proofpoint

The Value of Integrated Mobile, Social and Email Threat Defense

Criminals, hackers and hostile governments are targeting companies, their employees and individuals across all types of cyber vectors. The motivations are the same across all types of attack surface: to steal data, to steal identities, to make money, to perform espionage and to disrupt communications and systems. Attackers are increasingly attacking companies by attacking their employees. Many vectors are used and combined into sophisticated attacks. Evidence shows that attacks are often related, and that indicators of compromise are often the same between the different ways that companies are being attacked.

This whitepaper will answer these questions:

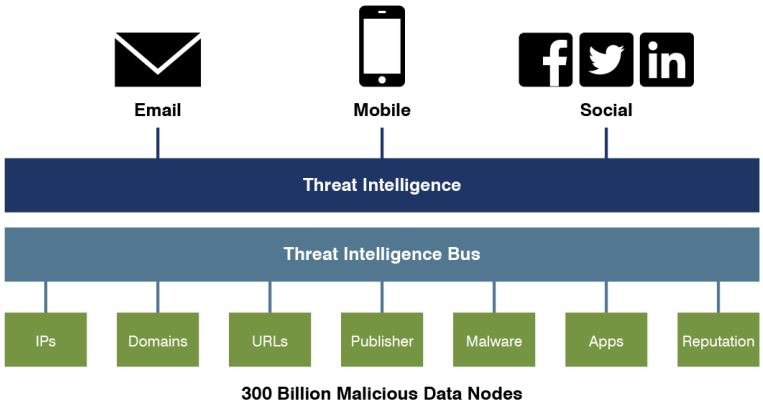
- How & why mobile, social and email threat vectors relate to each other from a security perspective
- How Proofpoint leverages intelligence gathering behind the scenes to protect customers on the front lines
- How each standalone Proofpoint solution (Mobile, Social, Email) protects against its namesake threat vector
- What is Proofpoint's big picture strategy for integrated Mobile, Social, and Email threat protection
- Why is an integrated solution better than standalone point solutions

Proofpoint Threat Intelligence

Proofpoint gathers threat intelligences across email, malware, mobile apps and social media to create a large database that is used to identify attacks in all of these diverse vectors. This database has over 300 Billion threat indicators and grows every day.

Proofpoint gathers information about attacks that include:

- URLs
- IP addresses
- domain names
- Mobile app identifiers
- Email addresses
- Malware across computers, mobile devices and servers
- Compromised social media accounts
- Contact information about malicious actors
- App publisher information and reputation



At Proofpoint, we are constantly gathering intelligence behind the scenes to protect customers on the front lines. When we detect an IP address that is used as a command-and-control server for malware that is delivered by an email attachment, we can scan millions of apps to see if that IP address is also being used to control malicious behavior inside of mobile apps. If we find fake social media accounts being used to trick customers into divulging account information and personal data, we can also scan emails and mobile apps to see if the company's brand name and assets are being used in connected attacks.

Email Threat Intelligence

Proofpoint processes email for many of the world's largest companies and ISPs. Seeing billions of emails a week, allows Proofpoint to have unprecedented visibility into attacks as they emerge. Proofpoint defends against malicious senders, malicious URLs and malicious email attachments. This data is entered into the threat database, so that if these URLs, addresses or other indicators are found inside mobile apps or in blog or twitter postings related to a company, these are immediately used to protect customers on those other threat vectors.

Proofpoint Targeted Attack Protection actually detonates URLs and attachments in sandboxed environments, seeing if they contain malicious behavior, and protecting users in realtime.

Mobile App Threat Intelligence

Similarly, Proofpoint Mobile Defense runs mobile apps in sandboxed environment, seeing if they exhibit malicious behavior, if the apps mine corporate or personal data, or connect to malicious or risky locations on the Internet.

Proofpoint analyzed millions of apps per year on iOS and Android, finding malicious and highly risky apps and app publishers. When command-and-control servers are discovered in these apps, that information is shared with the threat database, which alerts email sensors to look for those same malicious servers by URL, domain or IP address. Proofpoint is protecting not only against malicious and risky apps on user devices, but also proactively scans the Internet to analyze apps before they can compromise your employees.

Social Media Threat Intelligence

Proofpoint also scans the Internet's social media channels to find attacks against companies, their employees and customers. Proofpoint detects fake social media accounts that attackers use to trick people into divulging usernames, passwords and other personal information. This approach proactively protects a company's brand, and detects targeted attacks against a company. By combining this protection with proactive scanning for apps that also impersonate a company or steal it's brand in order to get people to download malicious or dangerous apps, Proofpoint gives the broadest protection.

The Power of Integrated Threat Intelligence

By providing an integrated fabric of threat intelligence between email, mobile and social threat vectors, Proofpoint brings to bear the most powerful database in the industry to protect customers across all these ways that attackers are targeting their employees and customers.

Standalone solutions cannot fully protect employees as attacks occur, because they do not see the relationships between varied attacks that today's threat actors use.

Proofpoint is continuing to increase our threat intelligence gathering, sharing and utilization between our products and protection services. Contact us to learn more.

about proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

proofpoint™

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com