

Identity is Security



It's a familiar story: a large enterprise experiences a data breach. 43% of the time, it's from an insider.¹ Other times, it's a negligent employee who's left a laptop out where they shouldn't. Or, it's an easy-to-hack password or default administrative username compromised by malicious actors. However, the breach ended up occurring and the result is the same: lost money, time and reputation, and the organization is left scurrying to catch up their defenses in time for the next attack.

To put this into perspective, in the first half of 2017, over 1.9 billion records were exposed in data breaches.² With many notable breaches occurring in the latter half of the year, it's very possible we could call 2017 the new "Year of the Breach."

So, What's the Problem?

The way we used to protect our enterprises is no longer enough. The network perimeter has dissipated. Employees no longer have to work within the corporate building, and simply putting a perimeter around that network cannot protect those working outside of it. Hackers have also become increasingly skilled at alternative methods by which to gain entry.

For example, security is the top priority for CIOs, and 88% of them plan to increase their spending over the next year. But, network security is fifth on the priority list. Identity governance, meanwhile, keeps increasing in priority and in budget.³ Clearly, security leaders are recognizing the paradigm shift in how their organizations are being targeted and accommodating for it.

55%

of CIOs are planning on increase their spending in identity solutions this coming year.³

¹ Infosecurity Magazine, *Insider Threats Responsible for 43% of Data Breaches*

² Gemalto, *Data breach statistics 2017: First half results are in*

³ Piper Jaffray, *2018 CIO Survey: IT Budgets Up; Security, Public Cloud, & Mobile Top Priorities*

Put simply, hackers have a new preferred method of entry: us. People are far easier to crack than a 512-bit hash. At any large organization, the number of entry points for a hacker is as populous as the number of users they let into their systems.

Many Paths to Entry

Part of the problem facing security leaders today is not just that each user in their infrastructure is a point of access, but there are also many ways in which that user can be manipulated.

Social Engineering

From Twitter and Facebook to LinkedIn and Whatsapp, a good portion of the population is active on social media. These networks have brought about a new age of communication and ease with which we can talk to each other. But, they've also opened windows of opportunity for each of us to say too much. Whether we're tricked into it by a malicious actor who nonchalantly asks "How is that last deal of yours doing?" or baits us into clicking a malware link after reading "Wow, these pictures of you are horrible," it's now very easy to give away information we didn't mean to. Sometimes, simple facts like relationships that are exposed through social media are enough for hackers to exploit you.

Phishing

Email is still the primary form of business communication for nearly all of us, but we're so inundated with messages that fake emails can be extremely tough to spot in the hubbub of the everyday. While the misspellings and almost-correct logos can give away some of the less advanced hackers rather quickly, other phishing attempts look just right enough to warrant a click. And it only takes one click for someone to open the door to a malicious party.

Employee Negligence

We've seen the headlines of laptops left where they shouldn't, or the infamous note under the keyboard containing all a user's passwords. But we're also still seeing things like credential sharing being a common – and dangerous – practice in today's organizations.



37%

of organizations are plagued with employees' poor password hygiene.⁴

It only takes one of these points of exposure to be compromised to cause problems. And with each point of exposure, there is a person – an identity – associated to it. More often than not, it's people that end up either causing or being responsible for loss of information, whether it is malicious or negligent in nature.

⁴ SailPoint, 2017 Market Pulse Survey

Not All Paths Lead to Security

Just as there are multiple ways for hackers to find their way in, organizations have built many methods by which to protect themselves.

Network Security

While it may not be a top priority for organizations to increase their spending or stack more firewalls on top of what they already have, it doesn't mean network security isn't still an important part of an organization's security infrastructure.

Endpoint Security

Devices such as smartphones, laptops and tablets are requirements of business today, and we have to continue securing them. But endpoint security only secures the data stored on those devices, and standard features include multi-factor authentication, encryption and automatic device wipes. It does not account for the policies for accessing sensitive data from smart devices or adding additional layers of validation to ensure the right person is accessing that data.

Data Security

Our data has shifted from being in data centers to the cloud, and we must evolve our methods to match the changing landscape. We're creating so much data – some of it incredibly sensitive – and saving it wherever we can. Structured systems like Oracle and SAP aren't the only places financial data lives anymore. It's in presentations, emails and the cloud. And all of it needs to be secured.

**IDG estimates
that by 2022,
93%
of all data will
be unstructured.⁵**

Identity

Identity management is at the center of security today, and it is a much larger and complex problem than just giving employees access to apps, systems and data. It is about managing and governing the digital identities that get access to sensitive data whether it resides in systems, cloud apps, or in files and folders.

Identity is Security

Some may believe identity is just about governing access to certain applications or systems in an enterprise. But identity is not just access; it's more than that. Identity goes beyond the network, but ties into both endpoint and data security. It takes information from every piece of an organization's security infrastructure and ties it all together.

⁵ DarkReading, *Unstructured Data: The Threat You Cannot See*

Enterprises have more systems, applications and data than ever before, and each part is interconnected. There are employees, contractors, suppliers, partners and customers. There are resources those users need to access. Each line of connection between each point in the massive web that is an organization's systems, applications and data has an identity attached to it.

Identity gives context to everything an employee, partner, supplier, contractor, etc. does to the entire enterprise infrastructure. Cloud and on-premises apps. Devices both on- and off-network. Privileged Access Management. Structured and unstructured data. With this context, your organization can see everything, govern everything and empower everyone.

The bottom line is: if the entry method of choice for malicious actors is the users that connect all your organizational resources, protecting those identities must be your security.

**SAILPOINT:
THE POWER
OF IDENTITY™**

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.