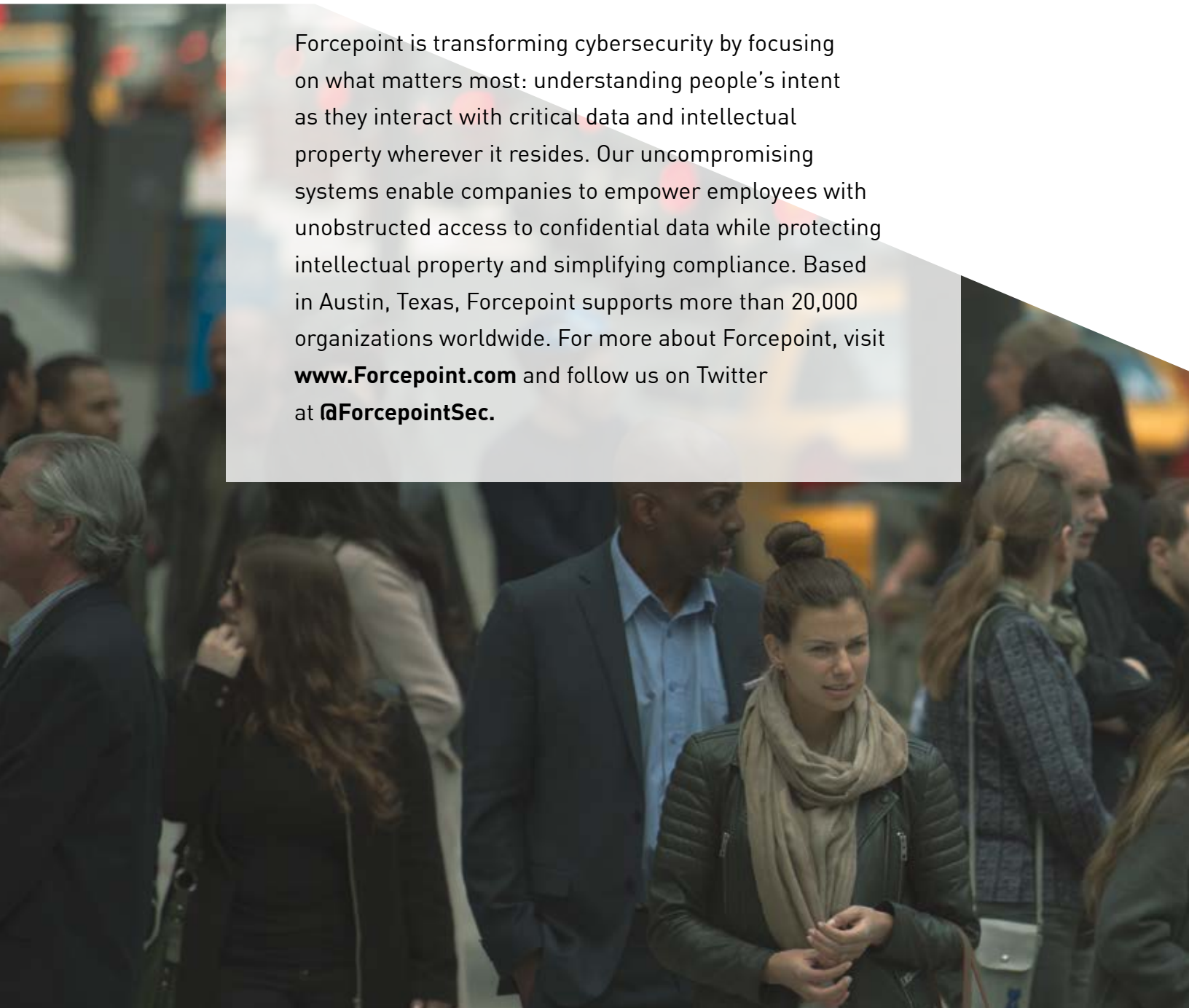
THE 2017 STATE OF CYBERSECURITY

A new security paradigm: understanding human behavior and intent to protect employees, critical business data and IP

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

ABOUT FORCEPOINT



Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit **www.Forcepoint.com** and follow us on Twitter at **@ForcepointSec.**

Table of Contents

Executive Summary | 4

Enablement in the Modern Enterprise | 6

A Look into People-Based Risk | 8

Technology Alone Is Insufficient | 13

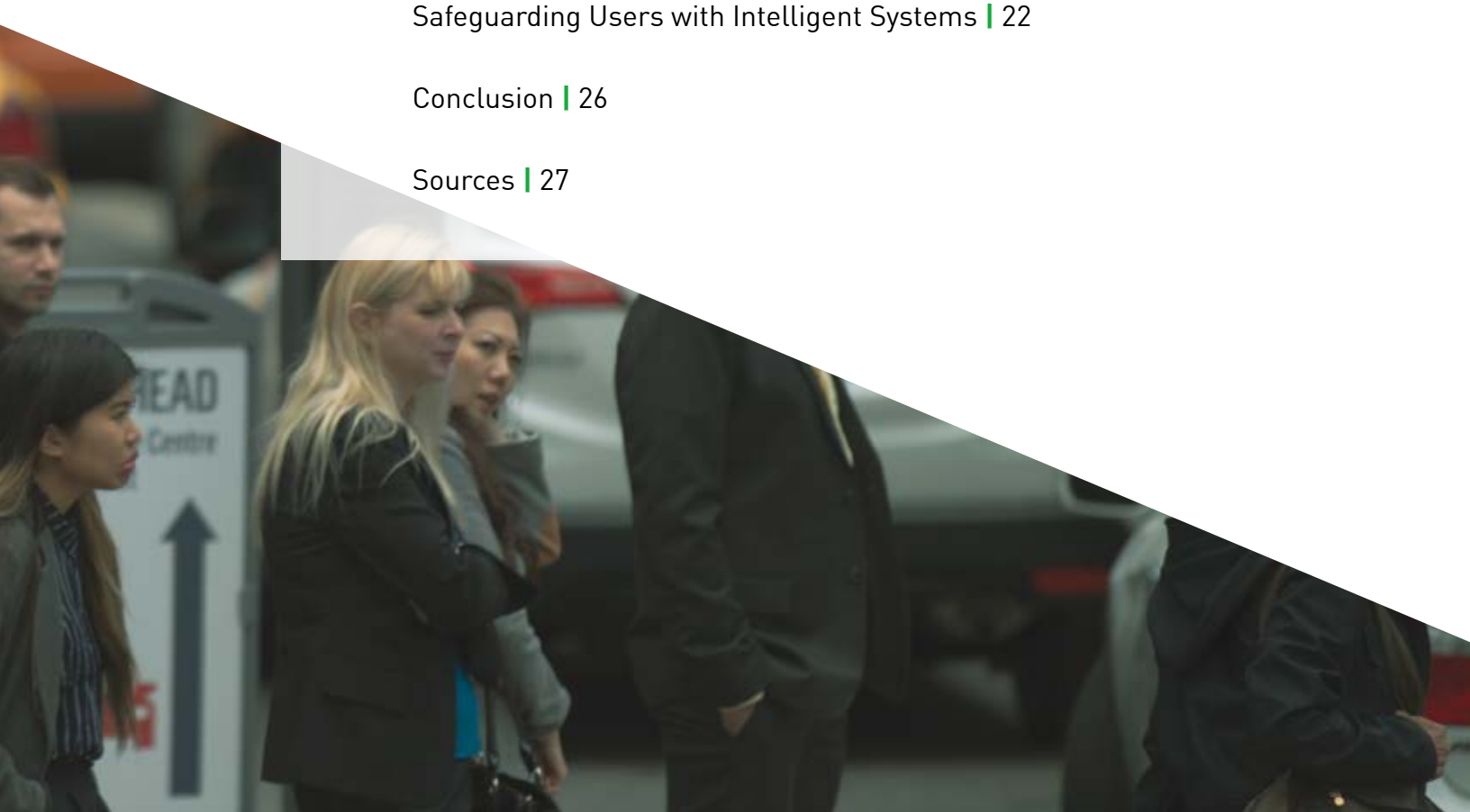
The Human Point | 14

The Cyber Continuum of Intent | 15

Safeguarding Users with Intelligent Systems | 22

Conclusion | 26

Sources | 27



Executive Summary

Modern enterprises with aspirations of improving efficiency often leverage new technologies to reduce costs, attract a millennial workforce, improve employee retention and enhance organizational agility. While good for business, this enablement presents new security challenges. Critical data is everywhere — stratified in private and public clouds, on removable media and in mobile devices — and co-mingled haphazardly with personal data on employee devices.

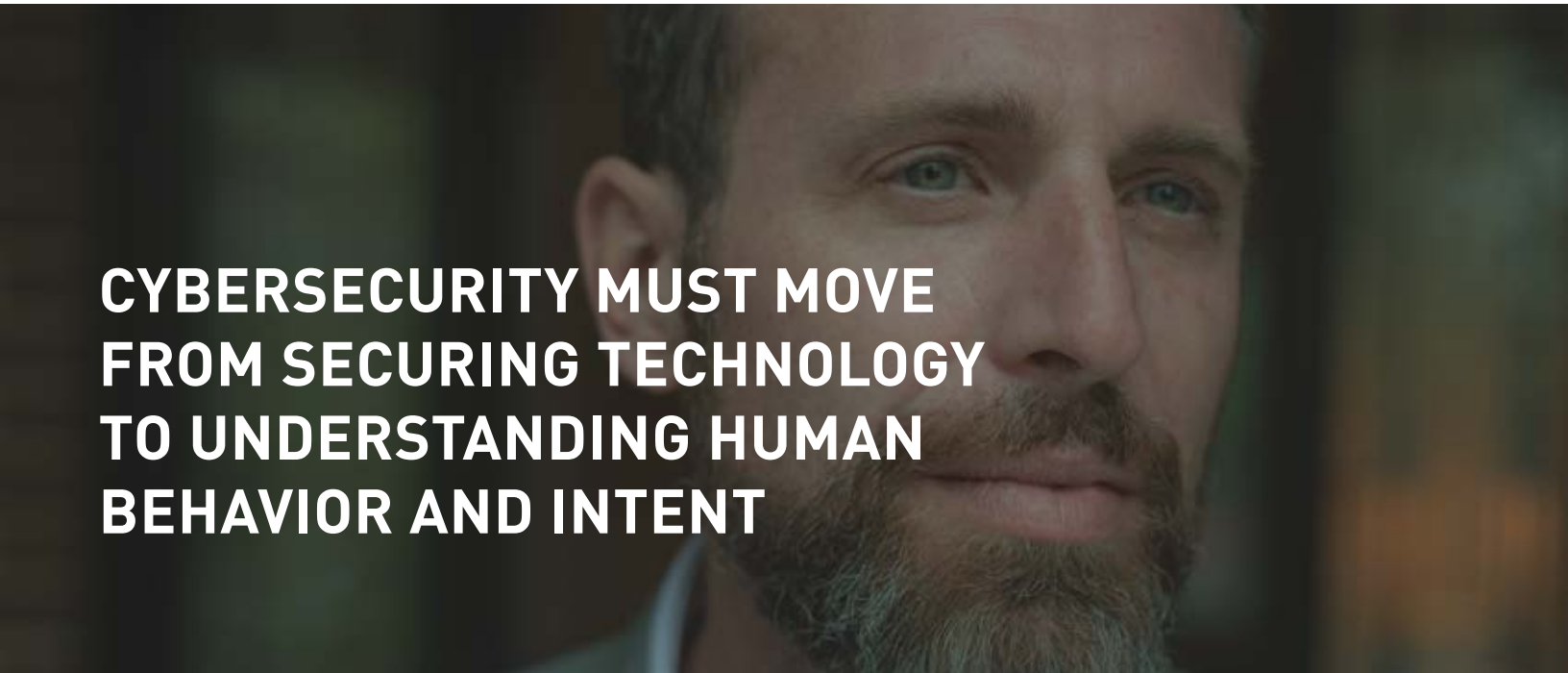
Visibility has introduced new organizational risks, yet many security professionals today can't see how and where data is used as it sprawls across company-owned, employee-owned and hosted applications. Without this insight, people-based vulnerabilities destabilize even the most secure networks and greatly reduce the efficacy of cybersecurity investments.

Regardless of how attacks originate, they ultimately inflict the most damage at the points in which people interact with critical business data and intellectual property. These human points of interaction have the potential to undermine even the most comprehensively-designed systems in a single malicious or unintentional act. For this reason, the approach to security the industry has relied upon for years — centered on protecting technology infrastructure — will not work. New technologies arise, products are refreshed and the overall IT infrastructure-centric view sets up a never ending game of catch-up. By focusing on the constant — people interacting with critical business data and IP — security professionals are better able to manage the risk facing their organizations.

To determine the cause of security incidents (e.g., data theft, intellectual property loss) and prevent them in the future, security professionals must look at the intent behind peoples' actions. Insiders fit into three groups along a spectrum that we call the continuum of intent, which categorizes users as accidental, compromised or malicious. And it's important to note that people can move in and out of those categories depending on a number of factors, so we also examine typical behaviors that map to these categories and span the full continuum.

Security professionals identify the need to observe human behavior and understand intent as people (e.g., employees, partners, privileged users) interact with data, yet acknowledge industry-wide shortcomings in being able to do so. Only by taking a people-centric approach to security can we better understand, manage and mitigate organizational risk.

The industry needs intelligent, integrated systems to provide visibility into user behavior and uncover intent by providing the context behind a user's actions. These systems of integrated solutions, when coupled with comprehensive cybersecurity programs, can secure the mobile workforce, reduce IT's incident management burden, increase the value of new security investments and provide proactive security that promotes innovation within the organization.



CYBERSECURITY MUST MOVE FROM SECURING TECHNOLOGY TO UNDERSTANDING HUMAN BEHAVIOR AND INTENT

Enablement in the Modern Enterprise

Throughout the history of cybersecurity, the industry has focused steadily on threats that arise from evolving technology infrastructure and environments. Years ago, when desktop PCs sat in most offices, employers might not have had absolute control over their workers' use of technology and data, but they could contain it (for the most part). IT departments determined which computers and software programs to acquire and provision, then created guidelines for what constituted "appropriate use" of that technology. When workers finished for the day, they turned off their computers, went home and stayed offline until the next morning.

Today, the concept of a network has shifted dramatically — boundaries have extended and now include everything from consumer social applications to hosted cloud infrastructure and employee-owned devices. Employees have an insatiable appetite for new devices, apps, social media and content, as well as individual preferences for their work environments.

Remote Employees Are Increasing In Number

The issue of how, when and where people work is forcing organizations to shift their management styles to optimize performance at a time when only 33% of U.S. workers feel engaged in their roles. According to Gallup's *State of the American Workplace*, the number of employees working remotely rose by four percentage points between 2012 and 2016, from 39% to 43%, and employees working remotely spent more time doing so.[1]

Organizations are focusing their attention on how to attract, engage and retain employees, and for good reason. Per Gallup, decreased employee engagement and commuting to the workplace cost U.S. companies $550 billion and $90 billion in productivity losses, respectively. Remote employees (those who work at least two days a week from home) report lowered stress levels, increased morale, better productivity and a greater sense of overall worth compared to in-office workers. Companies also benefit

from allowing employees to work remotely: It reduces employee turnover, decreases operating and real estate costs and leads to more highly-qualified potential hires. A recent survey found that 58% of human resource professionals cite flexibility as the most effective way to attract new talent.[2]

Lenient Organizational BYOD Policies

The bring your own device, or BYOD, concept is a major staple among enterprises today — the average organization has approximately 23,000 mobile devices (including personally-owned mobile devices) in use by employees.[3] Thanks to the Cloud, seamless synchronization, smartphones, tablets and lightweight laptops, workers often decide — overtly or covertly — which devices to use, and when and where they will use them. While 89% of employee mobile devices connect to corporate networks, only 65% of companies have policies in place that allow them to do so.[4]

While BYOD policies have helped companies cut hardware and service costs, they have also created an added burden for IT departments in charge of maintaining these devices. One study found that 75% of companies either already allow employees to bring their own devices or have plans to integrate a BYOD- friendly policy in the near future, namely due to the aforementioned employee availability and ensuing productivity benefits.[5]

Increased Use of Cloud Apps

The average organization uses roughly 13 cloud apps and 15% of businesses use both Office 365 and Google Apps, according to identity and access management startup Okta's *Business @ Work* report.[6] Cloud apps and services provide tangible benefits to businesses by allowing organizations to reduce capital expenditures and elastically allocate resources for computing, processing and collaboration. Users find anytime, anywhere access to services a productivity boon while organizations find cloud economies of scale result in lower operating costs and an ability to focus on their core business mission.

Many organizations have embraced public cloud services, which cover fast-growing SaaS areas such as Office suites, digital content creation and business intelligence. According to Gartner, worldwide public cloud services will grow to $246.8 billion in 2017, up from $209.2 billion in 2016.[7]

A Look into People-Based Risk

Companies store data using public and private cloud services, enable employees to work from anywhere in the world and outsource parts of their business to direct focus to mission-critical issues. Yet, the vast majority are far from having a holistic and comprehensive view of user activities that might point to immediate risk. The situation is serious enough that one-third of enterprises have suffered from an insider-caused breach, with possible losses from each incident amounting to more than $5 million, according to the SANS Institute.[8] Researchers at SANS also found that nearly three-quarters (74%) of these organizations are worried about negligent or malicious employees who might be insider threats.

In 2017, we conducted a study of 1,252 cybersecurity professionals worldwide to view common trouble areas and to better understand the state of cybersecurity; most importantly, how organizations might view a forward-focused strategy, one that moves beyond the current state of chasing infrastructure remediation. The resulting report, *The Human Point: An Intersection of Behaviors, Intent & Critical Business Data*, uncovered the following trends:

- **Lack of Visibility –** Cybersecurity professionals have a hard time maintaining visibility into how employees use critical business data across company- and employee-owned devices and company-approved services. (See Fig. 1)

- **Co-Mingling of Social and Enterprise Apps on BYOD –**The BYOD shift presents a paradox: Managed endpoint policies can allow users to access, modify and store data on their devices, while unmanaged devices require a more restrictive policy that prevents the loss of critical corporate data. Potential data leakage and exposure broadens as organizations allow access to critical business data, either through BYOD or corporate policies. (See Fig. 2)

Fig. 1 - Visibility of critical business data across company/employee owned devices & services

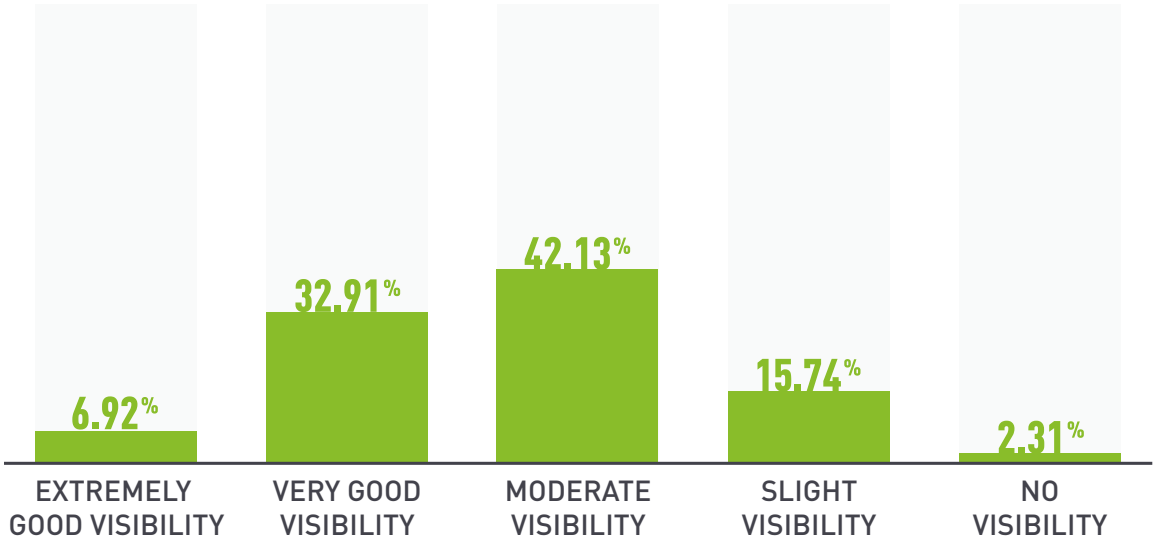
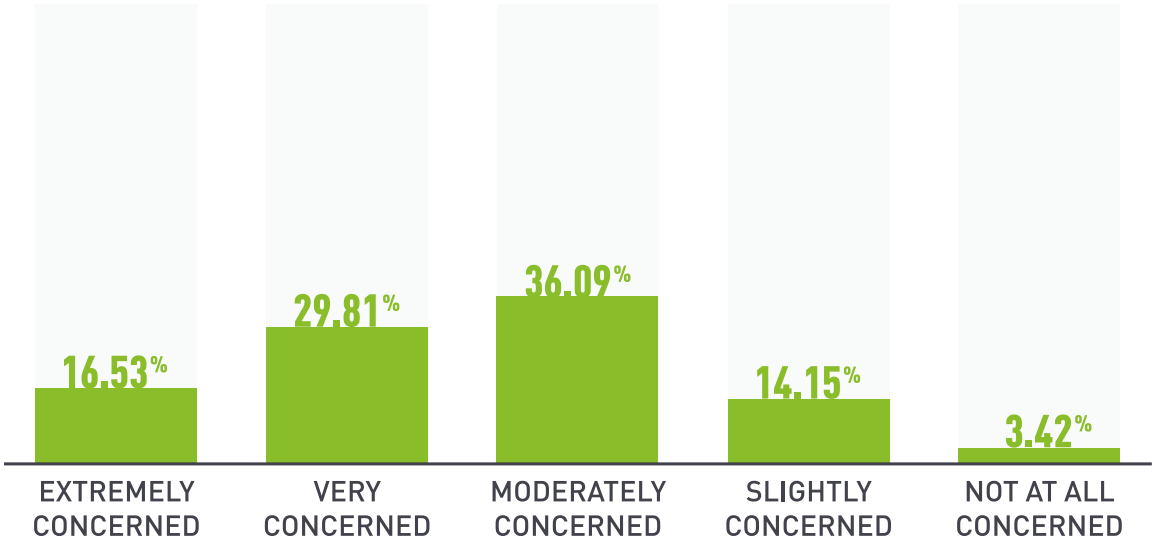


Fig. 2 - Concern regarding personal & business data co-mingling on devices



- **The Shortcomings of Big Data –** Big data tools are being used by IT to find security trends and make sense of hundreds of thousands of daily security incidents, yet statistics show it is not particularly effective at helping organizations strengthen cybersecurity posture.

WHILE

27%

OF RESPONDENTS REPORTED USING A

BIG DATA APPROACH TO HELP MANAGE SECURITY

THE MAJORITY

STATED IT MADE THEIR JOBS ONLY *SLIGHTLY* EASIER

- **Understanding Behavior and Intent –** Learning how users interact with critical data is a rising priority. And while there's agreement that understanding behavior and intent is vital to cybersecurity, most security professionals are unable to do so effectively. (See Fig. 3 & Fig. 4)

Fig. 3 - Ability to understand human behavior

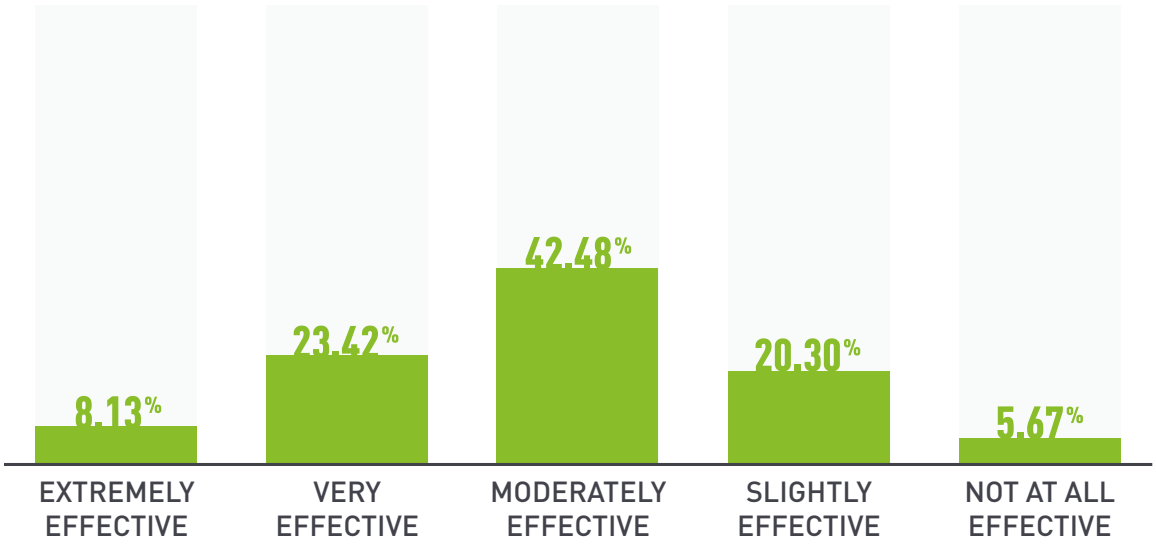
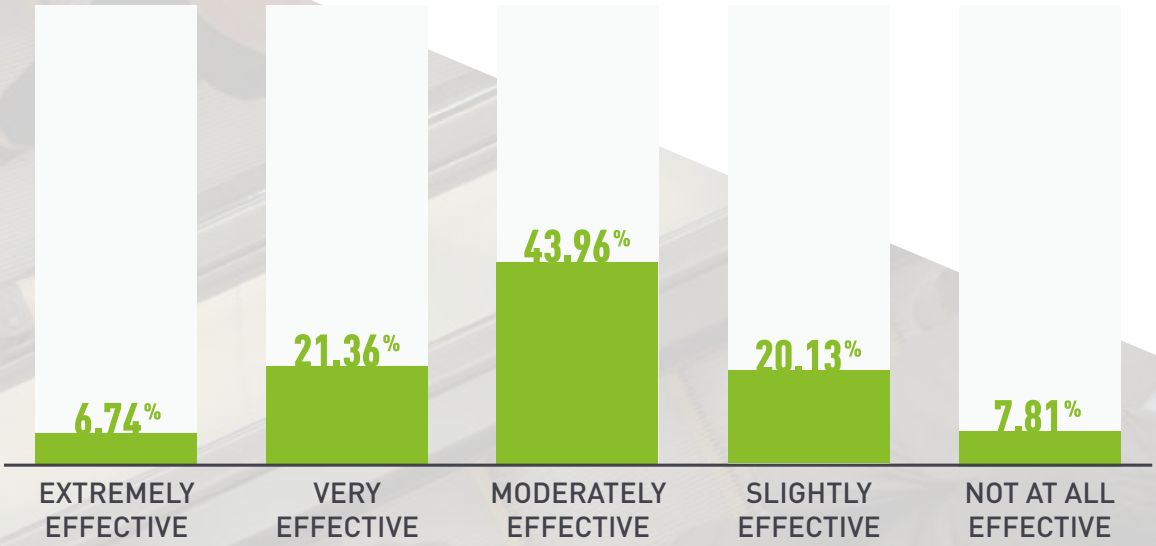


Fig. 4 - Ability to understand intent



ONE-THIRD OF ENTERPRISES HAVE SUFFERED FROM AN INSIDER-CAUSED BREACH

Technology Alone Is Insufficient

According to Gartner estimates, worldwide spending on information security is expected to reach $90 billion in 2017, an increase of 7.6% over 2016, and to top $113 billion by 2020.[9] More security spending should theoretically result in fewer incidents, yet U.S. companies and government agencies suffered a record 1,093 data breaches in 2016—an overwhelming increase of 40% from 2015.[10] Despite new cybersecurity investments, serious breaches continue to rise, proof that this never-ending hunt for new security technology lacks any legitimate efficacy.

Traditional Security Tools

With every new piece of owned or hosted hardware or application, cyber professionals are tasked with finding the latest tools that will lock these systems down. Most traditional security controls were not designed to help organizations gain visibility, observe users' behaviors as they handle critical data, or supply context behind these behaviors to truly evaluate user risk.

While existing security infrastructure can be leveraged in combination with a number of tools to help enterprises mitigate this issue, this does not provide enough visibility or control to form a comprehensive solution.

The social sciences are helping us open doors into a new understanding of how users and cybercriminals operate at the intersection of behavior and data. "We've had too many computer scientists looking at cybersecurity, and not enough psychologists, economists and human-factors people," Douglas Maughan, head of cybersecurity research at the U.S. Department of Homeland Security (DHS) said to Nature magazine in 2016. The DHS and other organizations in the U.S. and U.K. have been boosting funding for research on the "human side of cybersecurity" over the past five years.[11]

The Human Point

Threats evolve and technologies come and go, but people are the constant in cybersecurity. Regardless of how attacks originate, they ultimately inflict the most damage at the points in which people interact with critical business data and intellectual property.

The people at the center of today's most damaging breaches can include current or former employees, board members or anyone who has ever had access to an organization's proprietary or confidential information, including:

- Contractors
- Business associates
- Third-parties
- Individuals who have knowledge of an organization's security practices, confidential information or access to protected networks or databases.

The damage caused at the human point can take any of the following forms:

- Physical harm
- Information theft
- Monetary theft
- Identity theft
- Data corruption or deletion
- Data altering with the intention of producing inconvenience or false criminal evidence.

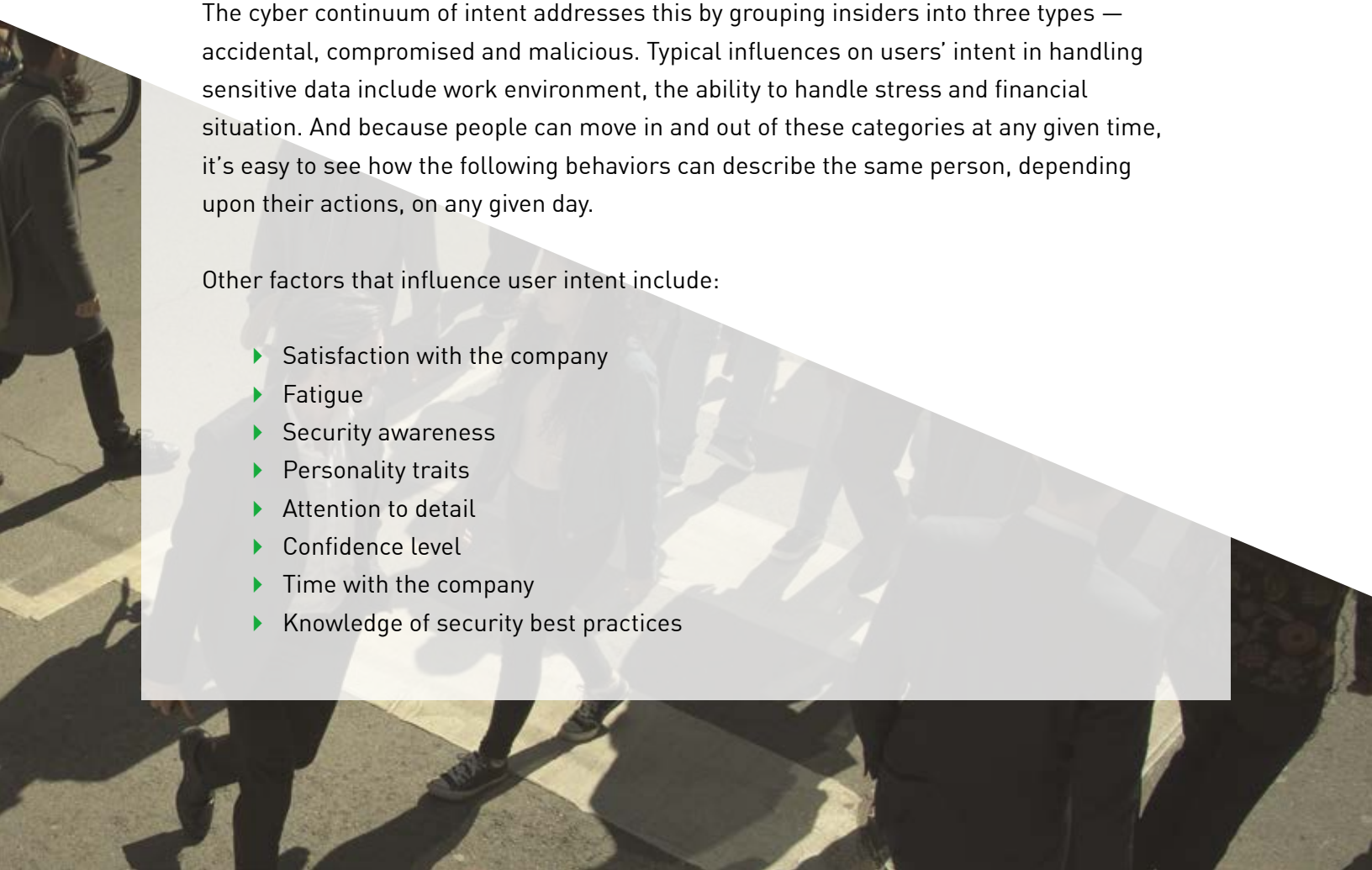
The Cyber Continuum of Intent

The point of interaction between people and data — where technology is most enabling and security is most vulnerable — can undermine the most comprehensively-designed systems in a single malicious or unintentional act. IT professionals may find it difficult to decipher whether the user is making a mistake, has been compromised or is intentionally causing harm. According to the Institute for Critical Infrastructure Technology, in 2015, only 17% of security professionals were aware of an insider threat on their network, even though enough anomalous activity suggested that insider threats occurred in 85% of organizations.

The cyber continuum of intent addresses this by grouping insiders into three types — accidental, compromised and malicious. Typical influences on users' intent in handling sensitive data include work environment, the ability to handle stress and financial situation. And because people can move in and out of these categories at any given time, it's easy to see how the following behaviors can describe the same person, depending upon their actions, on any given day.

Other factors that influence user intent include:

- Satisfaction with the company
- Fatigue
- Security awareness
- Personality traits
- Attention to detail
- Confidence level
- Time with the company
- Knowledge of security best practices



Understanding Insider Threats

Accidental insiders are people that make unintentional mistakes, perhaps because of a lack of training, awareness or existence of proper processes and systems, or due to negligent behaviors. They also may knowingly skirt the rules in favor of productivity, inadvertently exposing their organization to data theft. Types of accidental insiders include:

Inadvertent actors are victims of poorly communicated policies or simply lack awareness. They may make honest mistakes because they didn't know the rules; these users will hit the wrong button or send a document to the wrong person. Inadvertent users could also be under high levels of stress, which causes burnout and leads to sloppiness in organizational protocol. Unable to reinvigorate their brains adequately, these users are less likely to implement best security practices. More often than not, their behavior is negligent or careless. They may also be the company know-it-all who responds to a request when someone more qualified should or who posts unannounced quarterly results on social media. If these inadvertent actors turn malicious, they may intentionally steal or manipulate sensitive information for fun, out of curiosity — or to prove they *can*.

Convenience seekers break businesses processes, but not always maliciously. They put data were it shouldn't be, not where it should be. These types of accidental insiders are convinced that they have a right to certain types of data, or conclude they "own" data, including customer lists, source codes, scientific research and process documentation and templates. They might ignore process or policy. These are users with privileged access that do not believe that any of the scary stories could happen to them. They take advantage of their super-user credentials out of convenience, for example, only to cause malware infection of a mission-critical server after opening a highly targeted phishing email. This attitude can pertain to users at any level of the company: auditors, executives, developers, and others with privileges.

ACCIDENTAL INSIDER

Compromised insiders are users with access to the network whose credentials have been stolen and used by an attacker to penetrate and misuse the system. Profile alerts do not provide definitive proof a user has been compromised, so security teams often don't realize the threats exist until it's too late.[12] Some examples of compromised insiders are:

Malware victims have been targeted and infected with phishing emails or ransomware that creates a breach in the network or contaminates a device. These attacks usually come from outside the organization and use a form of social engineering to co-opt the compromised user into risky behavior that opens the door for an attacker to access the enterprise network. For example, Forcepoint Security Labs researchers recently discovered that Carbanak (also known as Anunak) hacking group, which stole one billion dollars from banks in 2015, is now trying to exploit office documents hosted on Google services to spread malware. People who open these weaponized documents allow the Carbanak gang to run a script to seize control of the machine.[13] Even with many well-publicized examples of phishing attacks, 30% of users still open phishing emails and 12% go on to click the malicious attachment or link, unintentionally enabling the hacker.[14]

Impersonated users have had their credentials stolen or have been duped by an external threat actor. These users may not intend to do harm but they've been manipulated by social engineering into opening a secure door or clicking the wrong file, or have not been keeping up to date the cyber hygiene of their devices, including maintaining backups and airtight passwords. Passwords falling into the wrong hands is one of the biggest causes of network vulnerability: 63% of known data breaches involved weak or stolen passwords.[15] Once their identities have been impersonated by attackers, compromised users are virtually impossible to detect because they look and act like many other users on the network. The eighth-largest dump of confidential information in history occurred in 2014, because hackers had a little help from employees who literally opened the office door to let them into the building.

COMPROMISED INSIDER

Malicious insiders have knowledge and access to organizational resources. These users generally have an easier time carrying out damaging attacks due to the extended length of time spent on the network. Their internal discontent due to differences with colleagues, bosses or the organization itself manifests itself destructively. Malicious insiders typically fall into these two categories:

Rogue employees are users who carry a grudge against their employer. They may have been model workers for years, but recent situations or activities have led them into bad behavior. In many cases, rogue employees may have received a poor performance review, or know they're about to be transferred against their will, laid off, demoted or disciplined. Both the FBI and the DHS believe that these disgruntled employees pose significant cyber threats due to their access to critical information and networks. On their way out the door, these employees use their access to copy, delete or corrupt data, steal IP, obtain confidential customer information or purchase things without authorization. In many cases, after they left, they used third-party cloud file sites and personal email accounts or had continued access to the network.[16] Measures need to be in place to detect such a breach. However, these insiders are motivated and knowledgeable. In some cases, rogue employees are influenced by outside parties to intentionally commit to steal data.

Criminal actor employees are people that conduct corporate espionage or act as agents for foreign nationals and organized crime syndicates. They've used their internal status to gain network access by compromising other users or finding a back door. They're motivated, knowledgeable and now command all of the access and privileges to break the law and steal an organization's intellectual property and data. Those insiders with access and criminal intent are just as dangerous, if not more so, than external threat actors. Employees who feel they deserve more pay may exfiltrate or steal sensitive information from their company to sell it on darknet markets such as Alphabay. They might also offer up the home address and social security numbers of the CEO or CFO to the highest bidders or to tabloid press for monetary gain.

MALICIOUS INSIDER

THE POINT OF INTERACTION BETWEEN PEOPLE AND DATA IS WHERE TECHNOLOGY IS MOST ENABLING AND SECURITY IS MOST VULNERABLE

Safeguarding Users with Intelligent Systems

The industry agrees the perimeter no longer exists — today's challenge is to control data as it moves in and out of the organization's possession while employees seek to use it on-demand, everywhere.

Instead of spending $113 billion on technology designed to protect a perimeter that has crumbled, we should look at people and protect against those behaviors we know lead to critical data and IP loss. A cybersecurity program that can make sustainable progress exists only with a blend of technologies, policies, cultural changes and intelligent systems. These systems must be capable of observing behavior and deciphering intent in order to proactively protect users, critical data and, most importantly, the point at which they intersect. Such systems include products that can be easily integrated to provide a comprehensive view of risky behavior and mitigate risks many steps before they turn into breaches.

This people-centric vision drives Forcepoint's strategy to create security solutions and programs that stop bad cyber behaviors and help organizations run more efficiently. Led by feedback from our customers and partners, we're developing a blueprint of people, processes and security systems that enables enterprises to better understand human behaviors and the intent that drives them in order to protect critical data and IP everywhere. This strategy aligns to our four focus areas, including:

- **Cloud Security and CASB:** Protecting people from compromise as they use the web and email from any location, on any device.

- **Network Security:** Giving visibility into people's actions throughout the network and keeping attackers out of data centers, offices and cloud environments.

- **Data & Insider Threat Security:** Identifying high-risk users and data behaviors that require further investigation and deployment of the right data protection controls.

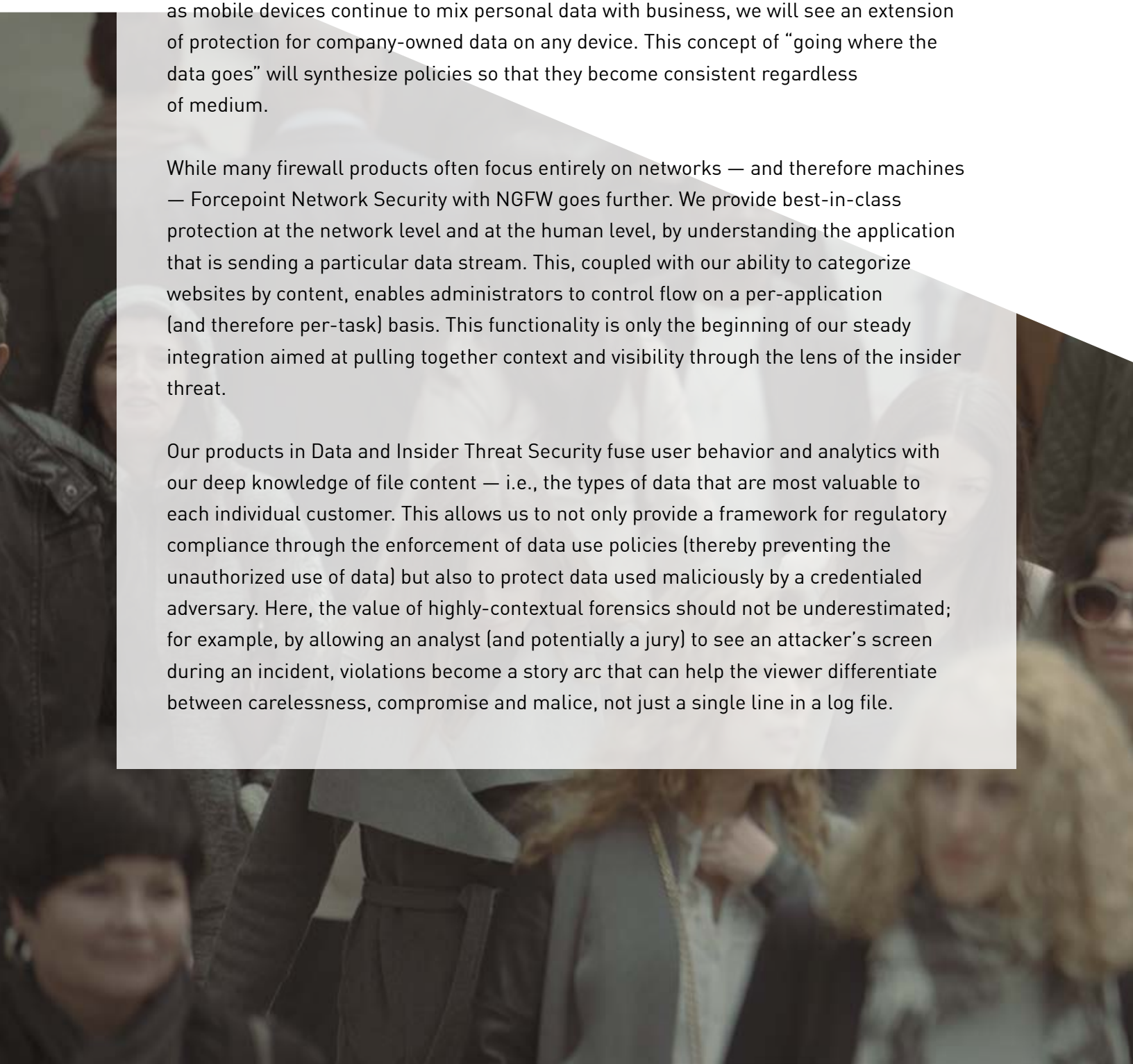
- **Cross Domain Solutions**: Enabling people to securely access and transfer sensitive information across multiple separated networks with control, ease and efficiency.

Executing a strategy founded on people-centric protection is clearly a process rather than a single point in time, as the market begins to adopt preventative approaches that focus less on the perimeter and more on safeguarding data through its entire lifecycle of creation, use, dissemination and deletion. Each of our focus areas represents an opportunity to gather context around those points of contact — and potential exposure — an attacker may leverage.

Human-centricity and knowledge of data also underpins our philosophy with respect to both Cloud Security and CASB solutions. As many compromises begin through spearphishing and the web, we have attempted both to detect and prevent when a compromise is impacting the data that is most valuable to the company. As we move forward, these systems will become increasingly integrated with our data protection solutions, eroding the artificial boundaries legacy product categories create. Similarly, as mobile devices continue to mix personal data with business, we will see an extension of protection for company-owned data on any device. This concept of "going where the data goes" will synthesize policies so that they become consistent regardless of medium.

While many firewall products often focus entirely on networks — and therefore machines — Forcepoint Network Security with NGFW goes further. We provide best-in-class protection at the network level and at the human level, by understanding the application that is sending a particular data stream. This, coupled with our ability to categorize websites by content, enables administrators to control flow on a per-application (and therefore per-task) basis. This functionality is only the beginning of our steady integration aimed at pulling together context and visibility through the lens of the insider threat.

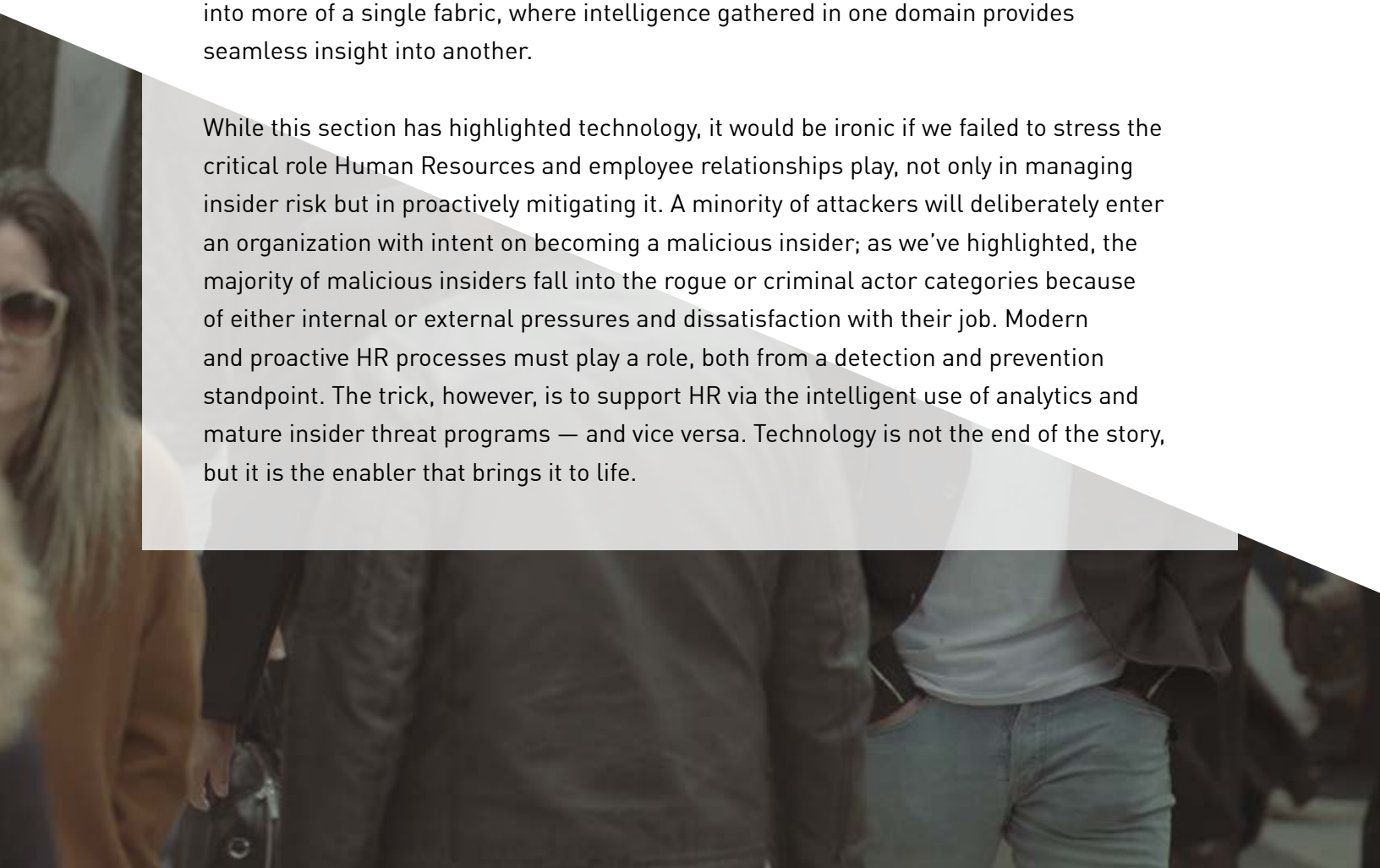
Our products in Data and Insider Threat Security fuse user behavior and analytics with our deep knowledge of file content — i.e., the types of data that are most valuable to each individual customer. This allows us to not only provide a framework for regulatory compliance through the enforcement of data use policies (thereby preventing the unauthorized use of data) but also to protect data used maliciously by a credentialed adversary. Here, the value of highly-contextual forensics should not be underestimated; for example, by allowing an analyst (and potentially a jury) to see an attacker's screen during an incident, violations become a story arc that can help the viewer differentiate between carelessness, compromise and malice, not just a single line in a log file.



Rounding out the portfolio are cross domain solutions that enable the efficient and secure use of physically segmented networks designed to enforce the storage and maintenance of information within data centers, instead of on local devices. These solutions provide a high degree of usability without compromising security to work with and for the user: They not only enforce secure and controlled access to critical data housed in multiple networks, they monitor the flow of data between machines and users so data gets to the right recipient at the right time, eliminating the need for manual downloading and "sneaker-net." Cross domain solutions establish a requirement for good security behaviors while also assisting administrators with robust auditing.

These technologies work together to provide managers with the situational awareness they need to make better decisions. None is disparate from the other; only when integrated can solutions truly execute across the vast array of human interactions that impact security to protect critical data. Thus, our long term vision is to help administrators and investigators move from answering the question of "what event happened?" to the more nuanced "why did this happen?" This shift will be a process, and one that has the potential to radically rewrite the traditional "stovepipes" of protection into more of a single fabric, where intelligence gathered in one domain provides seamless insight into another.

While this section has highlighted technology, it would be ironic if we failed to stress the critical role Human Resources and employee relationships play, not only in managing insider risk but in proactively mitigating it. A minority of attackers will deliberately enter an organization with intent on becoming a malicious insider; as we've highlighted, the majority of malicious insiders fall into the rogue or criminal actor categories because of either internal or external pressures and dissatisfaction with their job. Modern and proactive HR processes must play a role, both from a detection and prevention standpoint. The trick, however, is to support HR via the intelligent use of analytics and mature insider threat programs — and vice versa. Technology is not the end of the story, but it is the enabler that brings it to life.



Conclusion

Understanding the human point is an entirely new security paradigm. An approach rooted in securing technology has proven ineffective at minimizing threats; in fact, they are growing. It's time to think differently about cybersecurity to effectively prevent risks to critical data and IP. Only by understanding the intent behind a user's actions can we recognize the difference between good and bad cyber behaviors. And it's Forcepoint's goal not just to recognize that difference, but to provide intelligent systems that allow good employee behavior and facilitate business while stopping bad cyber behaviors.

Sources

[1] http://www.gallup.com/reports/199961/state-american-workplace-report-2017.aspx

[2] http://www.shrm.org/Research/SurveyFindings/Articles/Pages/Challengesinnext10Yrs.aspx

[3] http://www.ponemon.org/local/upload/file/AT%26T%20Mobility%20Report%20FINAL%202.pdf

[4] https://www.insight.com/en_US/learn/content/2017/01-16-2017-workplace-mobility-statistics-show-improved-productivity.html

[5] http://www.techproresearch.com/downloads/wearables-byod-and-iot-current-and-future-plans-in-the-enterprise/

[6] https://www.okta.com/Businesses-At-Work/2016-03/

[7] http://www.gartner.com/newsroom/id/3616417

[8] https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-37447

[9] http://www.gartner.com/newsroom/id/3638017

[10] https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked

[11] http://www.nature.com/news/how-to-hack-the-hackers-the-human-side-of-cybercrime-1.19872

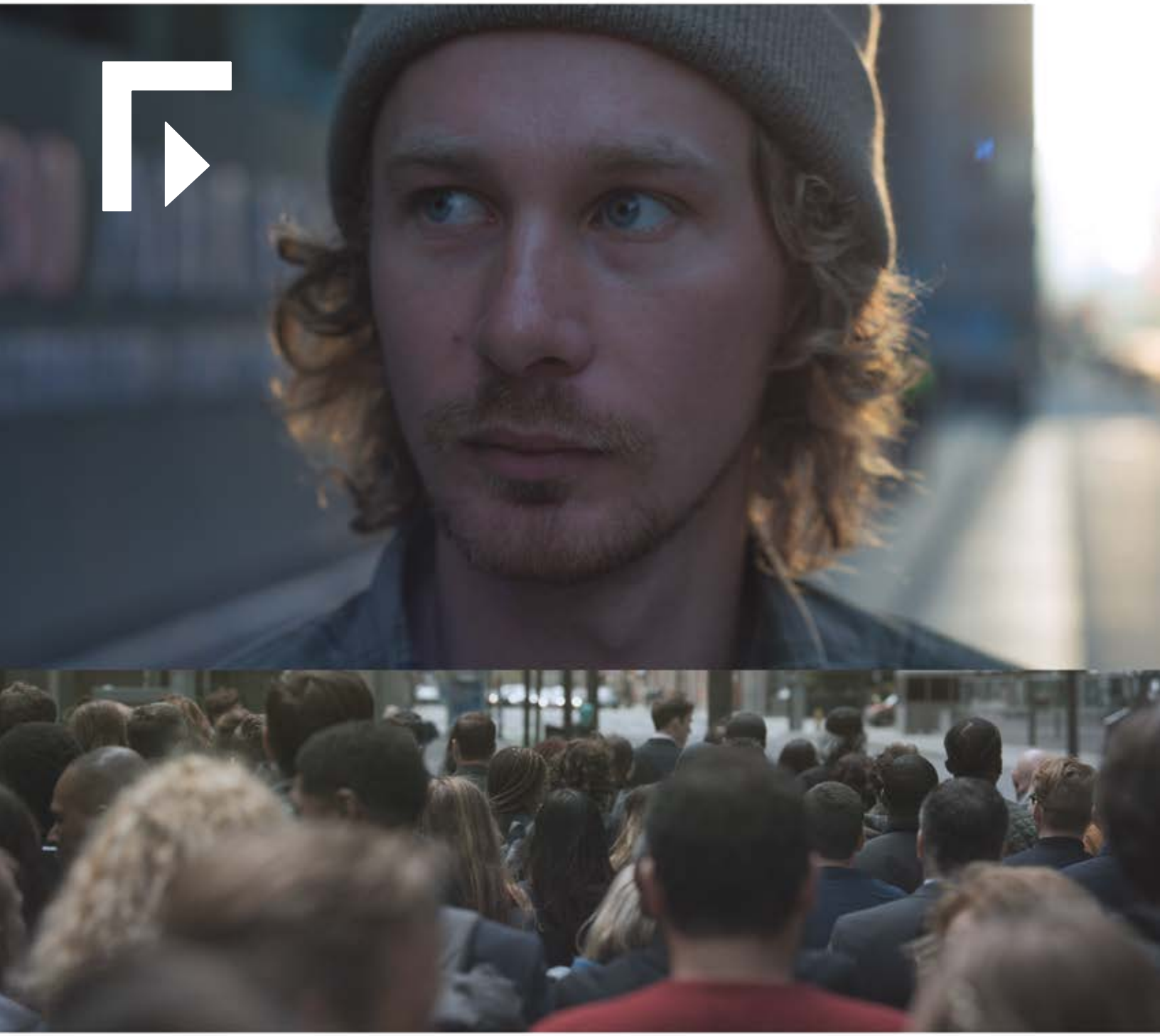
[12] http://assured-cloud-computing.illinois.edu/files/2014/03/Identifying-Compromised-Users-in-Shared-Computing-Infrastructures-a-Data-Driven-Bayesian-Network-Approach.pdf

[13] https://blogs.forcepoint.com/security-labs/carbanak-group-uses-google-malware-command-and-control

[14] Verizon 2016 Data Breach Investigations Report

[15] Ibid

[16] https://www.ic3.gov/media/2014/140923.aspx FBI Internet Crime Compliant Center Advisory: Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information, September 23, 2014



Forcepoint Headquarters
10900-A Stonelake Blvd., Quarry Oaks 1, Ste. 350, Austin, TX 78759
Tel: 1-800-723-1166 or 1-858-320-8000

www.forcepoint.com