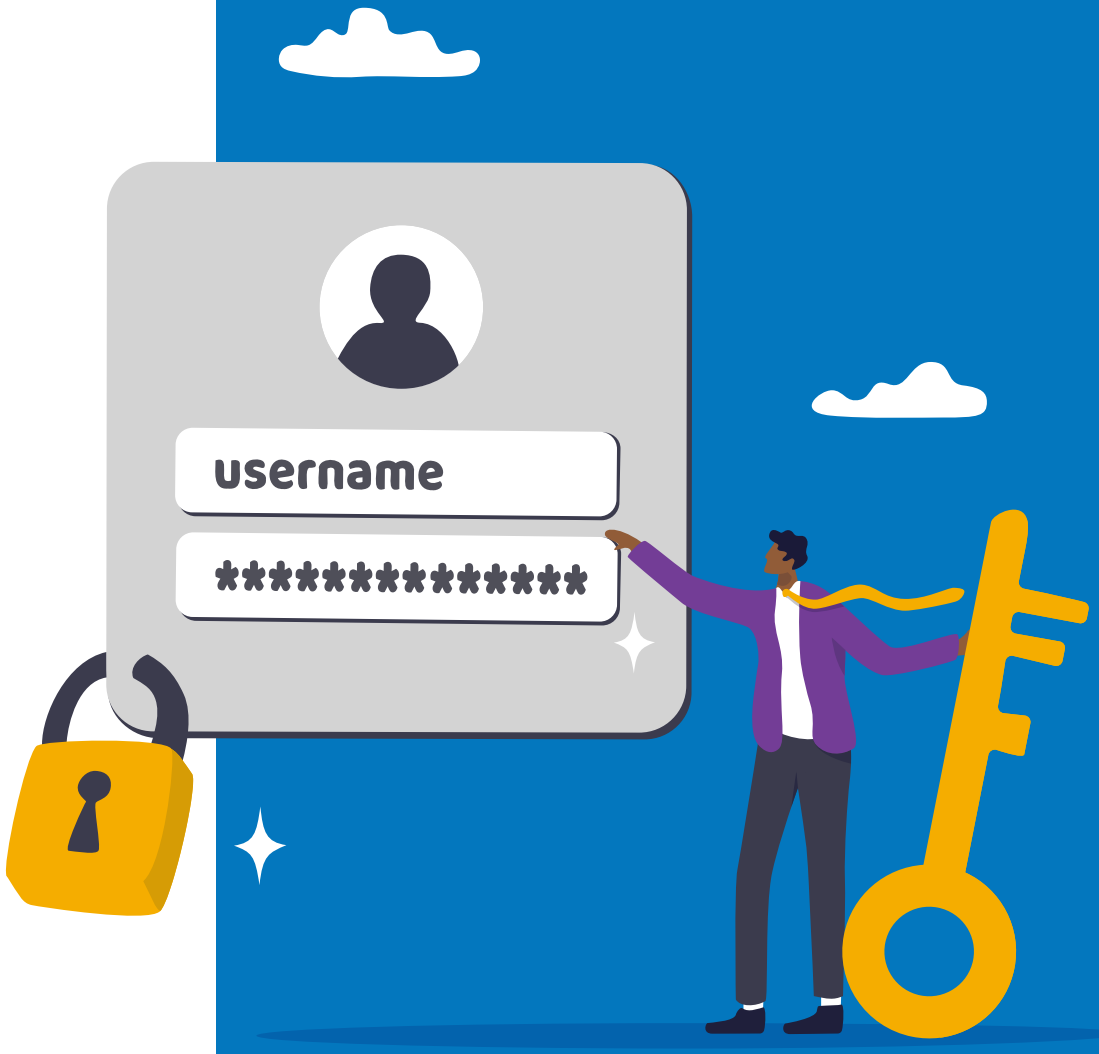
E-BOOK

Securing Your Identity with Proofpoint

Real-world use cases and success stories



proofpoint.

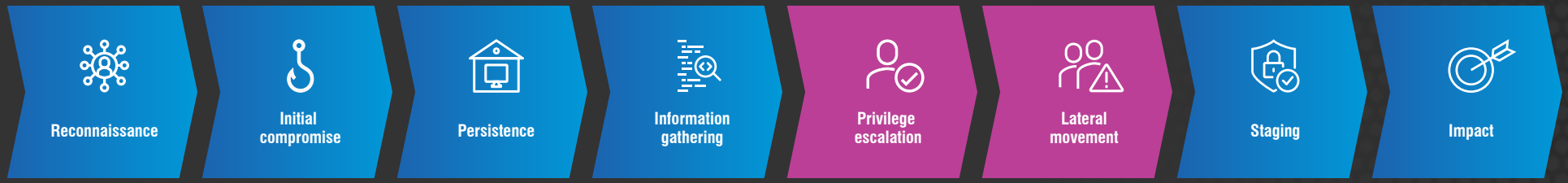
Introduction

Privilege escalation and lateral movement are a persistent challenge for most security teams—even at the biggest companies in the world. Just look at Microsoft. In January 2024, the company announced that it had been breached by a notorious group of threat actors backed by Russia.

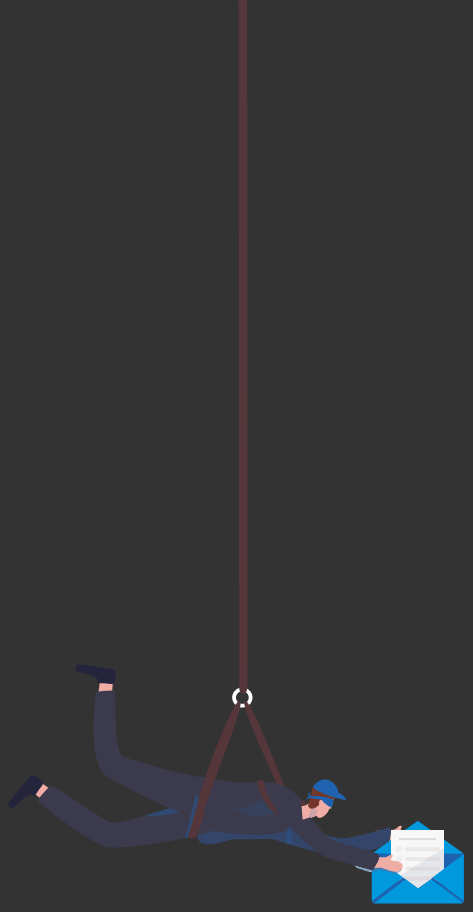
The attackers exploited an unprotected legacy test account. Once they compromised it, they escalated their privileges and moved laterally through Microsoft's cloud systems. And here's the rub: because they were posing as legitimate users, they weren't detected for more than a month.[1]

Breaches like this highlight the weakness in the middle of the attack chain. It's here that attackers use compromised accounts to break through the next layers of a company's defenses. They do so by exploiting misconfigurations and finding identity vulnerabilities to gain access to accounts with higher and higher privileges.

Privilege escalation and lateral movement



1 Bleeping Computer. "Microsoft Reveals How Hackers Breached Its Exchange Online Accounts." January 2024.



This part of the attack chain plays a critical role in cyberattacks. With a stolen identity, attackers look just like a legitimate user, which makes them effectively invisible. And because they're invisible, they can do almost anything. That includes resetting passwords, changing policies, installing software and extracting and encrypting data for ransom.

So what can be done to stop them?

Proofpoint Identity Protection gives you the analytics you need to find your vulnerable identities and remediate them before attackers get to them. But not only that. It also enables you to shine a light on active attackers once they get inside your environment.

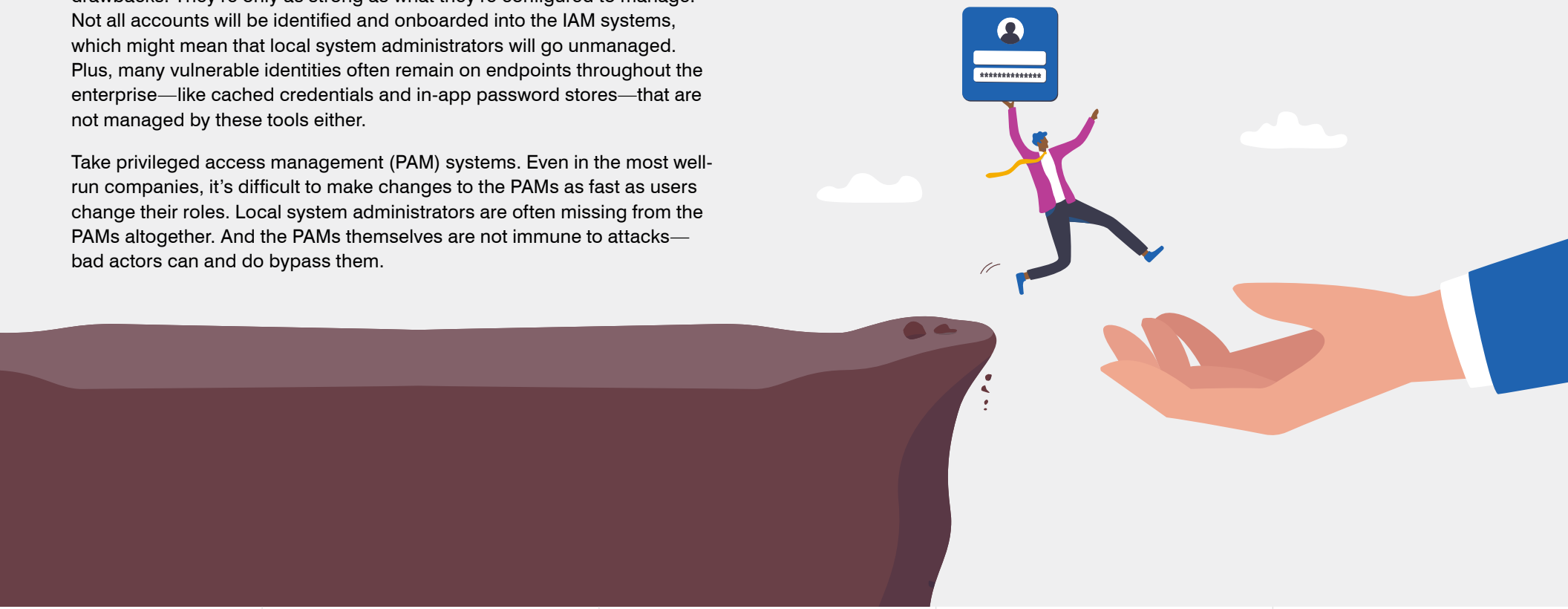
This e-book provides three use cases to show you how it works. And it details real-world customer stories so that you can see what Proofpoint Identity Protection looks like in action.

USE CASE 1:

Close Security Gaps Left by IAM Tools

All common identity access management (IAM) tools share the same drawbacks. They're only as strong as what they're configured to manage. Not all accounts will be identified and onboarded into the IAM systems, which might mean that local system administrators will go unmanaged. Plus, many vulnerable identities often remain on endpoints throughout the enterprise—like cached credentials and in-app password stores—that are not managed by these tools either.

Take privileged access management (PAM) systems. Even in the most well-run companies, it's difficult to make changes to the PAMs as fast as users change their roles. Local system administrators are often missing from the PAMs altogether. And the PAMs themselves are not immune to attacks—bad actors can and do bypass them.



Summary

An auto finance company uses Proofpoint to expand its security capabilities to include identity risk management.

Customer profile

Industry: Financial

Employees: 9,000

Location: Global

Solution

Product: Proofpoint Identity Protection

Component: Proofpoint Spotlight

How Proofpoint helps

A component of Proofpoint Identity Protection, Proofpoint Spotlight helps you see your vulnerable identities and close your identity security gaps before attackers exploit them. It does this by scanning your endpoints, IAM systems and identity repositories for unmanaged, misconfigured and exposed identities. The results of these scans are presented to you in an easy-to-digest report. The report shows you all the available attack paths, and it gives you a list of the identities that you should remediate first.

Proofpoint in action

An auto finance firm upgrades its security capabilities to better protect its identities.

This global auto finance company had built up a large and complex IT infrastructure over 30 years. Although it had a PAM system in place, only a few accounts on its legacy applications were managed by it. And some service and admin accounts couldn't be vaulted at all. This state of affairs meant that the company couldn't fully manage its privileged credentials and identities. Nor could it see all its identity risks.

During a routine review of the company's approach to automated risk assessment, the IT security team saw that it didn't have a way to manage its identity risks. So it chose Proofpoint Spotlight to close this security gap. Soon, Proofpoint was integrated with the company's Active Directory (AD) infrastructure and endpoints—both clients and servers. It then began scanning all its endpoints, its PAM system and other identity repositories for vulnerabilities.

The company's IT security team set up a regular meeting with its IT vulnerability remediation team to review its findings. Both teams decided it was best to work together to make changes to reduce identity risks. Over time, they also tracked the impact of these changes.

After using Proofpoint Spotlight for more than a year, the teams reported that their results were impressive. While several critical new issues still popped up each week, they had new processes to resolve them quickly.

> "[Proofpoint Spotlight] has opened up new insights. Without it, we knew we should look into these identity risks, but we just didn't have a way to do it."
>
> –Assistant Vice President, IT vulnerabilities for auto finance company

Key takeaways

It takes only a single identity vulnerability to bring your entire environment down. You need tools that can shine a light on your identity vulnerabilities so that you can see the risk and work to reduce it over time. That way, you can lock thousands of identity doors before attackers even try them.

Identity risks are often introduced because AD and identity systems are complex, and they are constantly changing.

When a person causes an identity to be compromised, it's usually not out of malice. Rather, it's likely that they just made a mistake or were in a hurry.

USE CASE 2:

"Win" Red Team Exercises

Even when defenses fail, the real winners of red team exercises are the companies that use them to boost their security posture. Nevertheless, when an exercise exposes unmanaged or misconfigured identities in your environment, it isn't a great feeling. But don't feel too bad—it happens to almost everyone. A staggering 95% of red teams find exposed domain admin credentials during their exercises.[2]

2. Illusive research.

Summary

A retail bank's SOC team uses Proofpoint to stop several attempts by a red team to log into its critical accounts and breach its servers.

Customer profile

Industry: Finance

Employees: 1,000

Location: EMEA

Solution

Product: Proofpoint Identity Protection

Component: Proofpoint Shadow

How Proofpoint helps

Proofpoint Identity Protection can help you detect attacks in the middle of the attack chain and stop a red team from succeeding without being detected.

- **Proofpoint Shadow** creates a rich maze of false data and fake routes through the network to seemingly sensitive assets and then spreads them across your enterprise. Even the most advanced red teams can't tell what's real and what's fake. And the only way for them to tell is to try using what they have discovered—and tipping off security teams to their presence. This web of deception makes it nearly impossible for them to move toward critical IT assets without being detected.
- **Proofpoint Spotlight** can help you see all the unmanaged, misconfigured and exposed identities in your environment. This gives you a chance to fix them before the red team—and threat actors—have a chance to exploit them.

Proofpoint in action

A major retail bank blocks two red-team attacks to come out on top.

A large retail and investment bank had multiple layers of security controls, as well as several tools for stopping malware on endpoints. But with the rising number of advanced persistent threats (APTs), it wanted to add new detection capabilities. So it installed Proofpoint Shadow. Soon after, the bank hired a well-known penetration-testing firm to attack its network. The twist: it didn't give the firm any warning that it would be using Proofpoint to thwart its advances.

Before the pen test began, Proofpoint Shadow put fake data that would be attractive to attackers on every endpoint within the bank's 5,000-node network. All of the data was customized to look like it belonged in a banking environment, including fake user credentials.

On Day 1 of the test, Proofpoint Shadow detected attempts at malicious activity on one of the bank's Citrix servers by a fake user ("User A"). In response, it collected details about the who, what, when and where of the attack and alerted the SOC and incident response teams.

When the teams investigated, they found out that the pen testers had installed malicious tools on the bank's network and were trying to use additional fake accounts—which they'd harvested after the initial compromise—to progress their attack. The pen testers had no idea that they had already tipped off the defenders.

Then, on Day 22, Proofpoint Shadow sent another alert in response to malicious activity by User A, only this time the activity was on a different server. When the SOC team did a second forensic analysis, it discovered aggressive attempts to log into critical accounts via that server. The attacker had unwittingly tripped the alert by using two different sets of fake user credentials.

Key takeaways

If your SOC team can win red team exercises, it's more likely that it'll be able to stop real cybercriminals when they target your environment.

Early detection of suspicious behavior enables SOC and infosec teams to stop attackers before they can move laterally and reach a company's critical IT assets. Critically, these detections also include valuable data so that teams can forensically analyze attacks. This helps with the response and mitigation.

Detecting a password-cracking attempt on a fake account ensures a highly reliable alert—a 100% true positive of malicious activity in the network.

USE CASE 3:

Secure Hybrid Identities in AD and Entra ID

Active Directory (AD) is a cornerstone of the modern enterprise IT infrastructure. By some estimates, 90% of enterprises use AD as a primary method for user authentication and authorization. And, as more enterprises move to the cloud, Microsoft Entra ID (formerly Azure AD) is becoming just as ubiquitous.

While these tools are popular, they are also notoriously difficult to manage and maintain. A big reason why: they touch almost every place, person and device on the network. Just like with IAM tools, these efforts can never be complete because permissions, users and organizations never stop changing. What's more, not every identity is covered. Take cached credentials on endpoints as an example. AD and Entra ID don't manage them—no IAM system does, either. They are just out there in the wild.

Summary

A bank holding company uses Proofpoint to assess the security posture of a new acquisition and uncovers 3,000 domain admins on its workstations.

Customer profile

Industry: Finance

Employees: 25,000

Location: U.S.

Solution

Product: Proofpoint Identity Protection

Component: Proofpoint Spotlight

How Proofpoint helps

Proofpoint Spotlight scans AD, Entra ID and multiple other identity repositories and finds the accounts that have privileges that they shouldn't. Plus, it finds unmanaged identities on endpoints, as well as privileged identities that aren't being managed in the PAM and other IAM systems. This way, you can remediate them before they fall into the wrong hands.

It also delivers bottom-up and top-down views into the risks that are related to all your unmanaged, misconfigured and exposed identities. This enables security teams to see the attack paths that cybercriminals could use to deploy ransomware and steal data.

Proofpoint in action

A holding company assesses a new acquisition's identity risk to complete M&A safely.

With about $200 billion in assets and 1,000 branches, this regional bank holding company acquires a new bank about every three years. For each merger and acquisition (M&A), its IT team combines systems, software, data and processes. But before this happens, the holding company must assess the purchased bank's security. In this case, the team had less than four months to complete its assessment.

Identity security underpins a bank's entire security posture. The bank's IT team knew that if it could see the new acquisition's identity vulnerabilities, it could get a good idea of what it was dealing with.

For the past six months, the team had been using Proofpoint Identity Protection to scan its own workstations and identity repositories, which meant that it was familiar with its valuable insights. So it decided to use Proofpoint Spotlight for its initial assessment of the acquired bank.

> "I'm glad we used [Proofpoint Spotlight]; everyone saw the value. It's a playbook we'll carry forward through the next M&A."
>
> –Director of Cybersecurity Engineering

After Proofpoint scanned the new acquisition's IT environment, it produced a risk scorecard that detailed several identity risk areas. And one quickly jumped out—there were a whopping 3,000 domain admin accounts live on its workstations. If just one of them were compromised by an attacker, the team would lose control of the whole environment.

Seeing the state of the new bank's security hygiene, executives agreed that there was enough risk to keep the two IT environments separate, at least initially. Without Proofpoint, it would have been a lot harder to justify the increased protection that the IT team believed was warranted.

Key takeaways

Often, identity risks result from ordinary business and IT processes that have been in place over many years. This makes them difficult to see and thus easy to overlook. This is especially true for newly acquired environments in the wake of a merger or acquisition.

It's critical to constantly scan AD, Entra ID, endpoints and other repositories for identity vulnerabilities. An attacker only needs to compromise one workstation with one resident to gain control of an entire environment.

Conclusion

Most companies regularly scan for vulnerable software and applications, but they often don't scan for vulnerable identities. Yet identities are immeasurably valuable. In fact, in many ways, they are companies' most valuable assets because they touch all other digital resources.

Protecting them couldn't be more important. Today's cybercriminals have access to a wide variety of tools that make exploiting credentials fast, easy and effective. Worse, it's difficult for companies to detect their use.

To break the attack chain, you need to protect your identities like you protect every other valuable asset. This starts by taking proactive measures. And that means cleaning up your vulnerable identities before attackers discover them and using deceptions to catch attackers before they can do real damage.

To learn more about how Proofpoint can help you protect your identities, visit: https://www.proofpoint.com/us/products/identity-protection

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0513-002-01-01 4/24