GUIDE

proofpoint.

PROTECTING THE END USER

A PEOPLE-CENTRIC APPROACH TO MANAGING VULNERABILITY, ATTACKS AND PRIVILEGE

proofpoint.com

TODAY'S ATTACKS TARGET PEOPLE, NOT INFRASTRUCTURE.

Organisations are spending more than ever on cybersecurity and getting less value from it. Attacks keep getting through. Sensitive information keeps falling into the wrong hands. And data breaches keep making headlines.

It's time for a fundamental rethink. Traditional cybersecurity models were built for an earlier era—when the prevailing security model was to lock down the perimeter and deal with threats after they got through. The approach barely worked then; it's hopelessly broken now.

That's because people, not technology, are attackers' biggest target—and your biggest risk. This change in the threat landscape requires a fresh mindset and new strategy, one that focuses on protecting people rather than the old perimeter.

But what does this new approach look like in practice? This guide explores that question by outlining the foundational elements of security in the modern era.

It describes the factors that play into end-user risk. It explains how to mitigate these factors. And it recommends concrete steps you can take to build a people-centric defence.

WHY PROTECTION STARTS WITH PEOPLE

It's clear that the usual defend-the-perimeter model of cybersecurity isn't working—and hasn't worked for years. More than two thirds of IT security professionals polled in a recent Ponemon study expect cyber attacks to "seriously diminish their organisation's shareholder value." And more than believe their cybersecurity posture is leveling off or even declining.[1]

Blame two converging trends: the perimeter is dissolving, and attackers are shifting their focus away from technology and towards people.

And the walls came tumbling down

There's a simple reason perimeter defences aren't working. In today's cloud-enabled mobile economy, there's no longer a perimeter to defend. Work takes place on devices organisations don't support, on infrastructure they don't manage, and in channels they don't own.

As Gartner puts it, the IT department "simply does not control the bounds of an organisation's information and technology in the way it used to."[2]

People always make the best exploits

As business shifts to the cloud, so have attackers. Cloud infrastructure may be highly secure, but the people who use them are often vulnerable.

That's why today's attacks exploit human nature rather than technical vulnerabilities. More than 99% of today's cyber attacks are human-activated.[3] These attacks rely on a person at the other end to open a weaponised document, click on an unsafe link, type their credentials, or even carry out the attacker's commands directly (such as wiring money or sending sensitive files).

Credential phishing, which tricks users into entering their account credentials into a fake login form, is one of the most dangerous examples. In the cloud era, those credentials are the keys to everything—email, sensitive data, private appointments and trusted relationships.

In the third quarter of 2018, for example, corporate credential phishing attempts quadrupled vs. the year-ago quarter.[4] And email fraud rose 77% over the same timeframe.[5]

ART OF THE STEAL

Cloud account compromise nets millions for attackers—no malware needed

The following is a real-life account of a company we worked with in the wake of an email fraud attack. Some details have been omitted for privacy.

Last year, a CEO was stuck in an intense meeting, carefully negotiating a deal with a key business partner. Hundreds of miles away, cyber attackers with control of his Office 365 account were working on their own, sneakier transaction.

Exploiting the meeting's sensitive nature—and the trust of the executive's direct reports—they stole millions through fraudulent wire transfers. Their only tools: email, patience and a little social engineering.

The attackers had taken control of the CEO's account months earlier after guessing his password in a brute-force attack. (In this kind of attack, cyber criminals systematically try hundreds or even thousands of passwords until one works.)

Undetected, the attackers set up an email forwarding rule. This move gave them free-ranging access into the company's most sensitive business. They knew the partner meeting was coming, what it was about, and that the CEO would be unreachable by phone or in person.

As the meeting wore on, a senior finance person received an urgent email from the CEO's account. The CEO was busy negotiating a deal, it stated. To close the transaction, he needed a large wire transfer, and quickly. The finance person complied, unable to check with the CEO directly.

But the email wasn't from the CEO. The account information wasn't the business partner's. And the normal fiscal controls weren't applied. The attackers had looted millions of dollars—all without a single malware infection, phishing email or technology exploit.

[1] Ponemon Institute. "2018 Study on Global Megatrends in Cybersecurity." February 2018.
[2] Rob van der Meulen (Gartner). "Build Adaptive Security Architecture Into Your Organisation." June 2017.
[3] Proofpoint. "The Human Factor 2017." December 2016.
[4] Proofpoint. "Quarterly Threat Report Q3 2018." December 2018.
[5] Ibid.

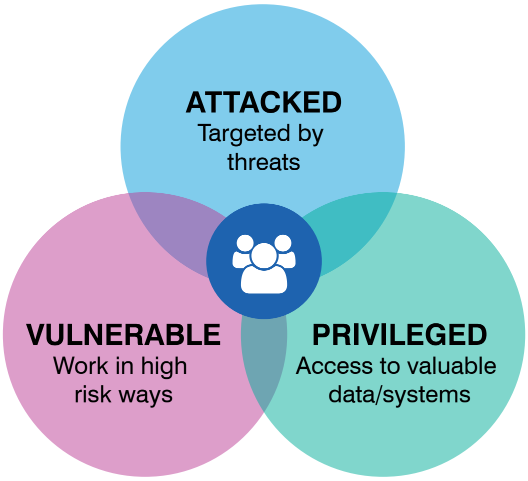
ASSESSING USER RISK: THE VAP MODEL

Just as people are unique, so is their value to cyber attackers and risk to employers. They have distinct digital habits and weak spots. They're targeted by attackers in diverse ways and with varying intensity. And they have unique professional contacts and privileged access to data on the network and in the cloud.

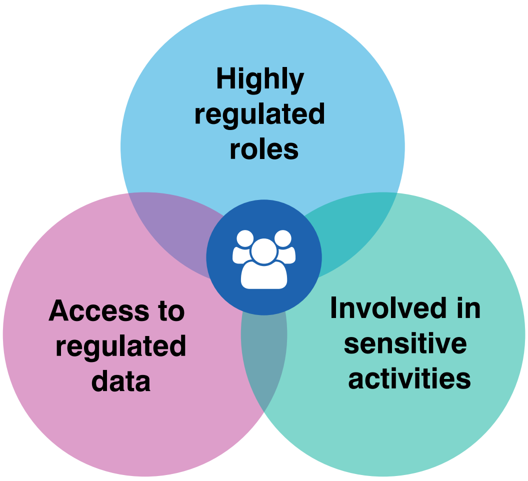
Together, these factors make up a user's overall risk in what we call the VAP (vulnerability, attacks and privilege) index.

Understanding People-Centric Risk

SECURITY



COMPLIANCE



Vulnerability

Users' vulnerability starts with their digital behavior—how they work and what they click. Some employees may work remotely or access company email through their personal devices. They may use cloud-based file storage and install third-party add-ons to their cloud apps. Or they may be especially receptive to attackers' email phishing tactics.

How your people work

Assessing vulnerability that stems from how people work is mostly straightforward—though it's not always easy, or even possible, with traditional cyber defences. It starts with knowing what tools, platforms and apps they use.

The more granular your visibility, the better. Gauging vulnerability on the user level, for instance, is feasible only when you have accurate user-level visibility. When you do, you can weigh factors such as:

- What cloud apps they use
- How many and what devices they use to access email
- Whether those devices are secure
- Whether the user practices good digital hygiene
- Whether they use multifactor authentication consistently

What your people click

The second part of measuring vulnerability is figuring out how susceptible your users are to phishing and other cyber attacks. Short of letting attackers in and seeing who opens a malware file or wires money to an attacker (not ideal for obvious reasons), phishing simulations are the best way to gauge this aspect of vulnerability.

Simulated attacks, especially those that mimic real-world techniques, can help identify who's susceptible and to which tactics.

Someone who opens a simulated phishing email and opens the attachment might be the most vulnerable. A user who ignores it would rank somewhat lower. And users who report the email to the security team or email administrator would be deemed the least vulnerable.

Attacks

All cyber attacks are not created equal. While every one is potentially harmful, some are more dangerous, targeted or sophisticated than others.

Indiscriminate "commodity" threats might be more numerous than other kinds of threats. But they're usually less worrisome because they're well understood and more easily blocked. Other threats might appear in only a handful of attacks. But they can pose a more serious danger because of their sophistication or the people they target.

VAP SNAPSHOTS

🟥 HIGH 🟧 MEDUIM 🟩 LOW

Here’s how the VAP model might apply to workers in a typical organisation.

Jane Barker, CEO

jbbarker@your.co

🟧 Vulnerability

No ThreatSim action, uses outside networks and devices, inconsistent use of multifactor authentication

🟥 Attack

Top 10% of all users in MaxThreat score, with 30-day total in the top 5%

🟥 Privilege

Has access to sensitive data in Office 365 and corporate network

Jane scores well on phishing simulations. But she is also highly mobile, logging into email and file shares from several devices on- and off-network. Her high-profile status makes her a target of malware and phishing attacks, many of them advanced and highly targeted. She has access to highly sensitive data. And she wields authority over many high-level employees, including people who can make wire transfers.

Maggie Brown, EA

mbrown@your.co

🟧 Vulnerability

Poor ThreatSim score, uses company-issued equipment on network

🟧 Attack

Mostly commodity threats, but some are socially engineered and targeted

🟥 Privilege

Has little access to sensitive data but can email for the CEO and has access to calendars

Maggie works solely on the corporate network during work hours using her company-issued PC. But she occasionally opens emails in phishing simulations. And given her role, she may be susceptible to email fraud that spoofs the CEO or other executives. Along with a large volume of commodity email threats, she receives some socially engineered and targeted email. While she doesn’t have access to sensitive information, she can send emails on behalf of the CEO and has access to executive calendars.

Ed Jeong, Engineer

ejeong@your.co

🟩 Vulnerability

Perfect ThreatSim score, uses outside networks and devices, inconsistent use of multifactor authentication

🟥 Attack

Top 1% of all users in MaxThreat score, with 30-day total in the top 3%

🟥 Privilege

Has access to highly valuable data sensitive data

Ed has excellent digital hygiene practices; he doesn’t fall for simulated phishing attacks, promptly reports suspicious messages and accesses company resources only when on a VPN. But he is targeted in a larger-than-average number of attempted attacks, many of them highly sophisticated. While his network and file access is limited to his own department, many of these files have highly valuable IP.

Rich threat intelligence and timely insight are the keys to quantifying this aspect of user risk. The factors that should weigh most heavily in each users' assessment include:

- The cyber criminal's sophistication
- The spread and focus of attacks
- The attack type
- Overall attack volume

You should also weigh these factors in context of what departments, groups or divisions the individual user belongs to. For instance, some users might seem not at risk based on the volume or type of malicious email sent to them directly. But they may actually represent a higher risk because they work in a highly attacked department—and are therefore more likely to be a key target in the future.

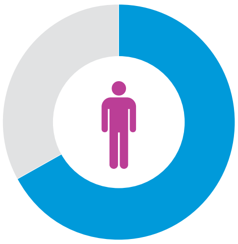
Privilege

Privilege measures all the potentially valuable things people have access to, such as data, financial authority, key relationships and more. Measuring this aspect of risk is crucial because it reflects the potential payoff for attackers—and harm to organisations if compromised.

Users with access to critical systems or proprietary intellectual property, for instance, might need extra protection, even if they aren't especially vulnerable or aren't yet on attackers' radars.

The user's position in the org chart is naturally a factor in scoring privilege. But it's not the only factor—and often, not even the most important one. For attackers, a valuable target can be anyone who serves as a means to their end.

According to our research, individual contributors and lower-level managers account for



67%

of highly targeted malware and phishing attacks

Attacks against executives and upper-level managers

rose 4 points to about a third of all attacks.[6]

MITIGATING END-USER RISKS: A BLUEPRINT FOR PEOPLE-CENTRIC PROTECTION

Protecting against all the factors that play into user risk requires a multipronged approach. In the VAP model, that means:

- Reducing users' vulnerability
- Stopping the threats that target them
- Managing their privilege to safeguard the valuable things they have access to

Reducing vulnerability

The first step to making users more resistant to cyber threats is making them more aware of the risk. That's why cybersecurity awareness training is the foundation of making users less vulnerable.

The most effective training programs are engaging and hands-on. They're based on active, real-world attack techniques. And given that attackers are always evolving their methods, they're current and updated regularly.

Security awareness education cannot be a once-a-year chore endured in the confines of a training room. Like any aspect of long-term behavior change, it's a continuous process. Effective training programs:

- Assess users' knowledge
- Educate them on current threats
- Reinforce those lessons with frequent reminders
- Measure changes in behavior over time

Especially vulnerable users may require follow-up instruction. Highlighting and correcting mistakes in real time is critical. Users who fall for phishing emails (real or simulated), for instance, should learn what they should have looked for before clicking—while the incident is still fresh. Follow-up lessons should be tailored and relevant to each user.

The most resilient users not only recognise threats that come their way, but also report them. The sooner a threat is reported, the sooner security teams can move to block it at the gateway and, if it has already been delivered, pull it from users' inboxes. Streamlining the reporting process strengthens your defences across the environment.

Stopping attacks

Today's cyber attacks are unrelenting, come in many forms, and are always changing. Even with the best training, some users will click on some threats some of the time.

[6] Proofpoint. "Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks." November 2018.

Protecting users means stopping not just some types of attacks but the whole spectrum of threats—ideally, before they reach the inbox.

Malware threats

Most organisations understand the dangers of malware. What they may not appreciate is how it actually enters their environment and the role that people play in putting it in motion.

Consider the typical security budget.

+80% of spending goes toward traditional infrastructure-focused defences

even though most cyber attacks today target people, usually through email.[7]

And whether it's a banking Trojan, credential stealer, ransomware, or remote-access Trojans (RATs), most malware requires the victim to act.

Non-malware threats

Traditional security deals with malware-based threats (though far too often only after they have entered the environment). But many of today's most serious threats don't involve malware at all. Instead of hacking technical vulnerabilities, they exploit human nature.

Examples of non-malware threats include:

- Phishing
- Credential theft
- Email fraud (also known as business email compromise, or BEC)
- Cloud account compromise

Because these threats use social engineering rather than malicious payloads, they can be harder to detect and block with infrastructure-focused defences.

Web-based threats

The web, including web-based social media tools, is one of the biggest sources of threats. Most people check personal email and use the internet for personal browsing during the workday. Much of this activity is uncontrolled and potentially dangerous.

Securing the vast reaches of the internet without impeding actual work is difficult, if not impossible. Trying to inspect users' personal activity—especially as more of it is encrypted by default—is costly, slows network performance, and won't catch all threats. It also creates potential privacy and security issues. Short of blocking personal web use altogether—an extreme approach that would upset most users—securing this gaping security hole is a challenge.

A far simpler approach: isolating personal web activity so that it never touches your environment to begin with. Using web isolation technology, users can browse the internet freely without exposing the corporate network to threats. They can also check their personal email without introducing new risks or giving up their privacy.

Managing privilege

To do their job, many users must access sensitive data and other resources. Managing privilege isn't about broadly denying access or making work cumbersome for authorised users. Instead, the goal is better controlling access to help mitigate the effects of account compromise and unapproved access to sensitive data.

Fine-tuning access is the first step to managing privilege. Front-line retail workers shouldn't have access to files created by the finance department. A healthcare CEO probably doesn't need to download patient records. By making sure the right people—and only those people—get what they need, you can limit exposure if those users are compromised.

Mitigating privilege-related risks also involves knowing when a privileged account may have been compromised. Unusual logins or activity should trigger stepped-up authentication measures or quickly cut off access. Attackers who take over a privileged account have free rein over any sensitive data the real account owner has access to. And anyone who gains control of an email account can exploit people who trust it—inside and outside of the organisation.

At the same time, apps and third-party add-ons installed by users on their own may have access to sensitive data. They should be routinely audited to ensure that they're safe. Even apps that aren't overtly malicious may be poorly designed or have vague security and privacy policies, making them too risky to have privileged access.

NEXT STEPS: BUILDING A PEOPLE-CENTRIC DEFENCE

In today's cloud-enabled, mobile, digitally transformed workplace, protection starts with people. That's why you need a solution that addresses all aspects of end-user risk outlined in the VAP model. That means:

- Reducing users' vulnerability
- Preventing, defending against, and responding to attacks that target them
- Monitoring and managing their network privilege to prevent unsanctioned access to sensitive information

At Proofpoint, we have always advocated a people-centric approach to advanced threats and compliance risk. Our solutions focus on protecting end users, the data they create and the digital channels they rely on every day.

[7] Gartner. "2017 Security Spending Forecast." August 2017.

To learn more about how we use the VAP model to protect people across email, the web, cloud apps, the web, social media and more, visit **proofpoint.com/us/solutions/protecting-end-users**

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT) is a leading cybersecurity company that protects organisations' 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 organisations of all sizes, including more than half of the Fortune 100, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint.