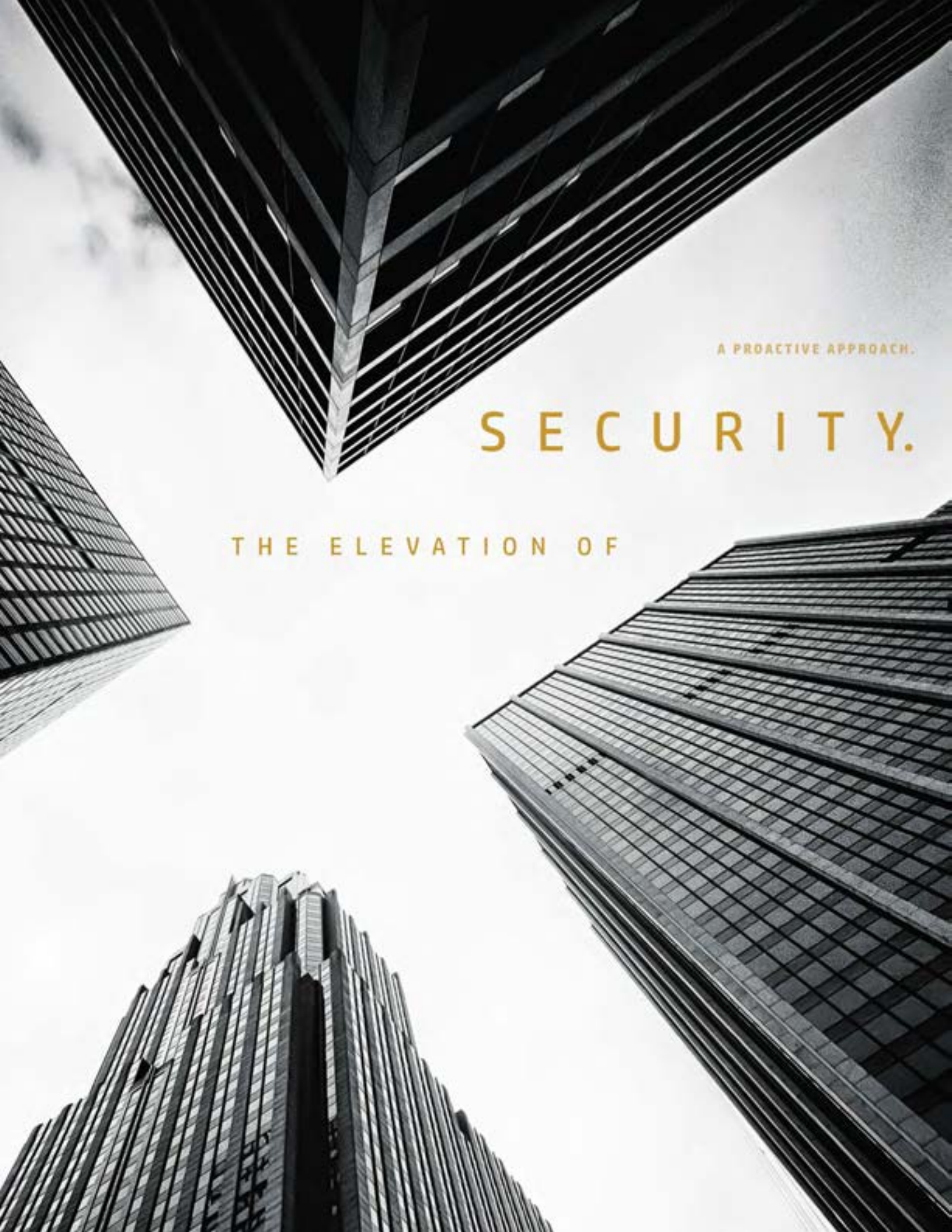
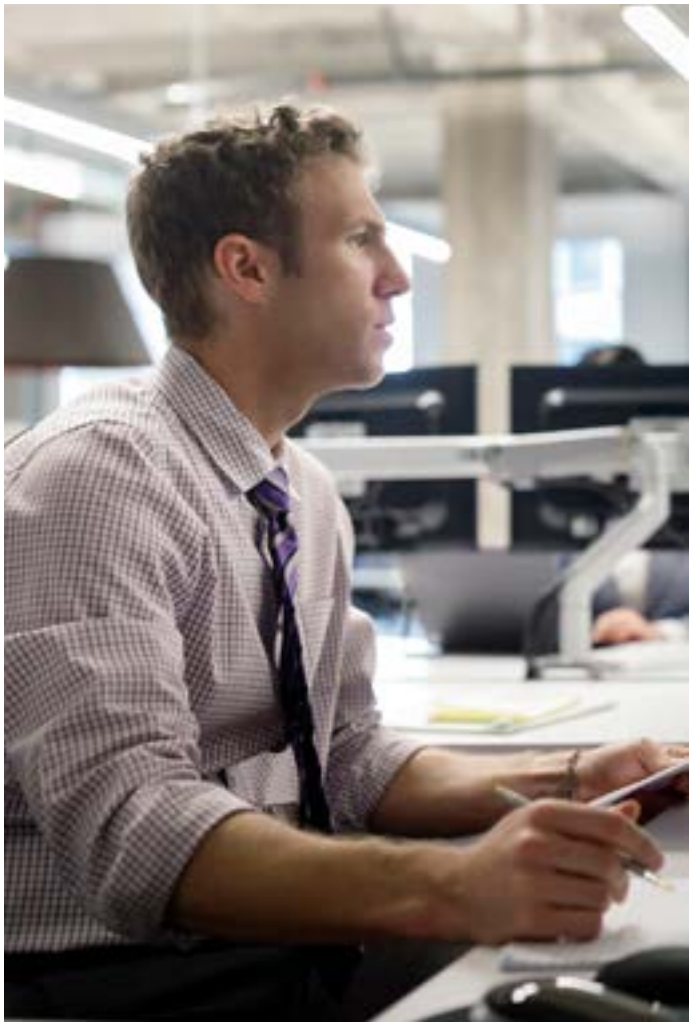

A PROACTIVE APPROACH.
SECURITY.
THE ELEVATION OF

CONTENTS

DATA SECURITY IN A CHANGING WORLD.

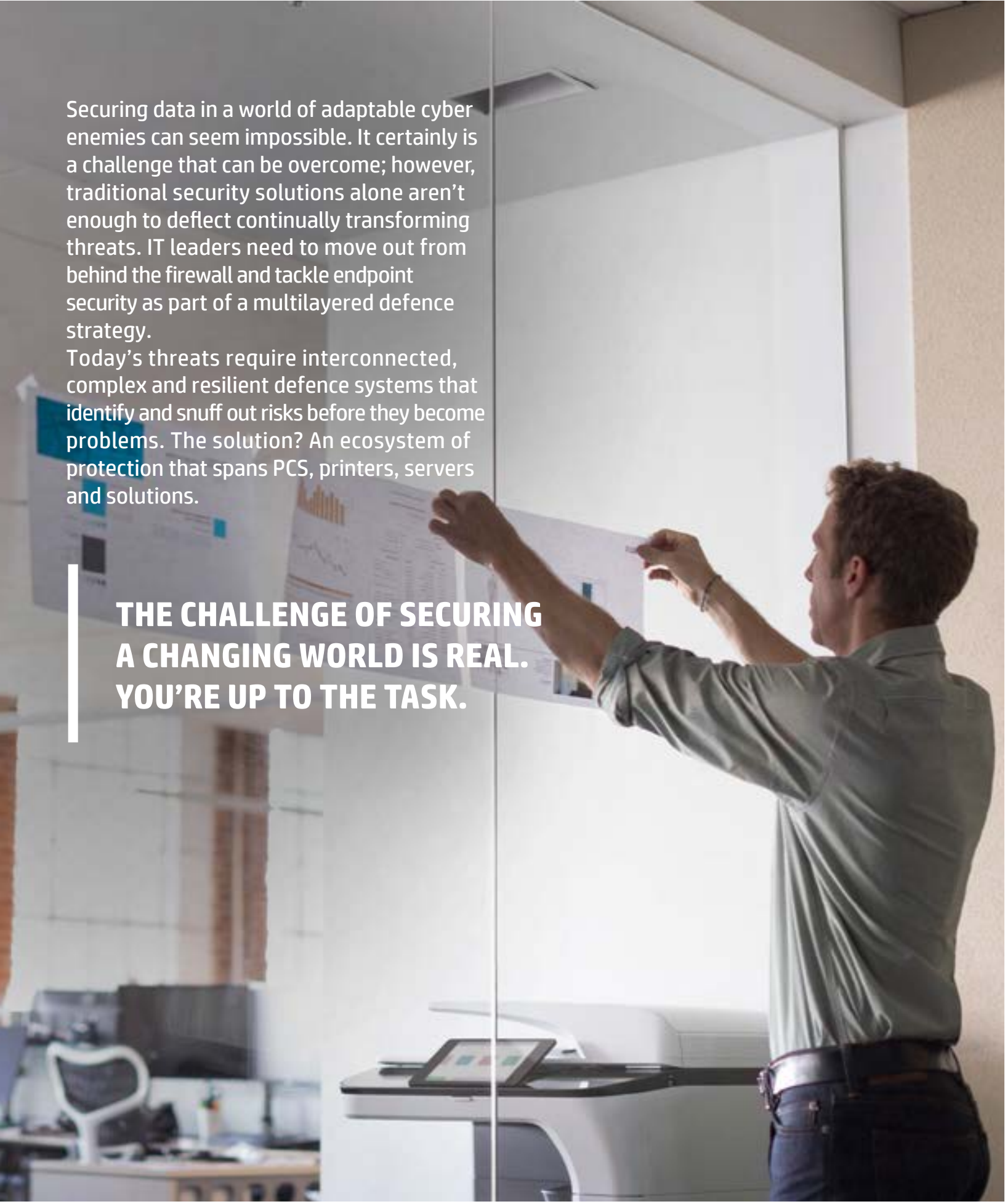
We live in the era of digital disruption, when always-on connectivity, a mobile workforce and globalisation leave us more vulnerable than ever to cybersecurity assaults. In this brave new world, keeping customer and company data safe is a seemingly insurmountable challenge.



The reality is that IT is tasked with not only thwarting known threats but also anticipating the ways in which cybercrime and cyberattacks evolve. For every new security patch, there's a cunning hacker ready to find an undiscovered path to your data.

What's more, daily workloads for IT professionals include hours spent chasing moving targets, with many alerts resulting in false-positive dead ends. This virtually endless barrage of notifications — called "alarm fatigue" — fosters skewed perspectives on cybersecurity issues and a compromised ability to protect the systems and infrastructure that comprise a business's data backbone.

In an age of digital evolution, new security strategies are needed to address internet-connected endpoint devices. It's no longer acceptable to maintain the firewall but ignore endpoint devices such as network printers and simply hope for the best. Every endpoint needs to be locked down.



Securing data in a world of adaptable cyber enemies can seem impossible. It certainly is a challenge that can be overcome; however, traditional security solutions alone aren't enough to deflect continually transforming threats. IT leaders need to move out from behind the firewall and tackle endpoint security as part of a multilayered defence strategy.

Today's threats require interconnected, complex and resilient defence systems that identify and snuff out risks before they become problems. The solution? An ecosystem of protection that spans PCS, printers, servers and solutions.

THE CHALLENGE OF SECURING A CHANGING WORLD IS REAL. YOU'RE UP TO THE TASK.

THE EVER PRESENT THREAT OF A DATA BREACH.

Threats are increasing, but some IT admins are stuck in the security paradox.

What is the security paradox? Put simply, it's the contradictory set of two factors:

1. A company's cybersecurity is current and well-suited to the risks.
2. Some of the company's infrastructure is likely under-secured.

In other words, everything's fine. Until something happens.

These contradicting viewpoints, coupled with the task of providing reliable security against nonstop, evolving threats, is a recipe for the type of inaction that invites hackers to locate and exploit vulnerabilities.

This security paradox is systemic to the current state of IT. Consider that 44 percent of organisations report being victims of

The numbers game

It was a record year for data breaches in 2016. A total of

4,149

breaches were reported, with 4.2 billion records exposed.[2]

cybercrime[1] — that's a much larger mark on organisational health than is commonly understood.

Hackers change strategies to exploit hidden vulnerabilities. Instead of chasing down firewall holes, IT admins can adopt holistic protection that secures network-connected endpoints and delivers layered coverage.

Evaluate endpoint devices with security features that have these capabilities:

- Automate protections and maintain device uptime.
- Minimise IT involvement.
- Enable mobility while adhering to business-grade security standards of authentication, identity protection and data encryption.

The risk of data breach is greater than many believe.

Despite the overwhelming evidence that data breaches can happen to any company in any industry in any country and via any device, there lacks a multilayered approach to security that protects every possible entry point. IT managers know a breach could be just a click away, but the staggering pace at which modern threats evolve often leaves them blind to the real impact outdated security can have on their organisations.

$3.2B

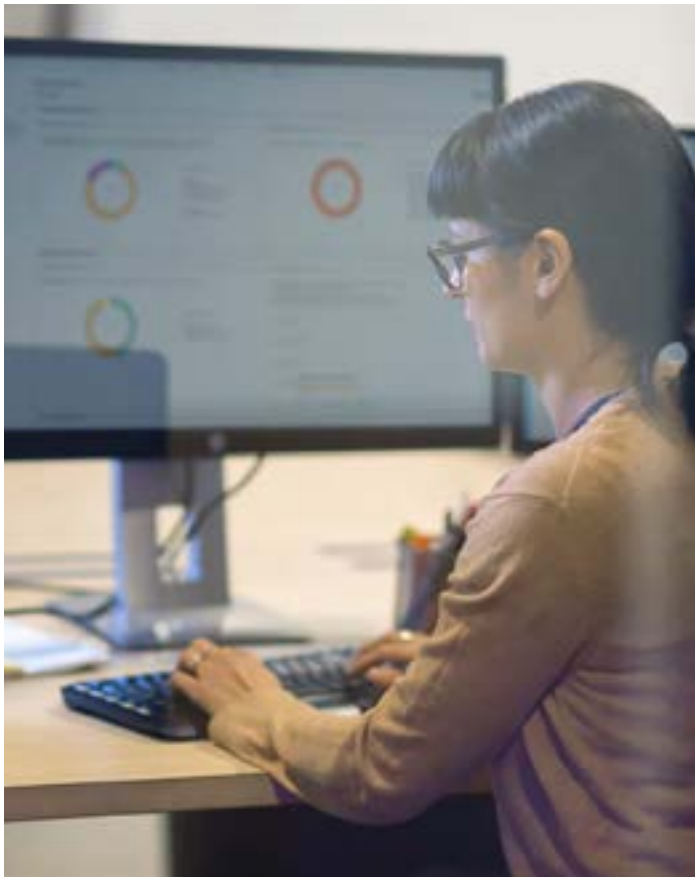
More exposed records than the previous all-time high in 2013.[2]

Formal information governance programs deliver a nearly $1 million reduction in cybercrime costs, but only 28 percent of companies reported having one.[3] Only 16 percent of organisations view printers as being at high risk for a security breach.[4] Print security practices trail those of other endpoints at just 57 percent, compared to desktop/laptops at 97 percent and mobile devices at 77 percent.[4] Only 49 percent of companies use advanced access management systems, and even fewer use extensive encryption.[3]

There's clearly a case to be made for security upgrades; however, many IT managers deem networked endpoints such as printers low risk because, for the most part, they can't be

Your printer is an endpoint!

Like Internet of Things (IoT) devices, printers are often not properly secured and maintained. Read more in the IDC Insight Report.



monitored. They don't anticipate intrusions they can't see: That's the security paradox.

A newer, stronger firewall is continually being developed for the market, and many consider any device behind it "low risk."[5] But today's threats have grown beyond perimeter security and are essentially moving targets that are difficult to neutralise. Layering security solutions provides localised protection across all devices connected to a network — and blocks uninvited connections from crashing the scene.

THE RISK IS GREATER THAN YOU REALISE.

> IT professionals feel real anxiety when it comes to preventing cyberattacks, but an inability to monitor everything, all the time forces them to rely on ad hoc security solutions.

Are you covered?

Beyond an underestimation of the endlessly adapting threat that hackers and cybercrime pose to organisations, there's also a general misunderstanding of the breadth of threats that can exploit inadequate cybersecurity. For example, half of security professionals believe mobile devices and cloud infrastructure present the biggest avenue for cyberattacks.[4] And while securing high-profile attack vectors is an important component of digital security, focusing on them without

addressing inconspicuous entry points, such as printers and applications (80 percent of which are vulnerable to compromise due to simple misconfigurations[6]), is like locking a home's doors but leaving ground-floor windows wide open.

Holistic protection seals up a system's total structure — the doors, windows and foundation cracks most IT admins and security departments wouldn't know exist.

Unprotected printers can provide uninhibited access to queued and cached document files and potential access to the entire network. That means when someone clicks "print" and a document is sent to an unprotected printer, that person is sending potentially sensitive information out into the world for hackers to intercept.

The average cost of a data breach is:

$9.5M[3]

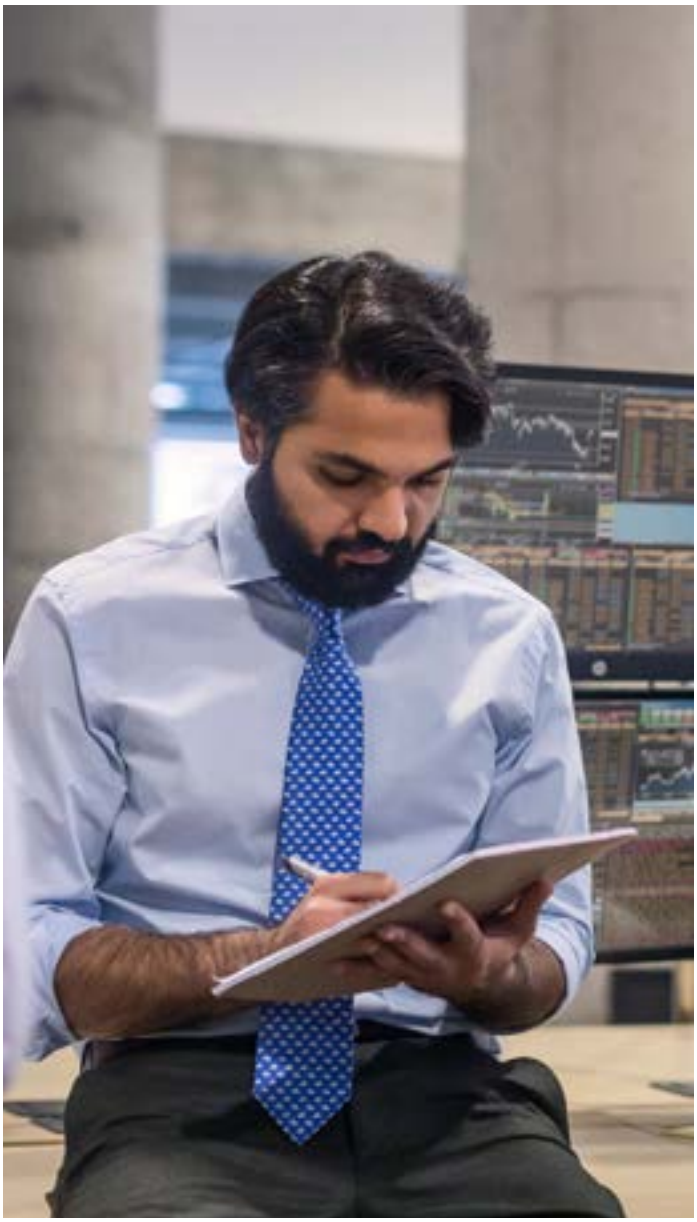
In early 2016, a hacker gained access to printers on college campuses across the country using a readily available search tool from the internet. Then he sent hateful messages through the machines. The hacker located 29,000 internet-connected printers in about a minute, and easily breached selected targets by sending a print job through an unsecured port.

483

PRINTERS HACKED PER SECOND

Dismissing these low-profile entry points as benign and ignoring the dangers of a partially protected network is both paradoxical and problematic — and dangerous to your bottom line.

However, when hardware and software solutions come with built-in, integrated security, an additional, dynamic layer of security helps cover everything from smartphones to backroom printers.



SECURITY IN THE DECENTRALISED WORKPLACE.

Today's workforce is in a state of flux. Work habits considered standard just a few years ago are growing outdated, with emerging trends — including cloud-enabled anytime / anywhere work schedules — disrupting traditional practices.

80%

Of today's workforce prefers benefits and perks such as mobile devices and nontraditional working environments to standard pay raise.[8]

It's an exciting time to be an employee — and a challenging time for IT professionals, with a decentralised workplace presenting never-ending opportunities for hackers to gain access to sensitive information. Waiting for things to get "back to normal" isn't an option, as these workplace changes are here to stay.

Millennials became the largest segment of the workforce in 2015,[7] and 80 percent of today's workers prefer benefits and perks such as mobile devices and non traditional working environments to a standard pay raise.[8] That means you might not have the option of dictating the types of

devices and programs employees use for work, making endpoint security more important than ever as each new entry point presents a new moving target.

When smartphones, wearables and tablets enable millennial and Gen Z employees to be as productive in the coffee shop as they are in a cubicle, the IT challenge isn't herding data back into the office. It's balancing mobility enabled productivity with securing data, no matter where it roams. Click here to read more about securing mobile devices.

Holistic approaches to security consider each endpoint as a possible hacker entry point, securing connections no matter where authorised users access the network or what device they use. When devices connect via secured linkage, layers of authentication and encryption safeguard data from access threats.

Securing company data outside the office is the IT challenge of the moment:

53%

Of office workers in European countries use personal devices outside the workplace to perform work-related tasks.[9]

62%

Of all employees work from more than one location.[10]

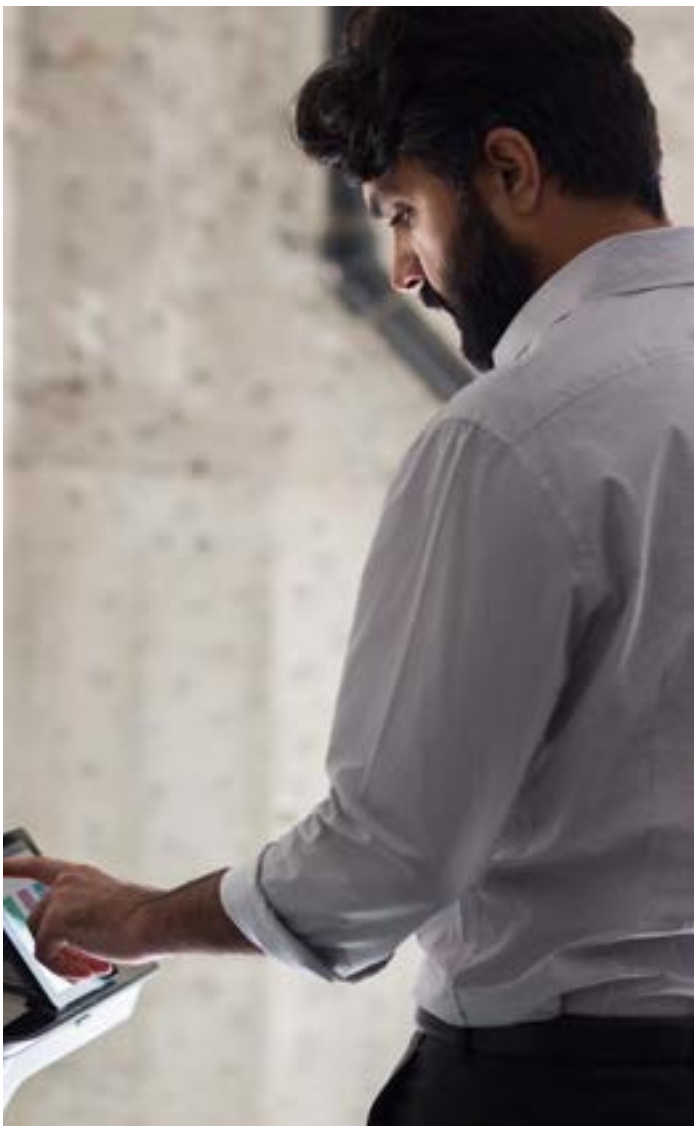
DATA, DATA EVERYWHERE.

Feel like you're drowning in a sea of data? You are. We create about 2.5 quintillion bytes of data each day. To better comprehend just how much data that is, the earth is thought to contain 7.5 quintillion grains of sand.[11]

In just three days, humanity creates a number of data bytes equal to the total amount of sand granules present on our planet. And IT professionals have to keep it from slipping through their fingers into the hands of hackers.

EVERY THREE DAYS,

technology users generate a number of data bytes roughly equal to the grains of sand on the earth. And the print environment — which manages data, documents and information — handles a staggering number of those bytes on a daily basis.



In addition to adopting the latest security approaches, changes in the way we work present new challenges as employees struggle to implement enhanced security practices in the office and abroad. Take the office printer, for example. As a checkpoint, it is often neglected by security departments, receiving streams of information all day, every business day. Sales and human resource departments are at high risk for print-related security breaches, and executives generate and print some of the riskiest types of data within a company. Gaining buy-in from these groups to adhere to new protocols is paramount to protecting data.

When the seemingly ubiquitous flow of sensitive employee data and confidential customer information is compromised, the effects are costly. But when printers are monitored for threats and and basic security measures such as pull printing are implemented, hidden security threats are eliminated before they can even begin. According to a recent study, 25.3 percent of

THE IT CHALLENGE:

Securing access to unprecedented amounts of data without limiting the benefits of a changing workplace.

data breaches in the U.S. financial sector were due to a lost or stolen device — more than hacking, which accounted for one in five data breaches.[12] And collaboration in a global workforce further complicates security, as workers connecting remotely don't always consider data protection practices.

Holistic security systems must assess "what ifs" associated with lost devices and emerging connectivity. Anti-theft software helps users track and recover misplaced machines. Network access control systems enable seamless collaboration and connect people securely and automatically. If a hacker does manage to gain entry and cause damage, BIOS recovery gets employees working again.

WHY THE WALL WON'T PROTECT YOU.

Data everywhere, overwhelming security threats, hackers seeking vulnerabilities — paralysing alarm fatigue and paradoxical viewpoints are natural responses to a problem that exploits the weaknesses (and underdeveloped strengths) of the modern workforce.

Nonetheless, IT leaders don't have to freeze in the face of threats. Ecosystem protection provides not only security that works without intervention but also peace of mind in an age of unrelenting disruption.

An IT admin may have the best firewall on the market, but what good is an isolated security initiative when users inadvertently invite hackers onto the network? Social attacks such as phishing present a serious vector for security breaches.

IT-led security initiatives, like ongoing education, periodic vulnerability tests and secure browsing, can go a long way toward eliminating employee-enabled data breaches and malware exposure; however, they can't eradicate the element of human error. When IT admins can train workers, knowing a holistic security system has their back, they can focus

Phishing: the cybercrime stalwart

Phishing preys on user inattention to security — and it works. According to the 2016 Verizon Data Breach Investigations Report:

90%

Of data breached by phishing are credentials.

30%

Of users open phishing emails.

91%

Of visual hacking attempts are successful.[13]

on developing programs without the persistent distraction of alarms and alerts.

A 2016 report found a 200-plus percent increase in attacks targeting notebooks and desktops over the last several years,[12] and these attacks are often successful in accessing a network. How? Weak or stolen passwords account for 81 percent of hacker breaches.[12] When 67 percent of used storage devices hold personally identifiable information, the majority of breaches, no matter the device, reveals potentially damaging data.[14]

WEAK OR STOLEN PASSWORDS ACCOUNT FOR 81 PERCENT OF BREACHES.[12]

It's time to rethink the way we protect data. Bandage fixes, such as passwords without comprehensive data encryption, are obsolete and provide a false sense of security. When threats come from all angles — including within — security tactics and strategies must grow to keep up with the hackers. Evolve with an ecosystem of protection: layered barriers to infiltration across all devices.

Multilayered security

While standard approaches to security quarantine data in a guarded castle, layered security creates multiple hurdles to further protect data against hackers — imagine horseback scouts, a moat and booby traps providing additional protection to the data castle. If one layer is breached, another

standing guard to stop the attack. Behind the network level of security, these layers can help thwart an attack that starts at an endpoint device:

- Control access with multifactor authentication.
- Apply unique administrative passwords. Reduce the attack surface, i.e., close un-needed ports and protocols.
- Encrypt data at rest on the device and in transit.
- Apply anti-malware software down to the BIOS level of device software/firmware.
- Check and maintain device security setup.
- Monitor for threats.
- Maintain network security.

LAYERED SECURITY SOLUTIONS PROVIDE LEVELS OF PROTECTION TO LET WORKERS IN — AND KEEP HACKERS OUT.

With 68 percent of experts now citing endpoint security as an important component of their security strategy[15], it's important to seek products and solutions to automate and increment your security with added layers. For example, including BIOS protection for both printers and PCs — a crucial area that IT professionals often lack visibility into — adds a key layer of security at the lowest level of the device firmware and automatically checks the validity of the BIOs when a device boots.

AN ECOSYSTEM OF PROTECTION DELIVERS ENDPOINT SECURITY WHEN AND WHERE IT'S NEEDED.

The security evolution.

In today's changing employee environment, where numerous entry points are spread across a decentralised workforce, it's critical to adopt new, holistic approaches to data security.

Holistic security allows workers to connect when and where they need to, via secure connections that authenticate users accessing the network. And it empowers IT professionals to tackle cybersecurity threats regardless of their origin. A security ecosystem complements — not conflicts with — how work gets done.

That's the paradox antidote.

REFERENCES AND CREDITS.

[1] PWC, "Global Economic Crime Survey 2016: Cybercrime," **http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html** (accessed May 10, 2017).

[2] Risk Based Security, "Data Breach QuickView Report," **https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf,"** (accessed May 5, 2017).

[3] Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," 2016.

[4] Spiceworks, "HPI Printer Security Research: Strategic Market Research Report," November 2016.

[5] IDC, "The Printer Is an Endpoint: Proactively Addressing the Security Vulnerability," November 2016, **http://idcdocserv.com/US41939416-_1**

[6] HP, "Cyber Risk Report 2016," 2016.

[7] Pew Research Center, "Millennials surpass Gen Xers as the largest generation in U.S. labor force," May 11, 2015, **http://www.pewresearch.org/fact-tank/2015/05/11/millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force** (accessed May 10, 2017).

[8] Glassdoor, "4 in 5 Employees Want Benefits or Perks More Than a Pay Raise; Glassdoor Employment Confidence Survey (Q3 2015)," October 2, 2015, **https://www.glassdoor.com/blog/ecs-q3-2015** (accessed April 3, 2017).

[9] smallbusiness.co.uk, "Out of sight out of mind?

[10] Inc., "62% of Employees Now Work Remotely: How Your Office Will Need to Adjust," **https://www.inc.com/john-brandon/62-of-employees-now-work-remotely-how-your-office-will-need-to-adjust.html** (accessed May 1, 2017).

[11] **http://www.npr.org/sections/krulwich/2012/09/17/161096233/which-is-greater-the-number-of-sand-grains-on-earth-or-stars-in-the-sky**

[12] Bitglass, "Lost & Stolen Devices Account for 1 in 4 Breaches in Financial Services," August 25, 2016. **https://www.bitglass.com/press-releases/financial-services-breach-report-2016 (accessed May 25, 2017).**

[13] Verizon, "2016 Verizon Data Breach Investigations Report," 2016.

[14] Blancco, "67 Percent of Used Drives Sold on eBay and Craigslist Hold Personally Identifiable Information and 11 Percent Contain Sensitive Corporate Data," June 28, 2016. https://**www.blancco.com/press-releases/67-percent-used-drives-sold-ebay-craigslist-hold-personally-identifiable-information-11-percent-contain-sensitive-corporate-data** (accessed May 25, 2017).

[15] Ponemon, "2016 State of the Endpoint Report," 2016.

Learn more about how HP can help protect your company.

VISIT HP.COM/GO/HPSECURE

4AA7-0627EEAU, November 2017, Rev.8