Bringing enterprise security to the branch

Potential benefits

- Zero trust network security across branch locations with highly secure, context-based access for all users and devices
- Centralized visibility across locations, users, and devices
- Real-time prevention of threats and zero-day attacks with embedded ML and native cloud-delivered security services
- Branch network segmentation to isolate sensitive parts of the network from each other and minimize vulnerability
- Simplified deployment, security policy design, 24/7 monitoring, and maintenance provided by AT&T Managed Services

The challenges of a highly distributed enterprise

Distributed enterprises are extending digital transformation initiatives to their retail or branch locations in order to drive agility and innovation. However, the benefits realized may come with increased cybersecurity risk.

Branches, in particular, tend to be attractive targets for cyberattacks because they frequently handle sensitive consumer and financial data, yet they often lack localized security specialists. In order to defend the business against today's modern threats, it is critical that the same priority is placed on protecting branch locations, corporate headquarters, or data centers.

Closing the branch security gap

With machine learning (ML)-powered, next-generation firewall (NGFW) capabilities built in, AT&T Premises-Based Firewall with Palo Alto Networks overcomes the complexities inherent to branch security. With this solution, administrators gain visibility and context into all users and devices across locations, including Internet of Things (IoT) devices, as well as the ability to apply unified security policies to protect against known and unknown threats.

The operating system natively classifies all traffic, including applications, content, and threats, and ties it to the user, regardless of location or device type. The applications, users, and devices then serve as the basis for security policies, which helps improve security posture and reduces response times.

Block data breaches at the branch with enterprise-grade security

Similar to corporate headquarters and data centers, branch locations require robust network security with support for cloud-delivered security services in order to defend against advanced threats.

AT&T Premises-Based Firewall with Palo Alto Networks delivers on all counts, with embedded inline ML and decryption capabilities to protect against known and unknown threats. All network security functions are consolidated into a single device, eliminating the need for separate intrusion-prevention system (IPS) or URL-filtering services, while single pass architecture helps maintain performance, even as additional services are activated.

Segment the network to protect data, applications, and resources

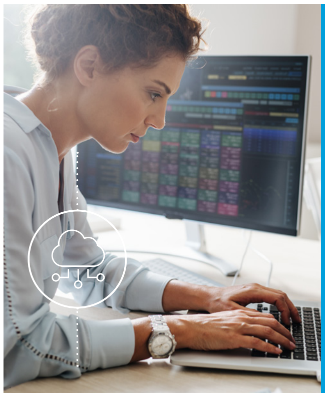
Securing modern networks requires that branches segment local traffic and isolate parts of the network from each other. Segmentation is fundamental in order to prevent a threat from spreading laterally throughout the network.

Minimizing threats to areas of the network where sensitive data, applications, or resources exist is an enterprise priority. AT&T Premises-Based Firewall with Palo Alto Networks include up to eight 10/100/1000 RJ-45 ports, enabling local traffic segmentation at the branch and isolating critical parts of the network from breaches that may occur elsewhere.

AT&T Premises-Based Firewall with Palo Alto Networks: Cloud-delivered security services

Today's sophisticated cyberattacks are capable of spawning up to thousands of variants in minutes using multiple threat vectors and advanced techniques to deliver malicious payloads. Natively integrated cloud-delivered security services coordinate intelligence and protect against threats spanning virtually every vector:

- **Threat prevention:** Single-pass prevention of known threats across all traffic
- **Advanced URL filtering:** Best-in-class web and phishing protection
- **Sandboxing:** Automatic detection and prevention of unknown malware
- **DNS security:** Prevents attacks within DNS traffic and blocks known malicious sites
- **SaaS security:** Provides visibility and security for new SaaS applications to protect sensitive data and defend against zero-day threats



Managed services from AT&T

The lack of localized network or security expertise is a significant contributor to branch network risk. Often small, space-constrained, and customer-facing, branches struggle to find discrete solutions to suit their unique hardware limitations. AT&T Premises-Based Firewall with Palo Alto Networks helps branches overcome the burden of procurement, provides simplified deployment, security policy design, 24/7 monitoring and management in one easy-to-buy service with AT&T Managed Services.