Credential Theft:

It's Time to Take Back Control

IT security—it's a ubiquitous concern for every organization. The sophistication of attacks is constantly increasing, and in response security teams have fortified their network perimeter defenses, strengthened advanced malware protections, upgraded vulnerable operating systems, automated patch deliveries, and developed counter-measures to spot intruders. Good? Yes. **But not good enough.**


- All Sights on the Weakest Link -
Threat actors have shifted their attention to the user
Passwords are one of the weakest links in IT security
Faster, cheaper, and far easier to steal a user password
Recent refinements in trick techniques
Highly-focused approach targeting very specific victims

Top Five Ways Attackers Steal Credentials

Now that we know why they do it, it's important to understand how they do it. There are five primary techniques that attackers use for stealing credentials:

SOCIAL ENGINEERING

Can occur over email, with leading email subjects and texts designed to encourage the user to click a link or open an attachment

CREDENTIAL PHISHING AND SPAM

An email message attempts to lure its recipient into logging into an account

REUSING STOLEN PASSWORDS OR SHARED CREDENTIALS

There's a booming business buying and selling stolen credentials online

BRUTE FORCE

Many users simply use weak passwords

SECURITY QUESTION REUSE

Easy for attackers to find, guess, or exploit

How Do You Stop the Bad Guy that Looks Like a Good Guy?

Once credentials are stolen, it becomes very difficult to stop adversaries who appear to be valid users:

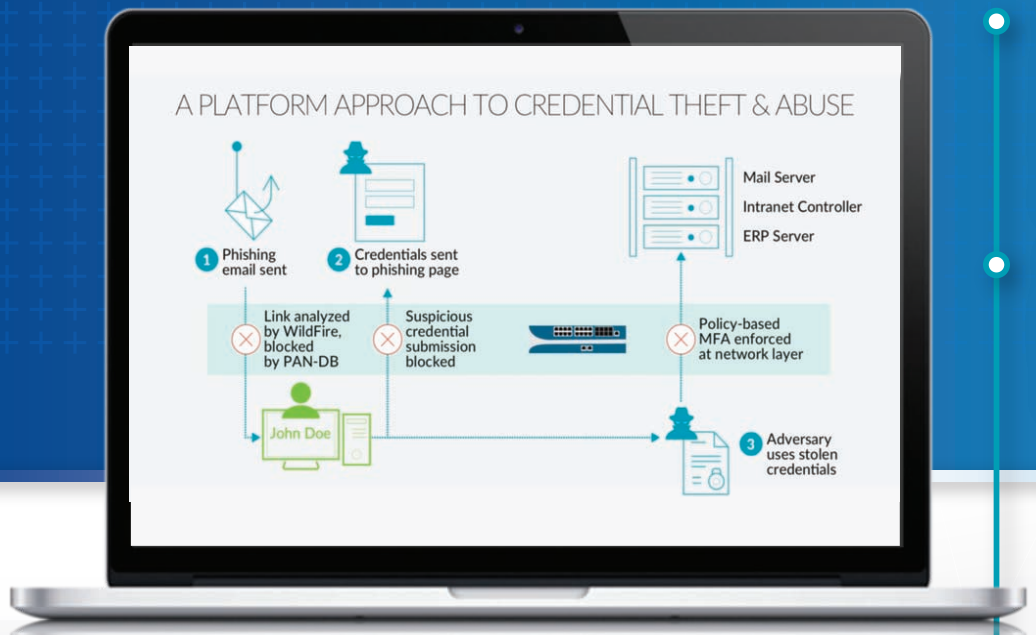
+ Stolen passwords provide a direct path towards application and network access
+ Attackers use lateral movement to set up a broader footprint inside the organization
+ Compromise other systems and stealing more credentials along the way

Why aren't best practices for passwords working?

- Filtering technologies are less effective on targeted attacks
- Multi-factor authentication is often deployed in a limited manner
- Cloaking techniques can allow attacks to reach the user

Neutralizing Credential Theft and Abuse with Palo Alto Networks

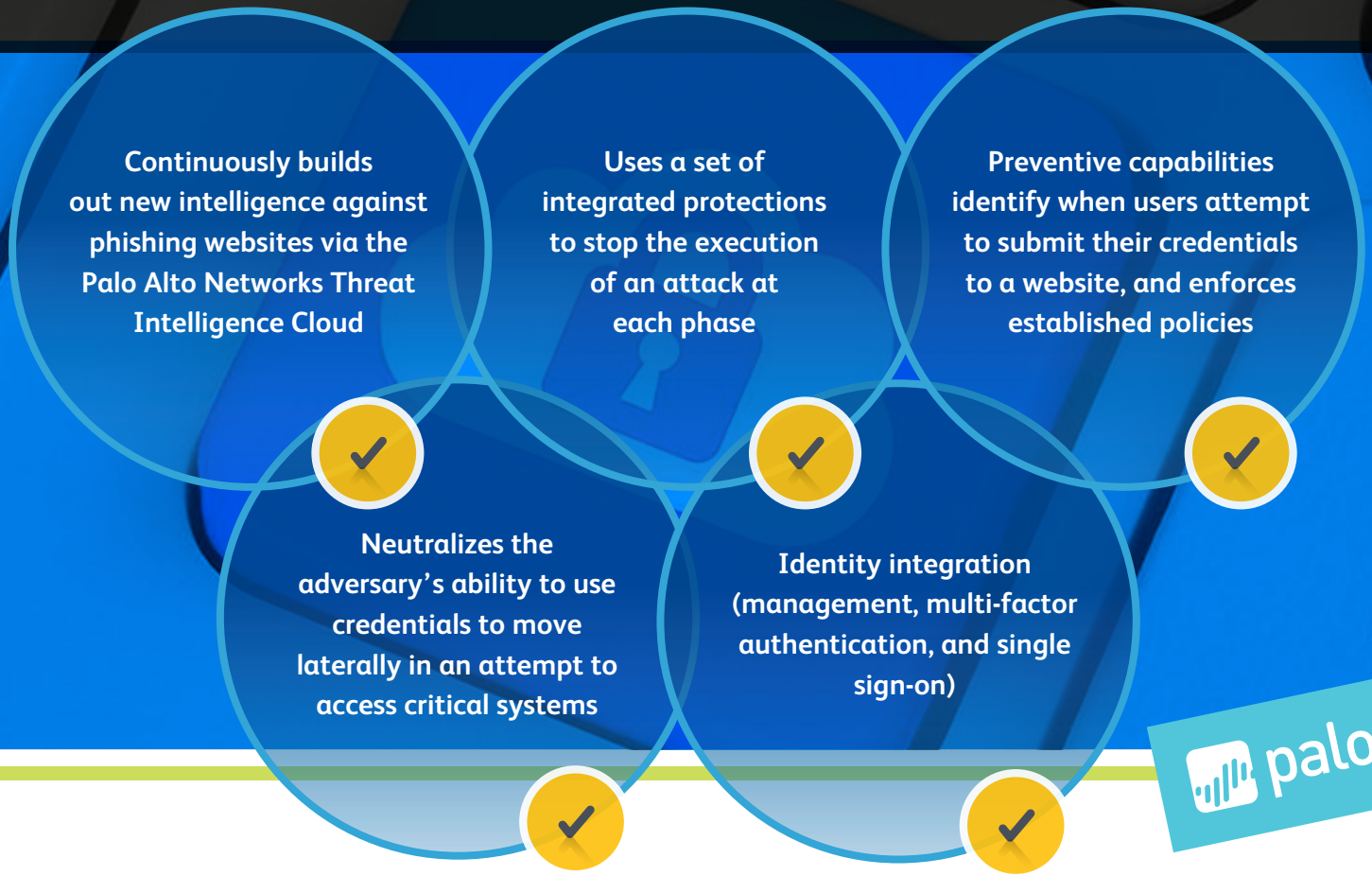
New ideas are necessary in order to break past the limitations of traditional security measures.



- Take action against your exposure to risks by implementing the protections of the Next-Generation Security Platform developed by Palo Alto Networks to address credential phishing and abuse.
- These measures establish important preventive capabilities to reduce risk and bolster the protections that are in place within your organization to stop cyberattacks.

Preventing Credential-Based Attacks

The Palo Alto Networks Next-Generation Security Platform takes a revolutionary new approach toward the problem of credential theft, using a set of integrated protections to stop the execution of an attack at each phase.



paloalto NETWORKS®

Optimizing Your Security Program and Deployment

As a leader in cybersecurity services, ePlus creates custom, integrated programs to help protect your organization—and your brand.

- Develop a strong risk management framework
- Prevent, defend against, and recover from malicious cyberattacks
- Reduce overall risk
- Ensure enterprise and data security across a new digital landscape
- Build a strong security culture
- Support innovation and digital transformation

To learn more about leveraging the joint expertise of ePlus and Palo Alto Networks to take back control and address today's credential threats, contact us today.

: 888-482-1122
: security@eplus.com
: www.eplus.com/security

Corporate Headquarters
13595 Dulles Technology Drive
Herndon, VA 20171-3413
Nasdaq NGS: PLUS