FatPipe Total Security 360

FatPipe Networks – Leading the Way with Total Security

Network security threats are becoming increasingly sophisticated and pervasive. Businesses are facing challenges from malware, ransomware, and data breaches that can compromise sensitive information and disrupt operations. There is a need to gain robust, end-to-end protection that secures your network while enhancing performance and reliability.

FatPipe understands that at its core, security involves delivering comprehensive, 360-degree security, protecting your network from every angle. FatPipe's advanced security measures are the defensive wall that defends against malicious cyber activities like malware, ransomware, DDoS attacks, and data breaches.

Here are the four distinguishing elements of FatPipe Total Security 360:

- **Network monitoring** and visibility into traffic flows and system integrity
- **WAN Transmission Security** to ensure that data is not compromised during transmission.
- **Advanced Firewall and Network Security** to secure your network and operations
- **Regulatory compliance and monitoring for HIPAA, NIST, GDPR, TSC, MITRE ATT&CK** and others.

FatPipe Total Security 360 elevate your organization's network to a new level of resilience, visibility, and security. DDoS protection isn't an added feature - it's a standard. Every service on the unit is automatically safeguarded against DDoS attacks right out of the box. No setup, no activation—just seamless, built-in defense that ensures your operations stay uninterrupted and secure at all times.

FatPipe Total Security ensures your network operates securely and efficiently, even under evolving cyber threats. FatPipe integrates MITRE ATT&CK with real-time threat intelligence and advanced analytics. This enables automatic correlation of detected activities with known adversary tactics, techniques, and procedures (TTPs), which is a major benefit for organizations in understanding the harmful approach of the adversaries. Whether it is MPSec providing an extra layer of security to keep your information safe or the advanced NextGen firewall features or other network, security, and compliance monitoring features, FatPipe is a clear choice for organizations that don't compromise on innovative SD-WAN and secure WAN Edge while optimizing network performance and meeting compliance standards.

FatPipe Data Security – Secure Your Organization's Information Assets

FatPipe MPSec – A True FatPipe Groundbreaking Security Feature

FatPipe solutions are equipped with a patented feature that ensures an extra layer of security called Multi-Path Security (MPSec™). MPSec can increase the security of data transmission by up to a factor of n (n being the number of lines). MPSec transmits data over a combination of secure lines to transmit encrypted data and monitors all connection paths, providing redundancy, security and load balancing for higher throughput. MPsec utilizes multiple active links scrambling the traffic paths preventing information interception and reconstruction.

FatPipe's SSL and VPN – Solutions for Secure Networking

FatPipe SSL and VPN enables you to securely access your network remotely. You can use either IPSec VPN client or SSL VPN client software with FatPipe VPN. FatPipe optimizes these technologies by combining them with intelligent path selection, dynamic failover, and advanced encryption, providing seamless connectivity and robust protection against potential threats.

Encryption: FatPipe appliances use standard encryption with IPSec and GRE encapsulation. Therefore, FatPipe appliances are compatible with other security appliances and can establish VPN/GRE tunnels with third-party security appliances. FatPipe security module is FIPS-certified.

Selective Encryption: When MPLS lines are combined with lower cost Internet lines for redundancy, data flowing over the internet lines can be selectively encrypted using Fatpipe's patented Selective Encryption, while data flowing over the secure MPLS lines are unencrypted. Customers save about 40% on bandwidth by avoiding encrypting the MPLS lines, and cost.

FatPipe's Transport Layer Security (TLS) technology to facilitates secure data exchanges between the LDAP server and FatPipe, safeguarding sensitive details such as usernames, passwords, and privileges. Organizations can also secure cloud applications with traffic inspection and ZTNA principles.

Device Authentication: Integral to Secure Device Access

FatPipe's device authentication follows industry standards and facilitates secure authentication and key exchange. Safeguards are also in place when a device is moved from one location to another.

FatPipe Geofencing – Security Across All Locations

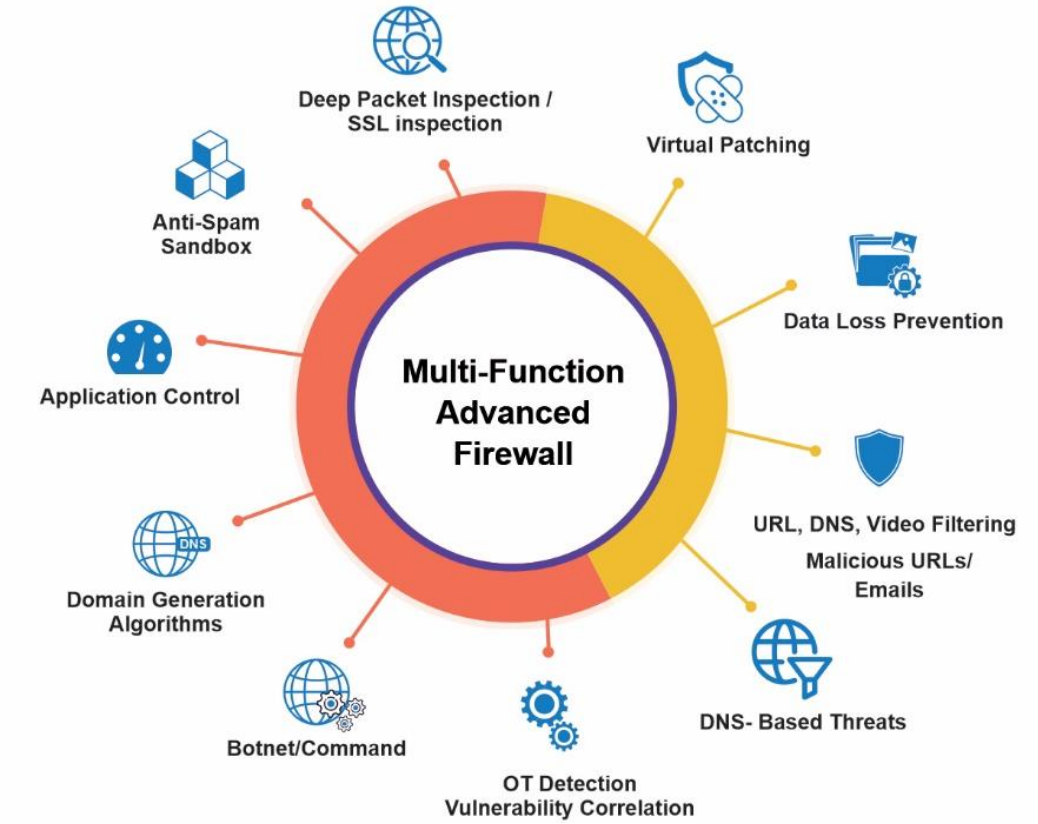
FatPipe's geofencing efficiently restricts network access based on geographic locations and IP

FatPipe Cloud Security

FatPipe provides many Cloud Security features including Cloud Firewall, Cloud Web Filtering, Cloud IDS/IPS

Man in the Middle to inspect encrypted data packets to ensure that only authorized data is sent out.

FatPipe Advanced Firewall



Firewall: The firewall acts as the first line of defense with built-in IPS functionality. The context-aware firewall makes smart decisions about which packets to allow and which to block. By monitoring and controlling traffic between different segments of a network, the firewall helps prevent unauthorized lateral movement by detecting and blocking suspicious activities from move laterally across the network.

IDS/IPS: FatPipe IDS/IPS monitors network traffic and alerts administrators when potentially hostile traffic is detected. It identifies potential security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). IDS/IPS can respond to malicious traffic by blocking the user or source IP address from accessing the network.

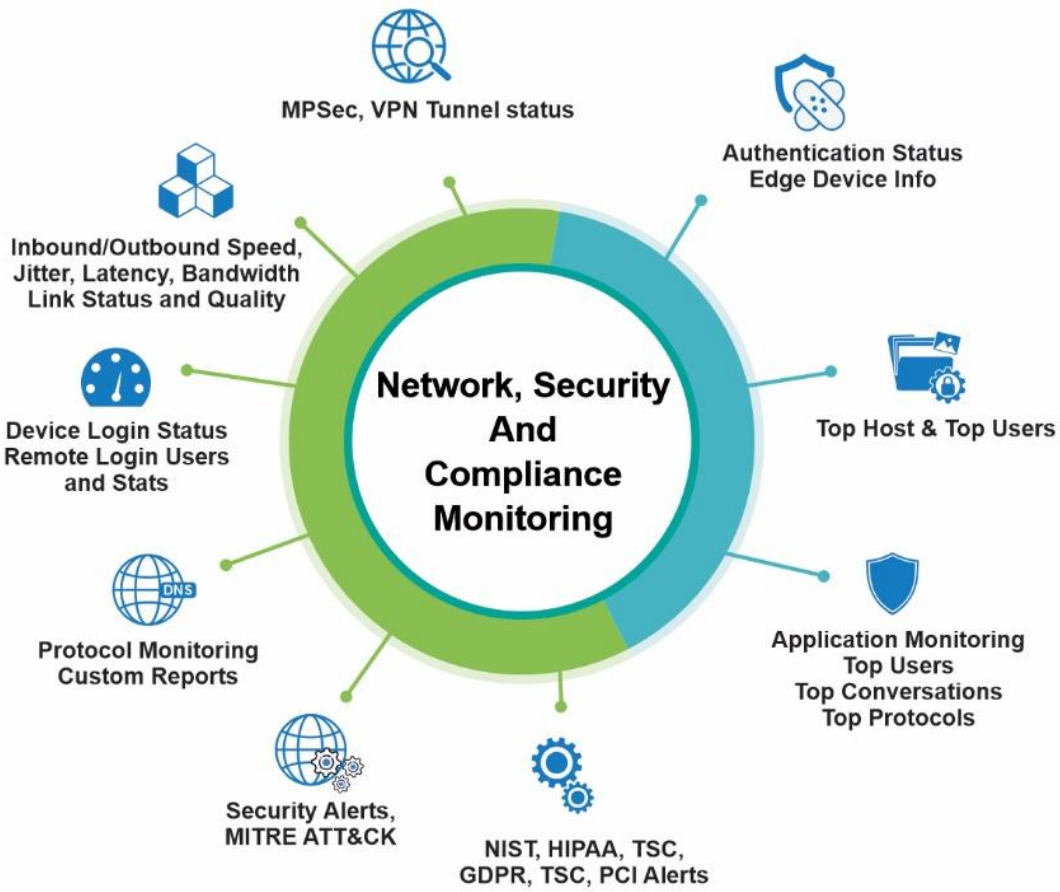
DDoS Blocking: FatPipe automatically safeguards against DDoS attacks and moves traffic on to a second line (if available). The DDoS blocker provides an extra layer of security. With its fortified protection, FatPipe ensures uninterrupted performance by safeguarding critical resources against even the most sophisticated DDoS threats.

Application Control: FatPipe provides network managers with advanced visibility into application usage and provides control over application and session flows. Customers can define how applications operate within a multipath network, ensuring they traverse only the paths that meet their specific requirements. This ensures optimal application performance, robust security, and an exceptional user experience.

- **Domain Generating Algorithms (DGA) Detection**: Detect and block DGA-based malware with FatPipe's intelligent traffic analysis. Identify suspicious patterns, effectively preventing malware from establishing connections to dynamically generated domains.
- **Botnet Protection**: Defends against botnet infiltration using deep packet inspection and rule-based threat detection. FatPipe provides signature-based analysis with behavior monitoring to block incoming threats.
- **OT Security:** FatPipe provides Deep Packet Inspection (DPI) to analyze network traffic in real time, identifying threats and vulnerabilities specific to industrial control systems (ICS or SCADA). FatPipe can swiftly detect and prevent unauthorized access or disruptions in OT protocols.
- **Malicious IP and Domains**: FatPipe integrates real-time threat intelligence to automatically block known malicious IPs and domains, ensuring continuous protection against emerging threats.
- **DNS Filtering:** FatPipe enhances DNS security by filtering traffic based on real-time reputation lists, blocking access to known malicious domains. This proactive approach leverages threat intelligence to prevent users from reaching harmful websites and reduces the risk of phishing or malware infections.
- **Web Filter**: FatPipe provides administrators the ability to restrict and log web access by various users and groups of users in an organization. This feature enforces Internet usage policy by blocking access to websites and Internet applications, and it easily and eliminates spyware from reaching the network.
- **Video Filter**: This technology ensures secure browsing by blocking inappropriate or malicious video content, safeguarding users and maintaining a trusted online experience.

- **Malicious URL Protection:** FatPipe uses gateway mode to filter and block harmful web traffic before it reaches the network. With real-time threat intelligence integration, FatPipe continuously updates its database of malicious URLs, ensuring that known threats are automatically blocked.
- **Virtual Patching:** FatPipe performs deep packet inspection to detect vulnerabilities in real-time and apply immediate security measures without the need for system downtime or software updates. By continuously monitoring network traffic and dynamically applying virtual patches, FatPipe ensures vulnerabilities are addressed promptly, minimizing the risk of successful attacks.
- **Deep Packet SSL Inspection:** FatPipe leverages deep packet inspection to enhance network security by performing signature-based threat detection, comprehensive network protocol and flow record logging, file identification and extraction, as well as full packet capture of network traffic.
- **Anti-Virus and Anti-Spam**: FatPipe appliance comes with an antivirus engine designed for detecting Trojans, viruses, malware and other malicious threats. It has an anti-spam engine that uses a wide variety of local and network tests to identify spam signatures.

Advanced Network, Security and Compliance Monitoring



FatPipe EnterpriseView delivers the following:

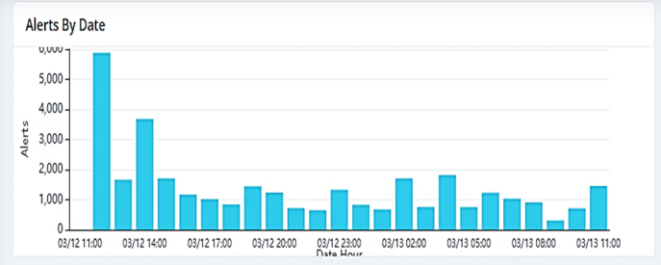
1. **Network Monitoring**: Real-time visibility and actionable insights into network performance, security, and user experience. Our monitoring goes beyond mere surveillance—it involves the meticulous collection and analysis of data to pinpoint any irregularities or unauthorized activities within your network.
2. **Security Monitoring**: Encompasses gathering information from your network, including security controls, servers/endpoints, and user applications. This comprehensive visibility allows us to establish triggers that promptly alert your business to any anomalies, ensuring proactive threat mitigation.
3. **EnterpriseView** also supports Compliance statistics through dedicated alert charts for NIST, HIPAA, GDPR, PCI/DSS, and TSC. Top MITRE Tactics are also monitored.

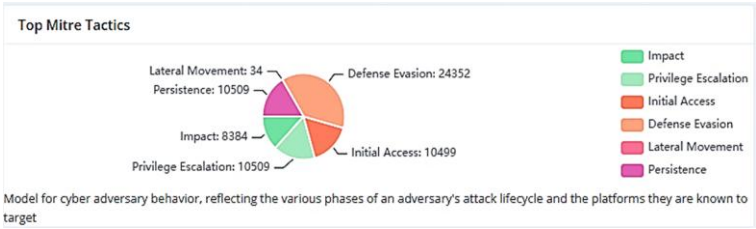
EV3 - FatPipe WAN Edge Monitoring

FatPipe's EV3 WAN Edge Monitoring enhances security by providing real-time visibility into network traffic and performance thus enabling early detection of anomalies, suspicious activity, or unauthorized access attempts. Key features include protocol monitoring, customizable reports, and insights into top hosts and users. Real-time metrics such as inbound/outbound speeds, jitter, latency, and bandwidth link status ensure visibility into network quality. FatPipe also tracks device login activity, remote user statistics, authentication status, and detailed edge device information.

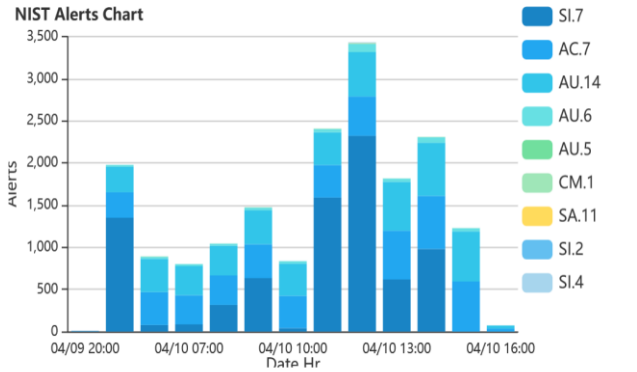
Compliance Monitoring

Compliance monitoring simplifies the compliance process and strengthens the overall security posture of organizations, providing peace of mind and safeguarding their critical data and operations. By continuously monitoring the system, organizations can detect and address potential incidents at their nascent stages, significantly enhancing their ability to respond effectively.

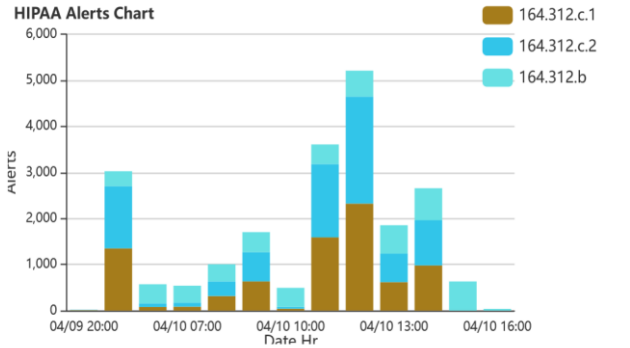




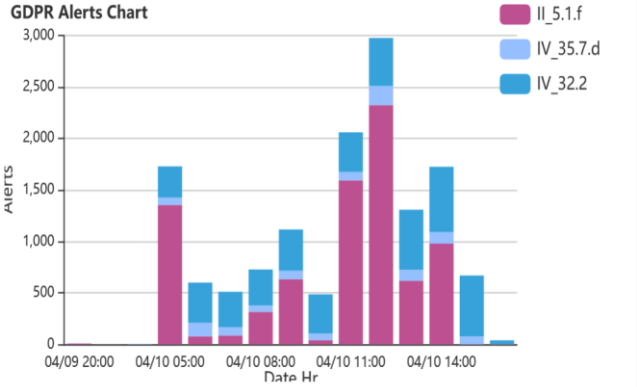
Model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target



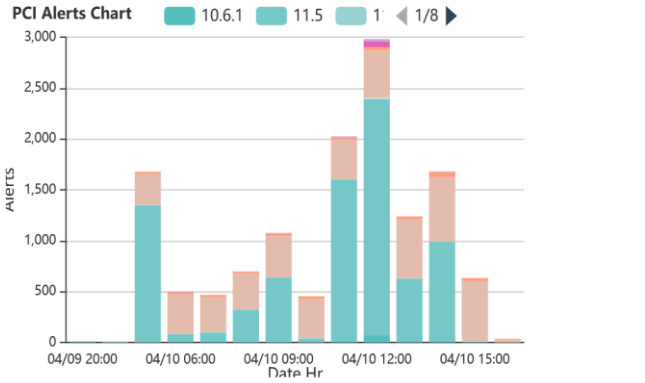
National Institute of Standards and Technology Special Publications 800-53 sets guidelines for federal information systems.



Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information



General Data Protection Regulation - National Institute of Standards and Technology Special Publications 800-53 sets guidelines for federal information systems.



Global security standard for entities that process, store or transmit payment cardholder data.