

### 1. State of cybersecurity

To keep our organizations healthy and productive, we must ensure the security of our employees, data and intellectual property. Breaches continue to rise, even with a steady influx of cybersecurity investments, which are expected to top \$113 billion by 2020.<sup>1</sup>

<sup>1</sup> <http://www.gartner.com/newsroom/id/3638017>

### 2. The enablement challenge

Cloud services, BYOD policies and remote working offer flexibility to employees and lower organizational costs, but present complex and unfamiliar security challenges. These initiatives have evaporated the traditional security perimeter and make it difficult to maintain visibility into how data is used.

### 3. People are the constant

One thing is clear—cybersecurity has been too focused on locking down technology infrastructure, and to little or no avail. But while cyber threats and opposing security technologies have evolved over time, one thing hasn't—people.

### 4. Getting to the root of the problem

The point of interaction between people and data can undermine the most comprehensively-designed cybersecurity systems in a single unintentional or malicious act. Our ultimate vulnerability is not a form of malware; it's our unpredictable human nature.

### 7. Human-centric security with a comprehensive approach

This approach requires both intelligent systems and transparent collaboration between an organization's stakeholders. Protecting the human point—where people interact with critical business data and intellectual property—is an opportunity to truly protect employees, critical business data and IP.

### 6. The future of cyber focuses on people

Observing cyber behavior allows security professionals to determine a baseline for normal, which then makes it possible to identify the risky actions that lead to data loss. Understanding intent can differentiate an accidental insider from someone maliciously planning a security incident.

### 5. A much needed paradigm shift

Many of today's disastrous breaches come from inadvertent behaviors by good employees with no intention of harming their organizations. Security can be simplified through one realization: we are all insiders because we work with sensitive data inside the network.

# THE HUMAN POINT.

