The SMB Guide to Affordable, Enterprise-Grade Security

paloalto® NETWORKS | STRATA™ BY PALO ALTO NETWORKS

Table of Contents

Introduction: Staying Ahead of Cybersecurity Threats

There's a popular misconception that cyberattacks only happen to giant organizations. But, in reality, smaller businesses are especially attractive targets because they have the sensitive information cybercriminals want but lack the security infrastructure to adequately protect themselves. Hybrid work, Internet of Things (IoT), and the explosion of cloud-based applications and services have introduced new risks—while, at the same time, threats keep getting more and more sophisticated.

If you're struggling to stay on top of cybersecurity, you're not alone.

With tighter funds and fewer IT resources, protecting your business against a constant barrage of threats can feel like an uphill battle. But with the right combination of skills, tools, and tactics, you can dramatically improve your security posture. And some good news for SMBs: The technologies you need to build an ironclad defense are more accessible than ever before.

This guide explores some cost-effective ways small- and mid-sized businesses can achieve the same level of protection as the Fortune 500.

Invest in a Next-Generation Firewall

Here's an alarming stat: **Nearly half (42%) of small and mid-sized businesses reported experiencing at least one cyberattack in the last year.**[3] The top three most common were malware, phishing, and data breaches.

These attacks can have disastrous impacts, including damage to information systems, regulatory fines, decreased productivity, and lost revenue.

So, how can SMBs stay ahead of cybersecurity threats? Reactive security can't keep up with today's threats—or prepare you for tomorrow's. A firewall should be your first line of defense to keep unwanted files from breaching your network and compromising your assets. But not all firewalls are created equal.

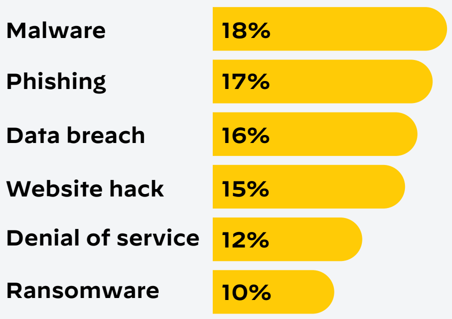
23%

of small businesses describe cybersecurity as one of the top 5 biggest threats they currently face[1]

3 out of 5

believe their business is more vulnerable to an attack as a result of employees working from home[2]

Small Business Exposure to Cybersecurity Breaches



Source: QuickBooks-commissioned survey of 2,031 small businesses throughout the U.S., March 2022.

Core Capabilities to Look For

Machine Learning-Based Analysis

Since attackers are constantly changing their techniques, security admins can't keep policy changes up to date fast enough using manual methods, let alone get visibility into the devices connecting to their networks. That's where machine learning can help by proactively identifying threats, such as malicious websites attempting to steal credentials, and then automatically updating policies to block them in real time.

Single-Pass Architecture

Historically, security professionals have pursued numerous integration approaches—including unified threat management (UTM) and deep packet inspection—to add new security innovations to their firewall. But these traditional approaches lack consistent and predictable performance when security services are enabled. As a result, IT teams frequently disabled security features on their firewall to increase throughput, putting their organization at risk. A single-pass approach to packet processing can address this challenge by ensuring traffic passes through the firewall only once—so performance never suffers no matter how many security services you enable.

Centralized Management and Visibility

As with any technology, new firewalls are not simple to deploy, configure, or manage on a day-to-day basis—especially for businesses without in-house expertise. Look for a solution that allows you to automate and centrally manage device configuration, policy deployment, and forensic analysis—while providing single-pane-of-glass visibility of your firewalls and other security tools.

SSL Decryption

Today, more than 80% of public internet traffic is encrypted.4 Because organizations can't see what's inside encrypted traffic, they can't spot potential threats before havoc ensues. Malicious actors often exploit this lack of visibility to infect legitimate websites, deliver malware through software-as-a-service (SaaS) apps, and even place infected files inside sanctioned file storage apps, such as Dropbox.® To protect your organization from these threats, you need a firewall with SSL decryption, which provides the ability to decrypt, inspect, and re-encrypt traffic before it reaches its destination. See 10 Best Practices for SSL Decryption.

5 Security Features to Include in Your Defense Lineup

1. Intrusion Prevention

Stop unknown and evasive threats in real time using custom machine and deep learning models garnered from millions of data points.

Why it's important: Today's attackers use evasive tactics to gain footholds in networks and launch advanced attacks at high volume while remaining invisible to traditional independent defenses.

2. DNS Security

Apply predictive analytics to disrupt attacks that use DNS for command-and-control or data theft.

Why it's important: Over 80% of malware uses DNS to establish communication with a command-and-control (C2) server.[5] But most security teams lack basic visibility into how threats use DNS to maintain control of infected devices, making it nearly impossible to identify and stop DNS threats.

3. Advanced URL Filtering

Perform real-time analysis of web traffic by categorizing and blocking malicious URLs before they have a chance to infect your organization.

Why it's important: Web-based attacks like phishing are coming at higher volume and greater speed, yet many security solutions depend only on databases of known malicious web pages that are quickly overrun by the hundreds of thousands of new threats created every day.

4. Automated Malware Analysis

Ensure files are safe with automatic detection and prevention of unknown malware.

Why it's important: In addition to securing a growing number of e-service portals, security teams have an ongoing storm to deal with: fighting email phishing. Triaging email phishing threats is time consuming, but automation can reduce the load on security professionals and accelerate incident response processes.

5. IoT Visibility and Security

Take a machine learning-based approach to discover all unmanaged devices, detect behavioral anomalies, and automate policies—without the need for additional sensors or infrastructure.

Why it's important: IoT has arrived in a big way, accounting for over 30% of all network-connected devices at the average business.[6] In far too many cases, organizations aren't aware of all the things that are running or the risks those things may represent.

Increase ROI and simplify deployment by utilizing subscription-based security services on top of the firewall, enabled at the click of a button

How AIOps Can Help Small Teams Optimize Firewall Operations and Maximize ROI

Investing in sophisticated security equipment pays only when that equipment is used properly. New technologies like AIOps address the top operational challenges security teams face—such as misconfigurations and best practice compliance—while delivering a wide range of insights for the best security posture and optimal health. Since AIOps can help to quickly discover issues, it decreases pressure on small teams—enabling them to focus on value creation.

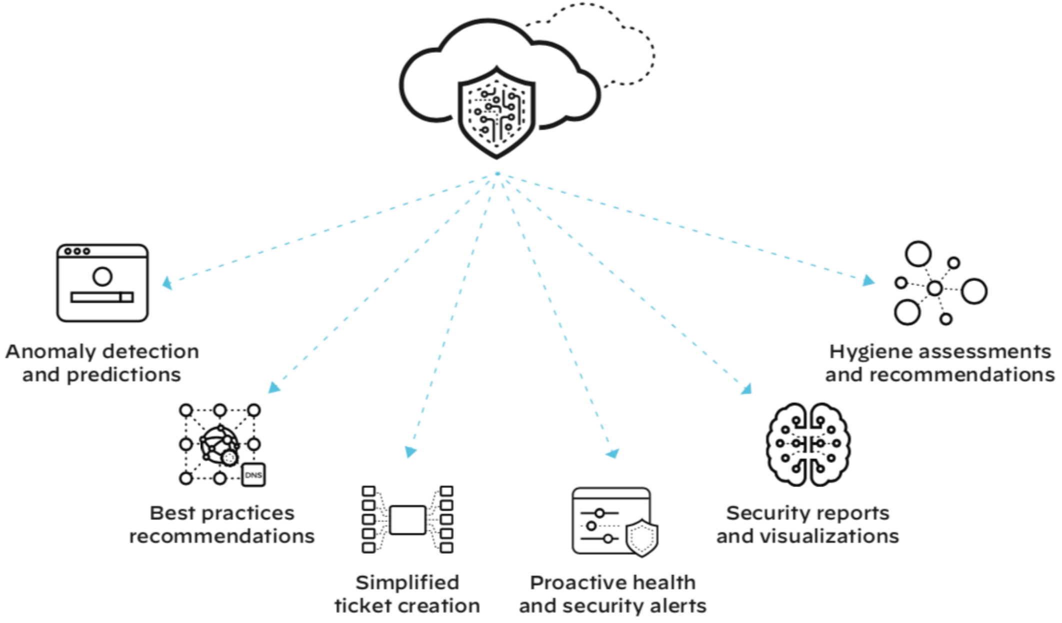

Anomaly detection and predictions
Best practices recommendations
DNS
Simplified ticket creation
Proactive health and security alerts
Security reports and visualizations
Hygiene assessments and recommendations

Figure 1: AIOps for NGFW delivers a range of actionable insights

Build a Strong Security Culture

Exploring the latest and greatest technologies is important, but one critical element often gets overlooked: the human element. According to the 2022 World Economic Forum Global Risks Report, 95% of all cybersecurity issues can be traced to human error.[7] Many threats, including phishing, can be mitigated using less-advanced methods grounded in creating cultural change through human behavior and education.

12 Simple Security Best Practices for SMBs

1. **Provide constant reminders of the importance of security:** While human error will always come into play, you can minimize incidents by implementing training and awareness programs. Topics should include:
   - Spotting phishing emails
   - Using good browsing practices
   - Avoiding suspicious downloads
2. **Make training more engaging:** Running "PhishMe" campaigns can be a great way to train employees on better email security. This includes regular phishing emails sent across the organization to test employees' response and action. Using gamification (think: badges or points displayed on a scoreboard) is one way to reward those employees who adhere to the correct security guidelines, which will further promote good behavior.
3. **Enforce safe password practices:** Require unique, complex passwords that include uppercase and lowercase letters, numbers, and symbols—and make sure employees change those passwords every 60 to 90 days.
4. **Use multifactor identification:** To be even more secure, think about requiring additional information beyond just the password to gain access. Using the multifactor identification settings on most major network and email products is simple to do and provides an extra layer of protection. Employees' cell numbers are a good second form since it's unlikely a hacker will have both the PIN and the password.
5. **Develop a robust patch-management program:** Be diligent about installing patches and updates as soon as they're available to best protect against ransomware, malware, viruses, and other cyberthreats.
6. **Stay educated on the evolving threat landscape:** Security is a moving target. Stay on top of the latest attack trends and the newest prevention technology to protect your organization.
7. **Focus on vulnerable targets:** Identify your exposed assets—anything on the public internet—so you can take steps to reduce your attack surface.
8. **Prioritize efforts:** Analyze the business impact of losing critical data to understand what's really at risk, including any potential upstream and downstream consequences, to help you prioritize efforts.
9. **Document your cybersecurity policies:** Cybersecurity is one area where it's essential to document your protocols and make sure key people in your company are updated on all changes.

10. **Back up all data:** With ransomware on the rise, the best defense is to constantly back up data. That way, even if data is stolen, it's not lost. The best way to do this is to auto-mate the data backup process, storing copies of word processing documents, databases, spreadsheets, human resources (HR) files, and other key files and data in the cloud or offsite.

11. **Provide access on a "must-have" basis:** Employees should only be given access to the specific systems they need for their jobs and should be strictly prohibited from installing software on their computers or other devices used for work without authorization.

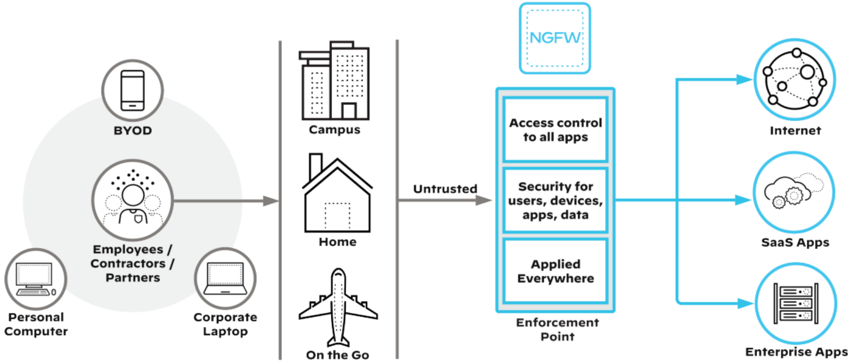
12. **Proactively identify risks:** A cybersecuri-ty risk assessment can identify where your business is vulnerable—across people, pro-cesses, and technology—and help you create a plan of action.

Create a Future-Proof Work-from-Anywhere Strategy

In 2021, over 80% of businesses surveyed by Gartner said they intended to maintain remote work part of the time—and the trend has not shown signs of slowing down.[8] In order to meet the needs of a hybrid workforce, SMBs accelerated the move to cloud-based tools and applications. But that's brought new challenges for over-stretched IT and security staff. To help counter the security threats created by today's borderless workplace, many businesses are making the move to a Zero Trust Model.

What Is Zero Trust?

Zero Trust is a strategic approach to cybersecurity based on eliminating implicit trust and continuously validating every stage of a digital interaction. This means eliminating implicit trust related to users, applications, and infrastructure.



Navigating the Zero Trust Identity Crisis

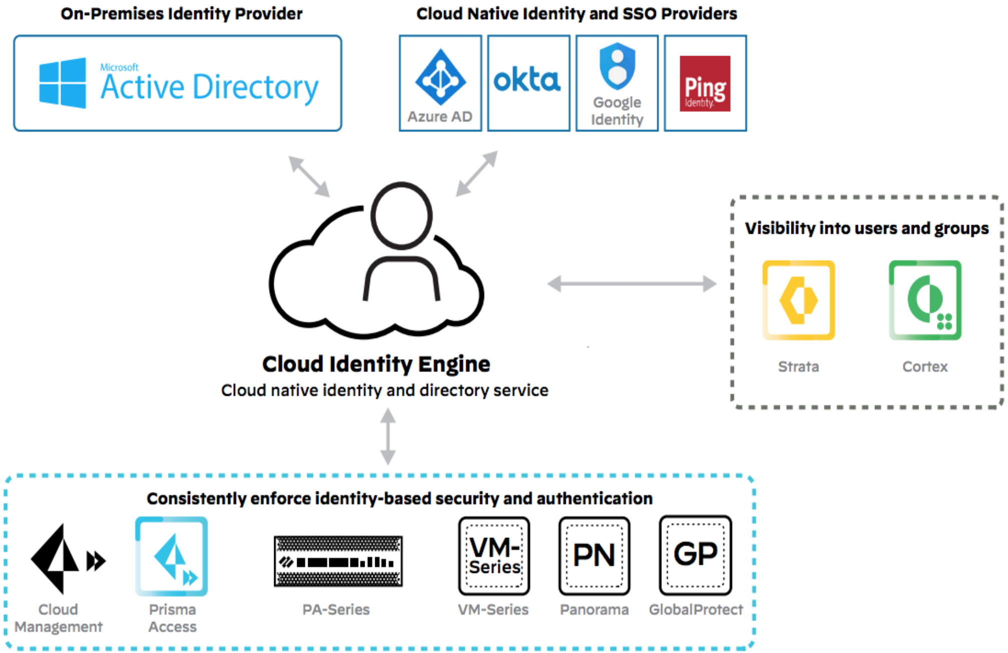
There are many elements to creating a Zero Trust architecture, but identity is at its core. A few years ago, managing identity was a simpler proposition, with users typically working from company offices and authenticating through an on-premises identity provider. The move to hybrid has resulted in many businesses maintaining a patchwork of on-prem and cloud-based identity solutions. But this fragmentation created a multitude of challenges. Security teams are struggling to consistently verify users and enforce identity-based security at all times for three primary reasons:

1. User information is distributed between multiple identity providers, resulting in increased operational complexity.
2. Authentication with cloud identity providers typically requires a labor-intensive authentication setup, with unique configuration requirements for each security device with every identity provider.
3. Lack of visibility into user activity and consistent application of identity controls across the network results in critical security gaps.

Why Today’s Cloud-First World Demands a Highly Adaptable Solution

To make Zero Trust a reality, SMBs need to adopt a new approach: a cloud-based architecture for identity management that can serve as a single source of identity, seamlessly connecting both on-premises and cloud-native identity providers. By unifying identity across the enterprise at a single point, security teams can reap a number of benefits:

- Zero Trust achieved through always-on identity
- Real-time synchronization of user group and authentication information across the entire network security infrastructure
- Fast and easy integration of new identity providers
- Enterprise-wide visibility into users and groups


On-Premises Identity Provider
Microsoft Active Directory
Cloud Native Identity and SSO Providers
Azure AD
okta
Google Identity
Ping Identity
Cloud Identity Engine
Cloud native identity and directory service
Visibility into users and groups
Strata
Cortex
Consistently enforce identity-based security and authentication
Cloud Management
Prisma Access
PA-Series
VM-Series
VM-Series
PN
Panorama
GP
GlobalProtect

How We Can Help

At Palo Alto Networks, we believe every organization deserves access to the same level of protection as the Fortune 500.

To bring that vision to life, we offer services and solutions designed to help small and distributed businesses bolster defenses and scale security as business grows. That includes affordable, all-in-one subscription bundles that provide the best security possible at the lowest total cost of ownership.

Learn More

Contact your sales rep

Download

PA-400 Series Solution Brief

Miercom Performance Validation Testing Report

Experience

Take a Virtual Ultimate Test Drive

Sources:

1. QuickBooks-commissioned survey of 2,031 small businesses throughout the U.S., March 2022
2. Hiscox Cyber Readiness Report 2022
3. QuickBooks-commissioned survey of 2,031 small businesses throughout the U.S., March 2022
4. Sandvine Global Internet Phenomena Report, 2022
5. Palo Alto Networks Unit 42™ Threat Research
6. Palo Alto Networks Unit 42™ IoT Threat Report, 2020
7. World Economic Forum Global Risks Report, 2022
8. Gartner, Inc. survey of 127 company leaders, representing HR, Legal and Compliance, Finance, and Real Estate, 2020

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