CYBERARK®

SOLUTION BRIEF

CyberArk & Proofpoint: Better Together

The shortcomings of the classical approach to cyber security

Attackers are continually getting smarter, continuing to use old and proven attack vectors and coming up with new ones. This results in continued growth of the number of successful attacks and data breaches on the backdrop of skyrocketing endpoint security spending.

The classic view of risk means understanding the probability of breach, likelihood that attacks will be successful, and the impact on your organization if that person is compromised. As a result, most defenders (people in IT) operate with a network-centric point of view, thinking in terms of IP addresses, ports, and segmentation. With this view, when you want to protect something on your network (e.g. server, database, device), you put a firewall in front of it, microsegment it on a VLAN, or control access to the system via VPN. The adoption of cloud apps and platforms, like Office 365 or Amazon Web Services (AWS), challenges the network-centric approach because it makes it difficult to:

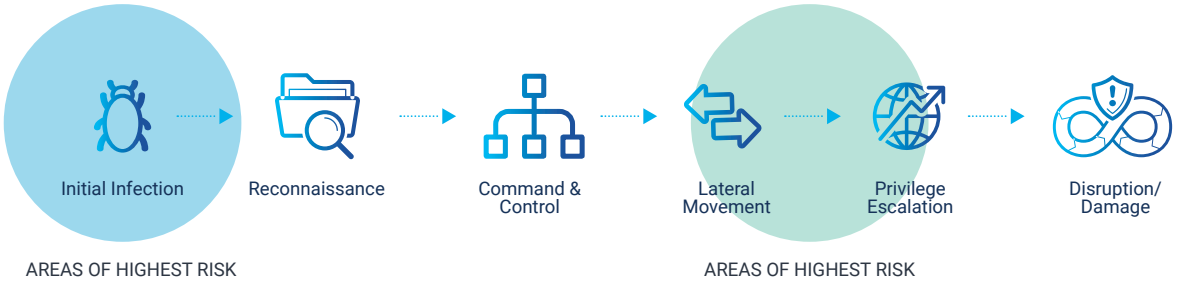
- Gain visibility into ALL types of threats that affect your people – threats in the cloud may never traverse your network.
- Prioritize alerts and incidents according to relative risk to your organization.

Attackers also do not think of their targets in terms of network diagrams. As the most widely used mechanism to overcome perimeter-based controls like firewalls, identities with access to sensitive systems are increasingly under attack. Attackers will try to exploit any weakness their target organization might have, be it a less knowledgeable or simply careless employee, a cloud service misconfigured to grant access to many identities, or privilege creep and permissions sprawl. They can also use cloud services to launch infrastructure as a foundation for a targeted threat campaign against your organization.

LOOKING AT THE AVERAGE ATTACK PATHWAY, THERE ARE MOST OFTEN TWO AREAS WHICH POSE THE HIGHEST RISK:

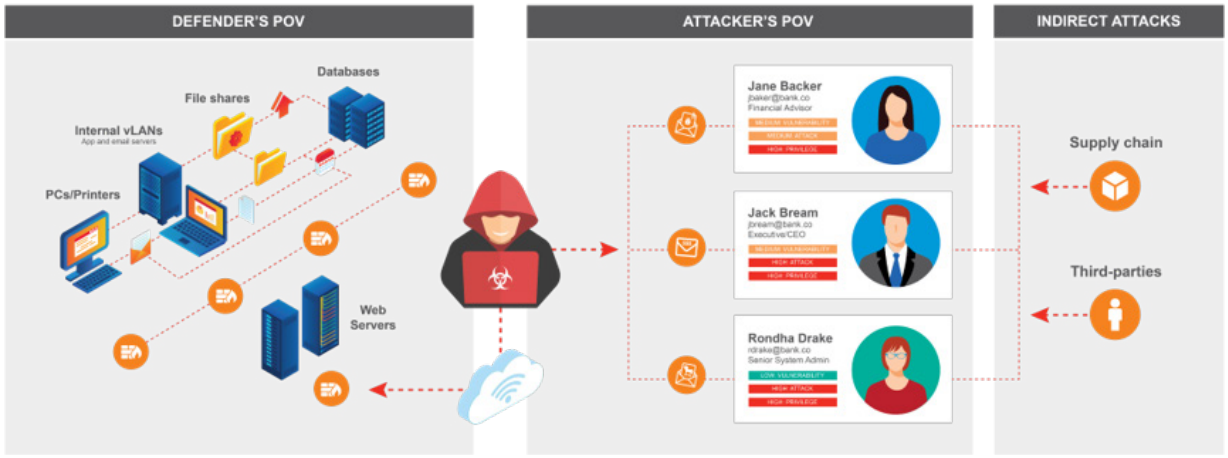
The initial infection > most of the time this happens through email

Credential compromise/privilege elevation > access to systems / data



How to better protect your organization

There needs to be a fundamental shift in how we approach cybersecurity strategy: exercising the attacker's view and adopting the defense-in-depth – a comprehensive, multi-layered security approach. Stop trying to win a "whack a mole" game by focusing on the fastest incident response and relying on your backups. Instead, start preventing the majority of incidents from ever happening by understanding how the criminals get initial access – compromised identities and credentials - and reducing risk with defense-in-depth controls.



The first step for most defenders should be to start by identifying which people pose the highest risk (i.e. being attacked) and how they represent risk to your organization.

RISK LEVEL WILL GENERALLY FALL INTO ONE OF THREE CATEGORIES:

Vulnerability: Who is likely to fall for threats?

- Clicks on malicious content
- Fails awareness training
- Uses risky devices or cloud services

Attack: Who gets targeted by serious threats?

- Receive highly targeted, very sophisticated, or high volumes of attacks

Privilege: Who has access to valuable data?

- Can access critical systems or sensitive data
- Can be a vector for lateral movement

Understanding this and striving to provide comprehensive protection from advanced cyber-attacks, Proofpoint and CyberArk teamed up and together enable your organization to significantly reduce the area of attack, block most common cyber attacker entry ways and help satisfy audit and compliance requirements. While Proofpoint helps you understand and gain visibility into your greatest risk – your people, and the data they have access to as well the behaviors that indicate they might fall for a modern, social-engineered attack, CyberArk helps remove local admin rights, manage privilege on the endpoints and lock down access to mission-critical resources. Together, the services position you to confidently defend against attacks, including ransomware.

WHO ARE WE?

What Proofpoint Does

Proofpoint delivers the most effective solution to protect your people and critical data from advanced email threats. Our complete email security platform not only blocks malware and non-malware email threats, such as email fraud, but it also provides visibility into your greatest risk—your people. One way it does this is by identifying your Very Attacked Persons (VAP), surfacing the threats attacking them as individuals, and scoring those threats with our Targeted Attack Protection (TAP). Having this visibility means you can better focus your security efforts where the risk is.

Proofpoint also continually protects your organization even after users receive emails by monitoring late-stage malware that can be activated through email forwarding, blocking those threats, and retroactively pulling those emails or threats when needed.

Benefits

- Recognize and Protect against imposter threats
- Defend against email and supplier fraud
- Detect and block advanced malware before they reach the Inbox
- Identify risky users
    - VAPs
    - Phishing users
    - Top Clickers
- Automatically pull malicious emails with one click
- Internal mail defense
- Email continuity

PROOFPOINT

- #1 most deployed solution for F100, F1000, G2000
- 150k+ Customers Globally
- Magic quadrant leader

CYBERARK

- #1 leader in Privileged Access Management
- 7,000+ PAM customers globally; 6,900+ Endpoint Privilege Manager customers globally
- Over 50% of the F500
- Leader in Gartner Magic Quadrant, Forrester Wave, and KuppingerCole Leadership Compass

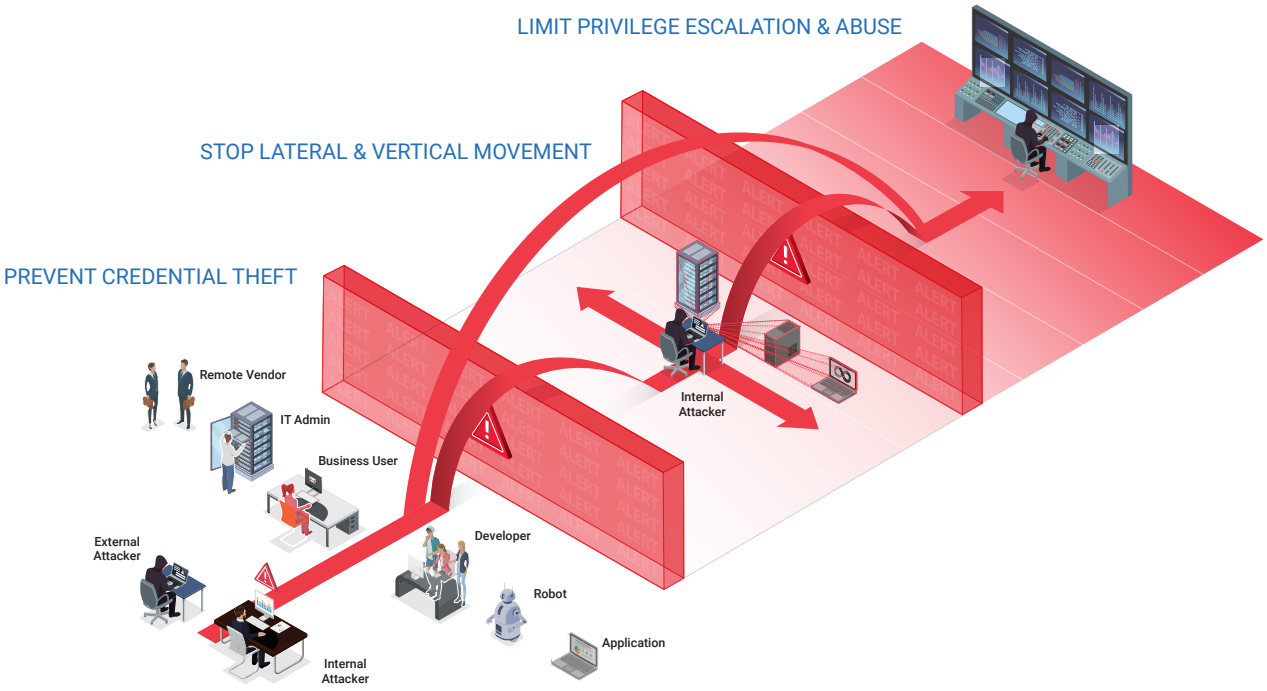
What CyberArk Does

At CyberArk we help organizations to put identity security controls in place that mitigate the risks associated with the most common attack paths the cybercriminals take. We use the three guiding principles that form our “best practice framework”, or Blueprint:

1. **Defend against Credential Theft:** Ensure your privileged passwords and keys, both for human & non-human entities, are kept out of harm's way. Securely store, programmatically rotate, and tightly control access to credentials providing access to sensitive resources. Cut back on the credential residue that exists across workstations, servers, applications, and source code repositories. Prevent adversaries, both internal and external, from gaining access to the keys to the kingdom by layering Adaptive MFA at both the endpoint login and privilege escalation.

2. **Stop Lateral & Vertical Movement:** Stop attackers from pivoting from a non-trusted environment to a high-risk environment. Prevent threats from getting off the endpoint by removing local admin rights. Isolate privileged sessions to prevent the spread of malware between systems. Reduce excessive privileges and permissions – on-premises and in the public cloud.

3. **Prevent Privilege Escalation & Abuse:** Drive down the number of privileged accounts and the capabilities of these accounts to reduce your attack surface. Control processes through which users gain privilege in order to limit opportunities for escalation. Identify and onboard sensitive cloud admin and shadow admin for secure credential management. Establish a baseline for what privileged accounts should actually be used and detect anomalies that signal someone may be abusing them.



Defend against attacks

- Reduce the attack surface, complicate lateral movement and render vulnerabilities unexploitable by removing local admin rights and requiring MFA at login or privilege elevation.
- Extensive protection against a range of attacks, from common identity-based attacks to highly sophisticated threats.

Drive Operational Efficiencies

- Simplify operations, reduce the risk of the human error and achieve endpoint hardening without impacting workforce productivity.
- Unified privilege and access processes across all identities using a consistent approach and best practices.
- Consolidation of key identity security technologies including privilege, access and secrets management

Enable the Digital Business

- Quickly adopt and secure modern technology (SaaS applications, public cloud workloads, DevOps tools, including those managed by third parties).
- Encourage user independence, flexibility and moving fast without jeopardizing security. Align security to your business goals.
- Improved customer trust by reducing risk of lost data or operational disruption

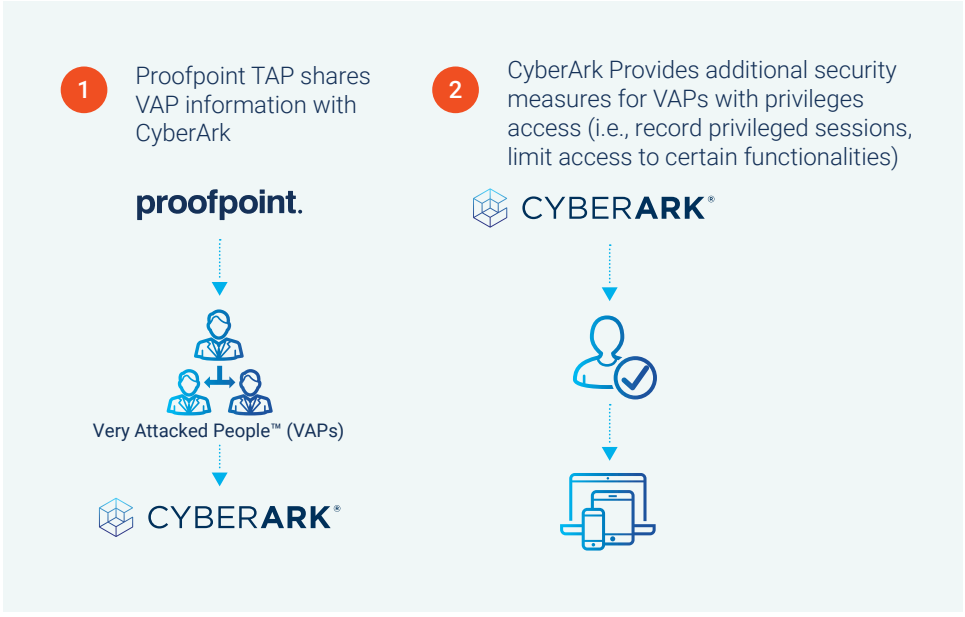
Enable audit and improve compliance

- Add identity, access, and privilege context, and boost visibility. Satisfy compliance requirements such a wide range of CIS Controls, create audit trail for privileged actions. Build and maintain software inventories for audit purposes.
- Continuous compliance with frameworks and regulations such as SOX, NIST, CMMC, PCI DSS, SWIFT and HIPAA with CyberArk's comprehensive, strategic and unified security approach.
- Improved confidence and efficiency in achieving audit/compliance requirements.

HOW WE WORK TOGETHER

Privileged Access for Proofpoint VAPs

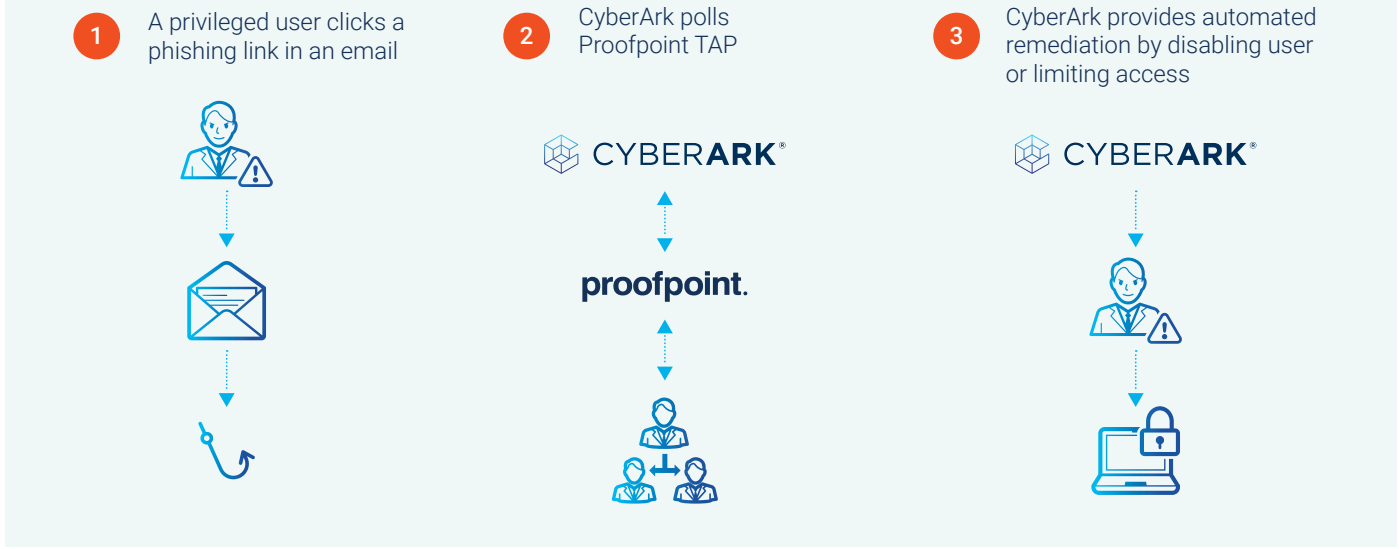
As mentioned earlier, Proofpoint TAP identifies the VAPs within your organization and shares that information with CyberArk. CyberArk can then manage the privileged access of those users who have a high level of threat severity to provide the security and privileged access needed to safeguard your organization.



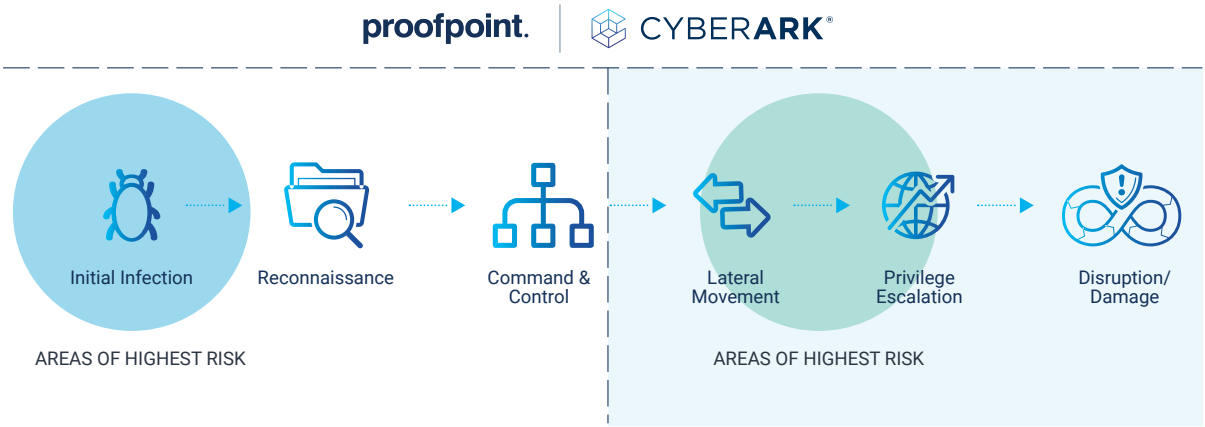
CyberArk provides additional security measures, including removing local admin rights, enforcing least privilege, requiring MFA at endpoint login and privilege escalation, privileged sessions recording, and limiting access to certain features.

Automated remediation for potentially compromised users

To guard against the more advanced techniques of today's threat actors, such as time-delayed attacks, Proofpoint TAP rewrites every single URL and provides click-time sandboxing for every one of your users. TAP can identify a malicious link when a user clicks it inside an email and then shares this with CyberArk. CyberArk then provides real-time remediation by automatically disabling certain features, disabling the user completely, or forcing a real-time change of password or credentials.



WHEN EMAIL SECURITY AND PAM ARE INTEGRATED:



With Proofpoint and CyberArk you can protect the high-risk areas of the attack pathway and guard against the way threat actors are targeting users.

- Identify and secure your organization's biggest risk: your people
- Contain and remediate email-based threats
- Apply adaptive authentication controls to thoroughly validate high-risk privileged users

PROOFPOINT AND CYBERARK

- Support Zero Trust initiatives by applying adaptive controls to users that present material risk
- Thwart attackers from reaching their end goal through a defense-in-depth approach
- No cost/free integration. Immediate time to value through out-of-the-box integration

CYBERARK