs
Operational Efficiency	✔ Improved; no reliance on cloud uptime	✘ Reduced; tied to vendor SLA and internet stability

**Fatpipe’s Hybrid Cloud Solution:** FatPipe offers integrated on-premise cybersecurity at an affordable price while ensuring the highest levels of network security, cybersecurity and SIEM. For those customers who have geographically distributed employees, FatPipe offers cloud-based cybersecurity and SIEM solutions as an alternative option. Customers can combine their on-premise solution with the cloud-based solution to optimize costs and support their geographically distributed workforce.



**Email Security:** Email is another common attack vector for cybercriminals, and with threats increasingly embedded in attachments. **Email security combined with attachment sandboxing** is no longer optional. An attachment sandbox allows suspicious files—such as PDFs, Word documents, or executables—to be opened and analyzed safely within a controlled environment before they ever reach the end user. This prevents malware, ransomware, and phishing payloads from entering the network. A major advantage of running these capabilities **on-prem** is that emails and attachments do not need to leave the organization for inspection, avoiding both privacy risks and compliance concerns. In today’s world, where governments and external providers may scan or retain email data as it transits through cloud systems, keeping inspection local ensures confidentiality, reduces exposure, and guarantees that sensitive client or business information always remains under the direct control of the organization itself. This approach strengthens both security and trust, while eliminating the hidden costs and risks of relying on third-party inspection.

In addition to cybersecurity, all elements of network security and email security are also built in the FatPipe system, resulting in a single orchestrated, high security wide area network for an organization.

**Fatpipe SIEM:** Fatpipe SIEM provides applications monitoring, PCI, HIPAA, NIST and DLP alerts, as well as NIST compliance data which is stored locally. Remote Device login, Desktop level user stats, as well as GDPR and TSC compliance. Customers can retrieve this data for compliance purposes, without incurring storage or data download costs.

Network Security	Cybersecurity	SIEM
DDoS Attack Prevention	Protocol Monitoring	Applications Monitoring
NexGen Firewall	Firewall IDS/IPS	PCI Alerts
Geo-Fencing	Data Loss Prevention	HIPAA Compliance
Transport Layer Security	OT Detection/ Vulnerability Correlation	Top Hosts and Top Users and DLP
Device Authentication	Malicious URL, URL and Video Filtering	GDPR Compliance
SSL and VPN	Botnet / Commands	Internet Access Control
Proactive Network Monitoring	Man in the Middle	NIST Compliance
Web Filtering	Anti-Spam Sandbox	Remote/Device Login
Multi-Path Security	DNS based Threats	Proactive Network Monitoring
Remote Login User Stats	Virtual Patching	Desktop Level user stats
Selective Encryption for Internet Connection	Deep Packet Inspection	TSC Compliance

*Integrated Multi-Function FatPipe Security*



## Key Fatpipe 360 Security features Include:

- **Attachment Sandboxing:** Suspicious attachments are safely opened in a controlled environment, blocking ransomware, zero-day malware, and phishing payloads before reaching users.
- **Integrated AV/DLP:** Advanced antivirus scanning and data loss prevention ensure email traffic is free of malicious code and that sensitive information is never leaked.
- **On-Premises Inspection:** Emails and attachments never leave the organization for filtering, preserving **privacy and compliance** while reducing exposure to third-party monitoring or government scanning.
- **Granular Policy Control:** Customizable rules for MIME types, domains, and content ensure precise enforcement and flexibility.
- **Unified Security Stack:** Seamlessly integrated with FatPipe's NGFW, IDS/IPS, Geo-fencing, DDoS mitigation, SD-WAN controller, and SIEM for consistent policy enforcement across all traffic.
- **Reduced Latency & Costs:** Local inspection reduces latency and jitter issues, avoids the bandwidth overhead, cloud hosting fees, and egress charges common with cloud-based solutions.

## ROI & Cost Savings with On-Premises Integrated Security

The diagram represents the **ROI (Return on Investment)** of using an **integrated on-premises security device**, showing the financial and operational advantages when compared to fragmented or cloud-hosted approaches.

ROI is supported by six benefits:

1. **Improved Compliance** – Keeping inspection and data storage in-house reduces exposure to third-party or government scanning, simplifying adherence to HIPAA, GDPR, PCI, and other regulations.
2. **Stronger Security Posture** – Multiple defenses (sandboxing, IDS/IPS, DLP, NGFW) work together at the edge to stop threats before they reach the LAN.
3. **Operational Efficiency** – Unified policy enforcement and a single-pane-of-glass management system reduce administrative effort and speed up response times.
4. **Predictable Cost Savings** – Eliminates recurring cloud hosting, bandwidth backhaul, and hidden egress/storage charges, keeping costs contained and predictable.
5. **Reduced Complexity** – Replacing multiple vendors and subscriptions with one coherent platform, minimizes integration headaches.
6. **Faster Response** – Local inspection and enforcement mean issues are resolved immediately within the customer's environment, without delays from cloud queues or third-party SLAs.





*ROI for a single integrated SD-WAN, Network Security, Cybersecurity and SIEM*

**Summary:**

An integrated on-premises security device combined with a Cloud solution for geographically distributed employees delivers **higher ROI by cutting costs that cloud vendors inevitably pass on, with their profit margins to customers, while also enabling faster, localized response times.** It avoids hosting, storage, and bandwidth markups, eliminates the line jitter and latency, latency of shared cloud services, slow troubleshooting response, and strengthens compliance and security. The result is a streamlined, high-performance network and cybersecurity and email security solution that enhances privacy, compliance, and trust, while delivering maximum protection at the edge without sacrificing speed or control.

**Comments:**

**Law Firm IT Director:**

*"With our old cloud setup, remote attorneys constantly complained about VPN sessions dropping during hearings and client calls. Since moving to FatPipe's integrated solution, latency and jitter are practically gone — our VPNs stay stable, and the team can finally focus on clients instead of troubleshooting connections."*

**2. Healthcare Clinic CIO:**

*"We were juggling three different cloud security providers and still couldn't meet HIPAA audit requirements without huge costs. FatPipe gave us SD-WAN, cybersecurity, and SIEM in one stack, with compliance data stored locally. Not only did we cut costs, but we eliminated the performance problems that came from routing everything through the cloud."*

**3. Manufacturing Operations Manager:**

*"Cloud-based inspection was killing us — large CAD files took forever to transfer, and jitter made remote monitoring unreliable. The FatPipe appliance fixed it overnight. With edge-level protection and SIEM built in, we get faster performance, stronger security, and clear visibility on one screen."*

