BLINDSIDED

Why Today's Biggest Cybersecurity Threats May Be the Ones You're Not Seeing

The visibility gap has become one of cybersecurity's most acute and fastest-growing problems. Even as organizations spend upwards of

$100 BILLION PER YEAR

on the latest tools, cyber attackers keep getting through.

The way we work is changing

Today's business transcends the bounds of traditional network perimeters and connected endpoints. It transpires over email. It flows through social networks. It plays out across all types of mobile devices.

Steve Morgan (Forbes). "Worldwide Cybersecurity Spending Increasing to $170 Billion by 2020." March 2016.

THREATS TARGET PEOPLE OUTSIDE THE NETWORK

More than one in every five clicks to a malicious URL in email takes place **off the corporate network** through email, social networks, or on mobile devices.

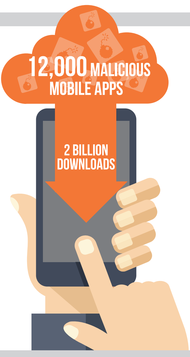
Proofpoint. "The Human Factor 2016." February 2016.

40% of Facebook accounts and 20% of Twitter accounts related to Fortune 100 brands are fake.

These accounts are designed to steal customer data, damage the brand, manipulate markets, and commit fraud.

Proofpoint. "The State of Social Media Infrastructure." 2014.

More than 12,000 malicious mobile apps are available from authorized Android app stores—capable of stealing information, creating backdoors, and other functions—accounting for more than **2 billion downloads.**

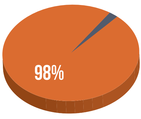


Proofpoint. "The Human Factor 2016." February 2016.

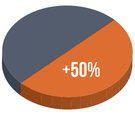
THE COST OF NETWORK MYOPIA

This lack of visibility increases your risk, makes security incidents more difficult to resolve, and leads to more costly cleanups.

More attacks get through



A whopping 98% of organizations didn't discover they were breached until a week after the fact.



And more than half aren't confident they found the root cause.

"The Post Breach Boom." February 2013.

Attacks take longer to detect

Delayed detection means the attacker has more time to spread laterally across your environment, steal more data, and cause more damage.

AVERAGE TIME TO DETECT:

Financial Firms **98 Days**

Retail Firms **197 Days**

Ponemon Institute. "Advanced Threats in Financial Services: A Study of North America and EMEA." May 2015.

Cleaning up and remediating a cyber attack takes an average of

31 DAYS AT A COST OF $20,000 PER DAY

Kelly Jackson Higgins (InformationWeek). "Cost of a Data Breach Jumps By 20%." October 2014.

WHAT YOU CAN DO ABOUT IT

Identify key blind spots. Determine whether your current defense is in the flow email, social media, and mobile devices.

Create a plan to close the gaps. This may include modeling your return on investment and potential impact to your security operation.

Consider solutions to improve visibility. The best tools will not only detect threats beyond the network and tie into your incident response tools.

To learn more about cybersecurity's visibility gap, download our whitepaper

Flying Blind: Why Cybersecurity's Visibility Gap Matters, and How Organizations Can Solve It >

proofpoint.