Bloomington-Normal Innovation Alliance

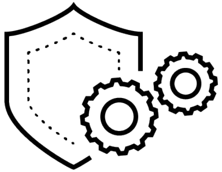
Central Illinois Cyber Security Summit

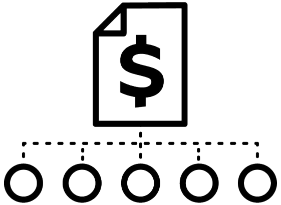
June 22, 2023

Daniel Skalitzky
Named Account Manager
Palo Alto Networks

June 2023

Small & Mid-Sized Business Security Challenges





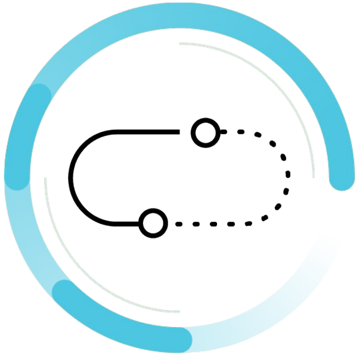
Limited IT resources can hinder the maintenance of a strong security posture with ongoing digital transformation, new apps and devices coming online everyday

Agility to move quickly and adopt new SaaS applications can create new security vulnerabilities

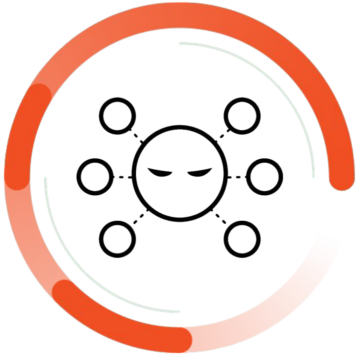
Low TCO is essential for SMBs to keep their operational costs lower and succeed in their business outcomes

The Challenge: Attacker Innovation is Increasing

Speed and Proliferation
of Attacks



Easy-to-bypass
legacy analysis techniques



Increasing
attack surface

7 Simple Steps to Help Deter Cyberattacks for SMBs

These 7 steps can help deter the fly-by-night script kiddy scanning the Internet for an opportunity. These are not in any particular order - you should implement each recommendation at the very least.

1. **Use a Next-Generation Firewall (NGFW)** – Protect the perimeter. Next generation firewalls utilize machine learning and AI to identify unknown and zero-day attacks. Constantly updated threat intelligence ensure firewalls are always up-to-date on the latest threats.
2. **Keep Applications and Operating Systems Updated** - Updates patch security vulnerabilities, add new security features, and fix bug issues.
3. **Train users to identify phishing attacks** – User education and awareness are critical in defending against cyber crime. Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines.
4. **Implement multi-factor authentication and require strong passwords** - Multi-Factor Authentication (MFA) is a method of computer access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).
5. **Make sure you can identify all users, devices, and applications on your network** - Visibility. Understanding what is on your network helps identify rogue users, devices and applications.
6. **Disable remote access or limit its use and use VPN for access** - Do not allow remote access on Internet facing desktops - Require a secure VPN for access to any inside resource.
7. **Privileged Access Management** - Limit Administrator rights to only those who need it. Do not set user rights on desktops to local administrators.

Enterprise-Class Security for SMBs and Branch Locations

Palo Alto PA-400 Series Next Generation Firewall

Simplified Operations

- **Easy deployment** - Zero Touch Provisioning (ZTP), compact form factor for out-of-closet deployments
- **Ease of management** - Web GUI, CLI and centralized dashboard (Panorama)

Better Performance

- **Zero trust security** model detects and responds to sophisticated attacks, segments sensitive data and critical applications
- **Enterprise-grade features and best in industry performance with** upto 2.6 Gbps of threat performance and embedded machine learning (ML) to predict next set of attacks

Low TCO

- **Competitively priced** hardware and bundled services that offer superior security feature set
- **Consolidated security** solution in a single appliance (including securing IOT devices and SaaS apps)
- **Reliability** - High mean time between failures (MTBF), power redundancy, fanless, no moving parts and Active/active or active/passive HA

Thank you

paloaltonetworks.com