proofpoint.

CONNECT WITH CONFIDENCE

THREE STEPS TO STOPPING ADVANCED EMAIL THREATS

Your biggest email security challenge isn't any single threat. It's the abundance of them. Ransomware, business email compromise (BEC), credential phishing, and more may be bypassing your security defenses. That puts your brand—and bottom line—at risk.

Ready to fight back? Here are three steps to a complete defense:

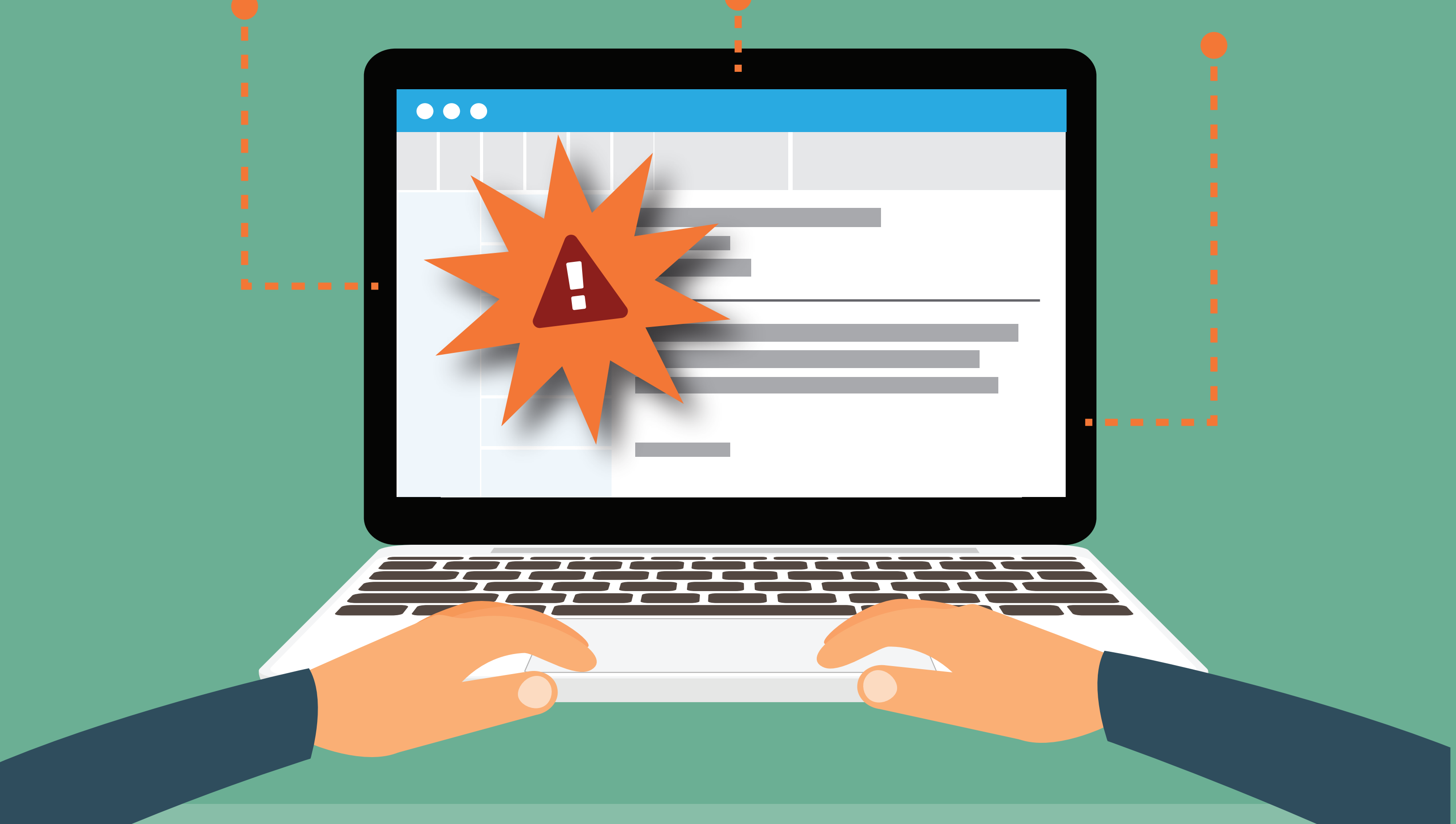
STEP 1: BLOCK MALWARE-FREE ATTACKS

Business email compromise (BEC) and credential phishing are effective because they rarely include malicious URLs or attachments.

45%
increase in BEC attacks in Q4 2016
(Proofpoint)

$3.1B
spent on BEC attacks since 2013
(FBI)

2/3
of BEC attacks spoofed the sending domain of a targeted company
(Proofpoint)



To fight malware-free attacks, ensure your security solution:

- Implements gateway policies to identify and block payload-free threats
- Implements email authentication policies to prevent all domain-spoofing attacks
- Leverages data loss prevention (DLP) technologies to keep sensitive information safe

STEP 2: FIGHT ADVANCED MALWARE-BASED THREATS

Malware-based threats delivered through malicious attachments and URLs continue to thrive, bypassing even "next-generation" defenses.

39%
of organisations were hit with ransomware in 2016
(Osterman Research)

12%
of targeted users click on malicious attachments
(Verizon, 2016 DBIR)

03:45
is the median time users click on malicious attachment
(Verizon, 2016 DBIR)

To fight latest advanced malware attacks, your team must:

- Get end-to-end visibility into every threat targeting your organisation
- Invest in a cloud-based sandboxing solution that adapts to threats as they evolve
- Leverage predictive analytics to identify suspicious payloads

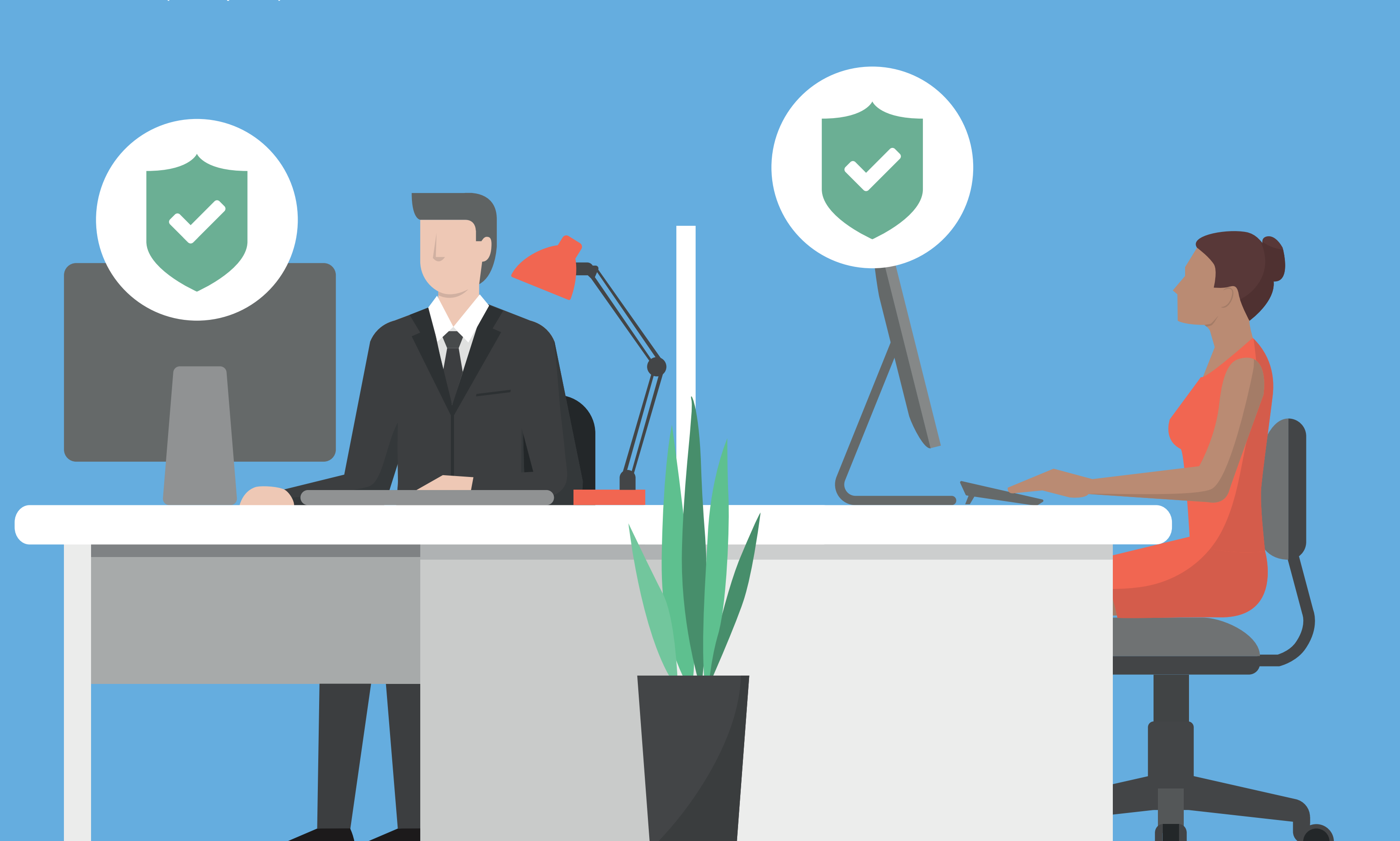
STEP 3: RESPOND TO THREATS

No security solution can stop every attack. Failing to prepare for the inevitable breach can result in disrupted business, costlier cleanups, and more risk.

22%
chance that your company will experience a breach of at least 10,000 records within the next 24 months
(Proofpoint)

31%
of companies have a budget in place for data breach mitigation
(Osterman Research)

75%
of organisations would take hours, days or weeks to detect a breach
(Osterman Research)



A modern threat response solution should empower your team to:

- Automate time-consuming forensics-collection chores
- Contextualise data to understand and prioritise threats
- Remove malicious emails and quarantine infected endpoints

To learn more about how to build an effective email security strategy, watch our webinar,
"How to Build an Advanced Email Security Strategy"