The Forcepoint Advantage

FORCEPOINT

Today's Cybersecurity Challenge

In the era of digital transformation, the world's most successful companies lead their industries by monetizing their data and intellectual property. And protecting this data and IP from cyber theft or corruption is critical; losses can devastate profits and hard-earned brand reputations. CISOs and other executives tasked with security understand the stakes but their jobs are harder than ever before in today's new IT operating model that embraces public clouds, BYOD, and mobility. Data is now everywhere and can be accessed from anywhere.

Attack surfaces continue to exponentially increase, making it even harder to block threats. Traditional cybersecurity approaches that depend on stand-alone products were never designed for this new world.

But Forcepoint's human-centric approach is different. Our transformative, behavior-centric security dynamically adapts in response to the risk level that users' behaviors pose, providing security professionals a new path forward to proactively secure their data and users in today's everywhere, anywhere world.

> 60 percent of enterprise IT are off-premises and in the cloud.[1]

> Security and risk management leaders must adopt a continuous adaptive risk and trust assessment (CARTA) strategic approach. This is vital to securely enable access to digital business initiatives in a world of advanced, targeted attacks. It will enable real-time, risk- and trust-based decision making with adaptive responses.[2]
>
> Gartner Research, Top 10 Strategic Technology Trends for 2018

[1] https://www.idc.com/getdoc.jsp?containerId=US41883016

[2] Gartner, Top 10 Strategic Technology Trends for 2018, by David W Cearley et al., 03 October 2017.

Traditional Approaches Are at a Breaking Point

The typical approach to cybersecurity depends on the use of point products that do not interoperate. Disparate technologies work for single use cases, but the lack of integration amongst them results in an overwhelming number of alerts generated. Security teams are challenged with trying to distinguish one real threat from thousands of false alarms. By the time they've found it, substantial damage might have already occurred.

The overload of alerts is a symptom of a bigger problem: a reliance on a binary, threat-centric approach where "good" and "bad" activity can be addressed through static policies, but the intent behind the vast majority of remaining events that fall between the two ends of the spectrum is unknown. Without understanding the context behind activity, security teams must manually investigate each one. Taking a threat-centric approach leads to a no-win scenario.

:14
sec

A business falls victim to a ransomware attack every 14 seconds.[3]

$3.62
million

$3.62 million is the average total cost of data breach.[4]

What's more, cybersecurity teams seem destined for failure. It's estimated that over 80 percent of cybersecurity incidents exploit well-known vulnerabilities.[5] The way we do things today simply will not work in the future.

[3] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[4] Ponemon Institute, 2017 Cost of Data Breach Study

[5] SANS Institute, Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017

Why Human-centric Cybersecurity

More than 80 percent of hacking-related breaches exploit compromised credentials. Simple user and device authentication and authorization services are unable to monitor behavior and offer no control over data after access has been granted. It is also nearly impossible to defend against hackers who have compromised good employees by illicitly "owning their systems" with traditional cybersecurity methods.

Furthermore, good employees can make mistakes, unwittingly leading to data leakage. Sometimes, disgruntled employees may not have the best intentions.

Instead of trying to fully secure networks that are owned and managed by third parties, blocking various access points and making sense of an overwhelming number of security events, it is critical to understand the cyber behaviors of all users—from employees, customers and partners—as they interact with data and systems, to proactively assess the risk that their activity may represent.

The Leader in Risk-adaptive Protection

The legacy, event-centric approach to security no longer makes sense in today's complex cyber landscape. The most effective security is risk-adaptive, providing the context needed to dynamically apply the relevant policies, down to the individual level. And it's only through context that we can understand whether a particular identity or user's behavior is legitimate, risky, or malicious.

Forcepoint's risk-adaptive approach senses, analyzes and enforces—it protects your users, data, and networks in real-time and increases the efficacy of your security investments.

Unlike other systems, our solution does not flood your SIEM with alerts that need manual disposition. It makes it possible to know what normal, productive employee activity looks like and all the unique ways your people interact with data, automatically applying the right policies for their risk profile.

Simultaneously, it gives insight into where your data lives and travels, in and out of the organization. Our risk-adaptive model provides greater visibility, a single policy across distributed systems, rapid enforcement, and stronger compliance.

It’s Time for Human-centric Cybersecurity.

Who is Forcepoint?

Forcepoint was purpose-built to provide next generation cybersecurity solutions.

- One of the largest private cybersecurity companies in the world, with thousands of enterprise and government customers in more than 150 countries
- Leading supplier to global intelligence community and high assurance cyber missions
- One of the most comprehensive security product portfolios in the industry

The Human Point

By moving away from a threat-centric approach to cybersecurity, you can narrow your focus to the two true constants in security—people and data.

Protecting the human point means securing the intersection of people, critical data, and IP, which starts with understanding the rhythm of your people and the flow of your data. It makes it possible to know what normal, productive employee activity looks like and all the unique ways your people interact with data.

Forcepoint Dynamic Data Protection is an industry-first converged solution for next-generation DLP that delivers risk-adaptive protection. It combines Forcepoint's industry-leading DLP capabilities with a behavior-centric analytics capability to protect against data exfiltration. Dynamic Data Protection establishes a "normal" baseline of user behavior and applies a range of automated security countermeasures based on fluctuations in a user's risk score, all without administrator intervention.

Forcepoint Human-centric Portfolio

Forcepoint is converging its capabilities to simplify deployment and management of your security stack and eliminate security gaps. Each capability is best-in-class; you can start anywhere and expand as your needs grow. Our unified policy and common analytics and orchestration streamline management.

Forcepoint's solutions include:

Forcepoint Behavioral Analytics
User and entity behavior analytics for a zero-perimeter world. The leader in actionable insights based on risk-adaptive scoring.

Forcepoint DLP
Discovery and protection to meet regulatory and industry compliance.

Forcepoint Insider Threat
User visibility and incident context for sensitive data. The most comprehensive understanding of user intent, trusted on over 1 million endpoints.

Forcepoint CASB
Visibility and control over your complete cloud environment. The broadest cloud application support with unique customized risk assessment based on user behavior and data access classification.

Forcepoint SD-WAN & Next Generation Firewall (NGFW)
Highly secure, efficient and available network security. Cuts network expenses by 50 percent, reduces cyberattacks by up to 86 percent and slashes incident response time by as much as 73 percent.

Forcepoint Data Guard
Secure collaboration and information sharing for government agencies. Eliminates costly and time-consuming manual data transfers of highly-regulated, sensitive data.

Forcepoint Web and Email Security
Unified protection from advanced threats at any location, on any device. Threat detection is 100 percent with zero false positives.

Industry Recognition

A Gartner Magic Quadrant Leader in Enterprise Data Loss Prevention nine consecutive times.*

*Gartner, Magic Quadrant for Enterprise Data Loss Prevention, 16 February 2017. Formerly positioned as Websense in the Magic Quadrant for Content-Aware Data Loss Prevention and Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention reports. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: people's behavior as they interact with critical data and systems. This human-centric approach to cybersecurity frees employees to innovate by understanding the normal rhythm of user behavior and the flow of data in and out of an organization. Forcepoint behavior-based solutions adapt to risk in real time and are delivered via a converged security platform to protect network users and cloud access, prevent confidential data from leaving the corporate network, and eliminate breaches caused by insiders. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

forcepoint.com/contact

[CORPORATE-OVERVIEW-GLOBAL-BROCHURE-US-EN] 2000XX.022219

FORCEPOINT