Your Retail Branches Are Under Siege

Machine Learning-Powered NGFWs Enable Zero Trust Security

Introduction

Retail branches are experiencing waves of cyberattacks unlike anything ever seen before. The attackers are determined, smart, innovative, and organized—in fact, most successful attacks are initiated by criminal enterprises, not basement hackers. They exploit weak points such as unpatched servers and endpoint devices to enter the network and steal information or launch ransomware attacks that can cripple the business. Today's interconnected supply chains mean that your network security is only as good as the security of your vendors and contractors—hardly reassuring to CIOs and CISOs charged with avoiding data breaches. In an ominous trend, this new breed of hackers is taking advantage of emerging technologies to defeat even the strongest of legacy security systems.

The security systems of the past are simply not up to the task of protecting the retail branch. Retailers need reliable, consistent security across their entire network and user base. This white paper explains the key challenges of branch security in this highly virulent environment and shows how organizations can meet those challenges.

Point-of-Sale Vulnerabilities

The most vulnerable part of any retail information technology (IT) system is the point-of-sale (POS) system simply because of the large number of users who interact with the business this way. One area of concern is the POS operating system (OS), typically a version of Windows®. Often the OS is an older version—sometimes even a discontinued version—that lacks the latest OS patches, resulting in known vulnerabilities that attackers can exploit to gain entry. Once inside, they look for and steal unencrypted payment card numbers and credentials for PayPal and personal bank accounts.

It gets worse. Upon gaining access to the device, the attacker can control the full functionality of the device, so they can cause mischief such as changing prices or remotely starting and stopping other POS terminals. In addition, these terminals are connected to the corporate network and thus can potentially lead to data breaches of millions of records—a financial and public relations catastrophe for the company.

Cybercrime Pays

The payday from breaching POS systems can be substantial. The typical selling price for a credit card or debit card number on the dark web—the place where hackers often fence stolen information—is US$17.36, while the credentials for a PayPal or bank account can fetch up to US$197. Depending on sales volume, a typical POS terminal may contain hundreds or even thousands of card numbers in unencrypted form, so the payoff from breaking into a single terminal can be in the tens of thousands of dollars.

Technology as a Weapon

Digital technologies such as cloud computing and data analytics are transforming the retail branch rapidly—and the pace is picking up. Bank branches are adopting self-service features such as in-branch kiosks and virtual agents. Healthcare organizations are partnering with pharmacy chains and even supermarkets to bring care delivery closer to their customers. Retail companies deliver more personalized experiences to shoppers by analyzing previous interactions and using social media to engage the customer in real time.

Unfortunately, those same technologies are being used as weapons to penetrate branch defenses and do real damage to your business. Hackers now deploy AI-based scanning programs to quickly locate the weak points in the network that represent their best chance of success. The high bandwidth and speed of 5G have enormous benefits for consumers and businesses, but cyberattackers see the opportunity to flood corporate websites with distributed denial of service (DDoS) attacks. Many companies are embracing the Internet of Things (IoT) as a way to accelerate and differentiate their business, while hackers find new ways to target a greatly expanded and less secure attack surface.

The Hairpinning Problem

Another factor in branch security is the network architecture itself. The traditional architecture for distributed enterprises connects each branch to the main data center using a wide-area network (WAN). Virtually all the IT resources that the branch needs—software applications, data, internet access, and more—are centralized.

In the cloud era, the modern retail branch is much more autonomous. Workers in the branch use the internet, not the corporate WAN, to access key applications such as customer relationship management (CRM) and enterprise resource planning (ERP) offered by software-as-a-service (SaaS) providers. In addition, individual branches have more communication with other branches as well as third parties in the supply chain.

For the most part, network architectures have not caught up with this new reality. The legacy model requires all traffic to go through the data center regardless of destination, which consumes bandwidth and introduces latency that can disrupt the user experience. IT professionals call this the hairpinning problem, because the network traffic essentially doubles back on itself, just like a hairpin (figure 1).

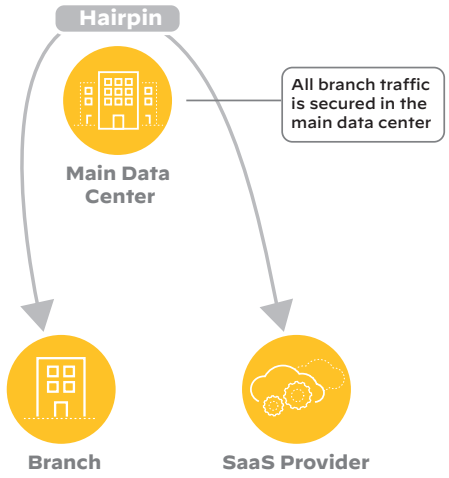

Figure 1: Traditional branch networking architecture

Many organizations solve this problem by implementing a software-defined wide area network (SD-WAN) to connect the branch directly to cloud-based resources such as SaaS providers and other branches (see figure 2). As is often the case, this approach solves one problem but creates another. In the hairpin model, all the branch traffic flows through a single location where a centralized security system can inspect the traffic and keep the branch safe from threats coming through the internet. In the direct-connect configuration, a significant amount of traffic moves directly between the cloud and the branch, bypassing security in the main data center. For this and other reasons, the modern branch needs its own security system tailored to the requirements of the branch itself, not the main data center.

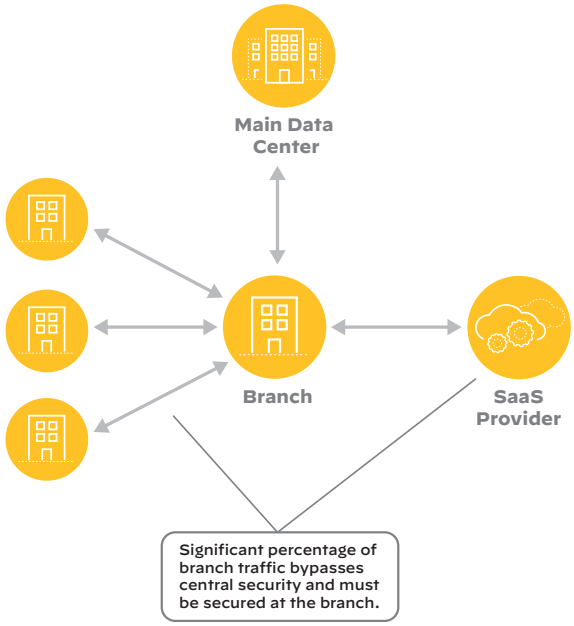

Figure 2: Modern branch networking architecture

The New Perimeter

Let's say you solve the problem of POS security to the extent that threats from the outside are no longer a concern. Mission accomplished? Hardly. Unlike the days when there was a distinction boundary between your company and the outside world—in other words, a security perimeter—today's cloud-based architectures are much more complex. The front door may be locked by a perimeter firewall, but hackers can still attack through back doors provided by contractors, vendors, and employees inside the perimeter (figure 3). IoT devices provide another tantalizing target because they often have little or no local security and can be easily breached.

The security challenges created by hyperconnectivity have prompted some analysts to proclaim that "the perimeter is dead." They no longer distinguish between threats from the outside versus threats from the inside—threats can now come from anywhere. Trust is obsolete—nothing and no one can be assumed to be safe.

In fact, the perimeter isn't dead—it's just too big and located in the wrong place, as the next section will show.

The Smarter NGFW

As cyberattacks get more and more sophisticated, they also get faster. For example, ransomware begins to encrypt information just a few seconds after penetrating the network defenses. Clearly, humans cannot react quickly enough to take the necessary steps to thwart cyberattacks. The process needs to be automated.

However, there's another problem. Today's threats are not only fast to act but they're also quick to morph into new threats. Again, humans cannot possibly keep up—the firewall has to be smart enough to automatically block threats. Traditional firewalls use signatures of known threats to detect attacks, but this is a reactive process that relies on an outside authority to identify and distribute the signatures. That takes time, and time is the enemy in cybersecurity.

The solution is to make the firewall faster and smarter using artificial intelligence, specifically, machine learning (ML). The key characteristics of the ML-powered NFGW are inline machine learning, zero-delay signatures, IoT visibility, and policy recommendations.

Inline Machine Learning

Sophisticated threats often attack a single victim and expand to others. Older-generation defenses either take too long to reprogram the infrastructure to prevent subsequent attacks or stop and inspect every file, frustrating users with their slow response. In an ML-Powered NGFW, ML algorithms are embedded in the firewall code so the firewall can inspect files as they are downloaded and block malicious files instantly.

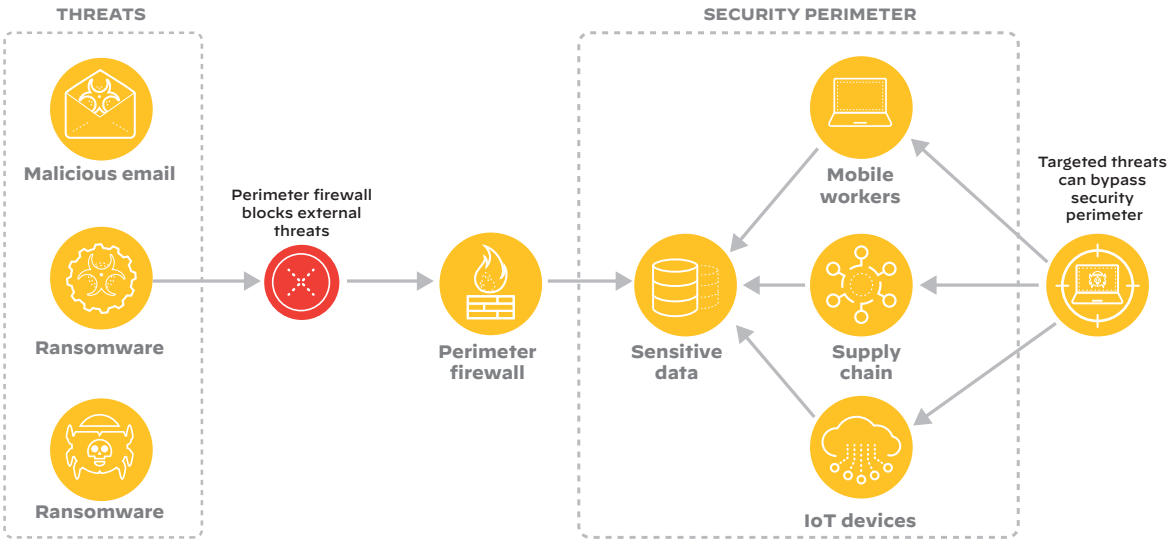

Figure 3: Network security perimeter

Zero-Delay Signatures

Inline security detects and blocks malware variants, but the most sophisticated attackers develop new malware from scratch. Traditional firewalls cannot detect these unknown threats until they receive the associated signature, which can take minutes. ML-powered NGFWs generate their own signatures via ML learning and stop unknown threats from spreading beyond the first victim.

IoT Visibility

IoT devices are proliferating at breakneck speed and IoT visibility needs to keep up. The ML-powered NGFW automatically groups similar devices together into categories derived from data analysis. As an example, the NGFW will group all security cameras into a single category, which makes it easier to track and prevent anomalous behavior in this kind of device.

Policy Recommendations

Security administrators struggle to manually update security policies to keep up with the changing threat environment as well as the proliferation of IoT and other connected devices. The ML-powered NGFW compares metadata from millions of IoT devices to that of the network to establish normal behavior patterns. For each IoT device and category, the ML-powered NGFW then recommends a policy of allowable behaviors, saving network administrators hours of manual updates.

Branch Security Redefined: PA-400 Series NGFWs

Fortunately, the ML-powered NGFW is not a hypothetical vision of the future—you can buy one today in the form of Palo Alto Networks ML-Powered NGFWs (figure 4). These innovative NGFWs offer the same world-class security as our larger models in a branch-friendly form factor that includes multiple mounting options, whisper-quiet operation, and high reliability to minimize the risk of downtime.

Palo Alto Networks recently introduced the PA-400 Series ML-Powered NGFWs, which are purpose-built for small office locations. The PA-400 Series provides the performance needed to deliver enterprise-grade security to distributed enterprise branch locations and small offices.

Independent Testing Shows Lower TCO

An independent performance validation test shows that the PA-400 Series ML-Powered NGFW offers up to a ninefold lower total cost of ownership (TCO) compared to the competition. Read the test report here.

With the PA-400 Series, network and security teams no longer must trade off security and performance at smaller offices, locations that could otherwise become targets for sophisticated attacks such as ransomware and advanced threats. Specific security

Figure 4: Primary features of the PA-400 Series NGFW

services such as Threat Prevention, WildFire Malware Prevention, IoT Security, DNS Security, Data Loss Prevention, Advanced URL Filtering, and SaaS Security are delivered via the cloud, so you can easily vary the mix of services as requirements change.

As the number of branch offices continues to grow, managing the cost of branch security becomes crucial to the organization. Panorama™ from Palo Alto Networks gives security teams a single pane of glass to manage policies centrally for all Palo Alto Networks firewalls, irrespective of their form factors, location, or scale. Security managers can use Panorama to better understand the network security deployment through centralized visibility and actionable insights.

Your Next Steps

As this white paper shows, the modern branch has security needs that transcend the capabilities of conventional approaches. Human operators—no matter how talented—simply cannot keep up with the volume and virulence of today's threat landscape. The need is for an automated security system that features inline machine learning, zero-delay signatures, IoT visibility, and policy recommendations—exactly what Palo Alto Networks PA-400 Series ML-Powered NGFW offers. Now you can have the security and performance of our larger firewalls in a form factor that is perfect for the branch environment. The benefits of the PA-400 Series appliances are low TCO, increased security, efficient operations, and intelligent policy recommendations.

Learn more about the PA-400 Series here.

See our full line of ML-Powered NGFWs here.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com