WHAT IF THERE WAS A SECURITY BREACH... AND NOBODY CARED?

A SHIFT TO DATA CENTRIC SECURITY

accenture

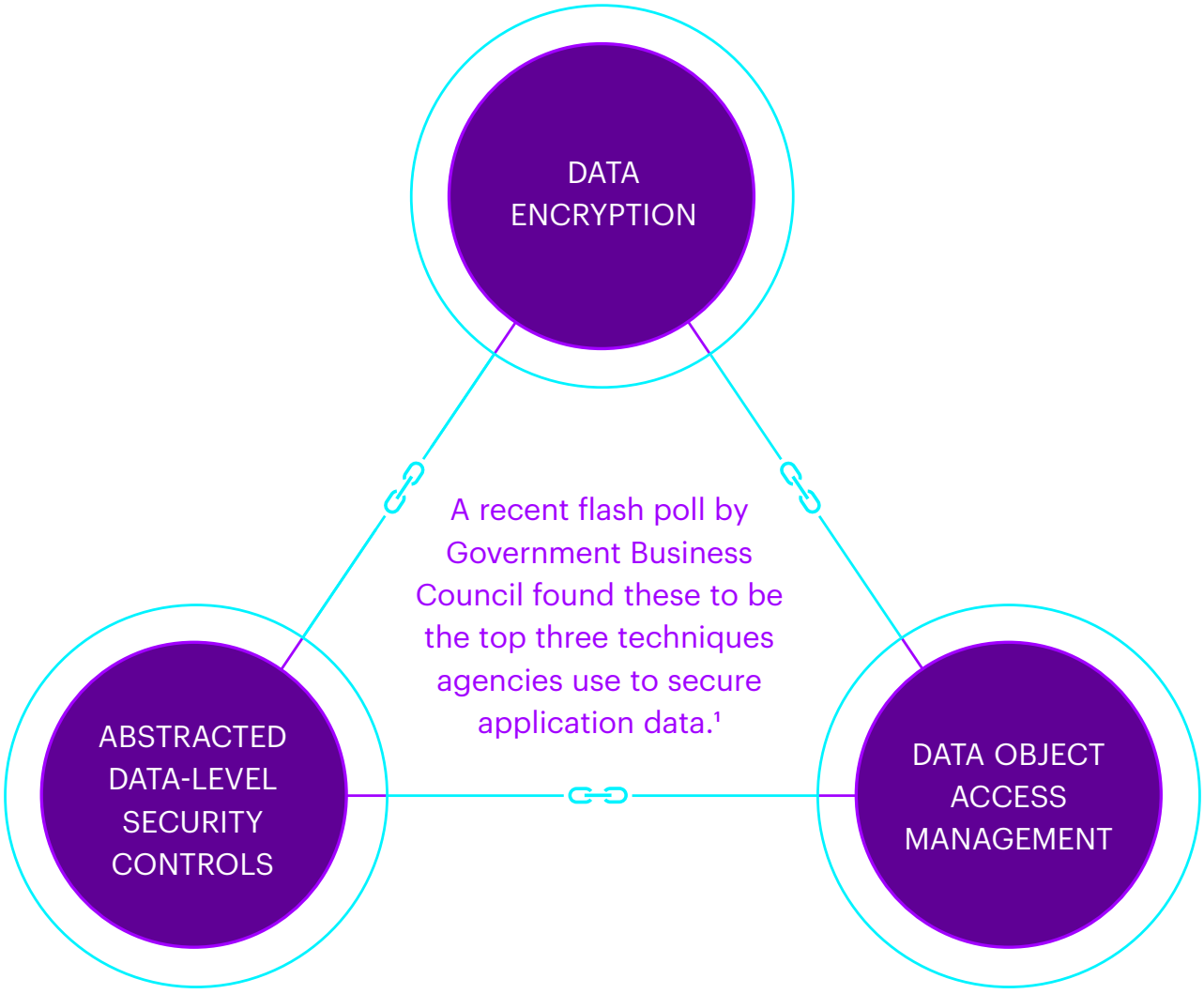
Imagine a scenario where an attacker breached the perimeter boundary and business continued as usual.

No televised news segment.

No newspaper article.

No walk down the long corridor to the boss' office.

It's a scenario that becomes a reality with a fundamental shift in security posture focused on data-centric security.



RE-IMAGINING CYBERSECURITY FOR THE 21ST CENTURY

Chief information officers (CIOs), chief information security officers (CISOs) and business leaders face a perfect storm of exponentially increasing volumes of data, types and quantity of devices, and velocity of threats.

Historically, the energy spent on securing data has been focused on building a better "wall." It's an approach that no longer works in today's perimeter-less world where some seven billion connected devices (one trillion by 2025[2]) have opened a liquid stream of data vulnerable to attack.

It is time to shift our security posture to focus on a liquid approach to cybersecurity—where strong, immutable identities, hardened data and an ever-changing polymorphic attack surface enable us to move beyond cyber resilience to a constant state of business operations.

THE PATH FORWARD

The shift to identity as the new perimeter requires a smart liquid security approach built on a dynamic platform that can keep pace with threats and easily adjust as the threats themselves change and adapt.

It demands a focus on data-centric approaches that harden and protect the data itself and ensure control over data, even after it has left the organizational boundary. This approach is achieved by embracing cloud technology and using the software-defined world to create constantly shifting, hard to find and self-healing attack surfaces that make it difficult for malware to gain a foothold.

We must focus the big data lens on internal and external behaviors and apply advanced analytics, artificial intelligence and machine learning to discover and act against threats in real time so that when the inevitable breach occurs, rapid detection, isolation and remediation without disruption of ongoing business operations becomes the norm.

Two important considerations:

1 Start where you are.

Remember, we got into our current cyber posture one system at a time, we will solve the problem the same way. The journey to a liquid security environment must begin wherever the organization is today. Which means applying a security layer to existing legacy systems while ensuring the security layer is agile enough to move forward as the environment evolves.

2 Build a culture of "security everywhere."

Security is everyone's problem—not just the CIO or CISO. Cybersecurity teams need leaders across the business to be vested in the liquid security journey and security must be built into all systems from the onset.

FOR MORE INFORMATION

Gus Hunt
Managing Director & Cybersecurity Practice Lead, Accenture Federal Services
gus.hunt@accenturefederal.com

NOTES

[1] Government Business Council, Flash Poll, September 2016

[2] http://blog.atollic.com/one-trillion-iot-devices-expected-by-2025-what-development-tools-to-use-for-development-of-internet-connected-iot-products

READ MORE

accenture.com/GusHuntQ&A

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 384,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE FEDERAL SERVICES

Accenture Federal Services is a wholly owned subsidiary of Accenture LLP, a U.S. company, with offices in Arlington, Virginia. Accenture's federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations.

Accenturefederal.com

@AccentureFed

Accenture-Federal-Services