

# 7 KEYS TO CYBERHYGIENE

Despite high-profile breaches, many organizations remain unprepared for a cyberattack.

Learn the 7 keys to “clean” security and how to protect your business.

## DID YOU KNOW?



of businesses **expect a breach in 2019<sup>1</sup>**



of them **may not even know when a breach happens<sup>2</sup>**

### KEY 1: PREPARE FOR THE INEVITABLE

Don't assume that the plan you put in place last year is still relevant. Today's threats require constant vigilance and a solid, ever-evolving security strategy.

### KEY 2: UNIFY YOUR SECURITY APPROACH

A patchwork of DIY security across your network introduces new gaps and vulnerabilities. A unified approach — with security at every level of the network — will minimize gaps.

### KEY 3: PROTECT YOUR NETWORK & DEVICES

Defend your network and endpoints from attack. Protect the perimeter and manage vulnerabilities. Ensure next-gen firewall protection, correct segmentation, deep packet inspection, TLS decryption, and functioning backup processes.

### KEY 4: MONITOR AND TEST SECURITY CONTROLS

Don't let your guard down. Continually test security controls and employ professional 24/7 security monitoring to help distinguish false alerts from true threats.

### KEY 5: CREATE A COMMUNICATIONS PLAN

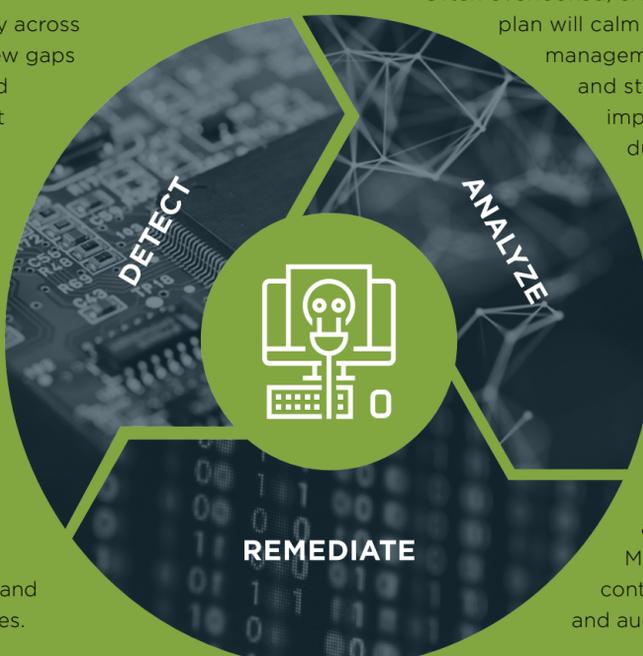
Often overlooked, creating a communications plan will calm nerves and empower management to inform employees and stakeholders swiftly on important actions to take during a breach.

### KEY 6: BETTER MANAGE USERS

Create user security policies and secure-use guidelines for systems and mobile workers. Establish effective management processes and limit user privileges. Monitor user activity and control access to activity and audit logs.

### KEY 7: ASSEMBLE AN INCIDENT RESPONSE TEAM

Bring together an internal Incident Response (IR) team and an external IR partner to detect, analyze, and remediate security incidents.



REMEDIATE

## SUMMARY

Good cyberhygiene requires a secure, unified infrastructure — from perimeter to endpoints — managed professionally for proactive control, visibility, and continually updated security measures.

**READ OUR LATEST SECURITY BLOG SERIES TO LEARN MORE!**

<sup>1</sup> The Ponemon Institute/Trend Micro, press release, "Trend Micro Survey Finds 80 Percent of U.S. Businesses Expect a Critical Breach in 2019," February 12, 2019.

<sup>2</sup> eSecurityPlanet, "74 Percent of Companies that Suffer a Data Breach Don't Know How It Happened," February 17, 2017.