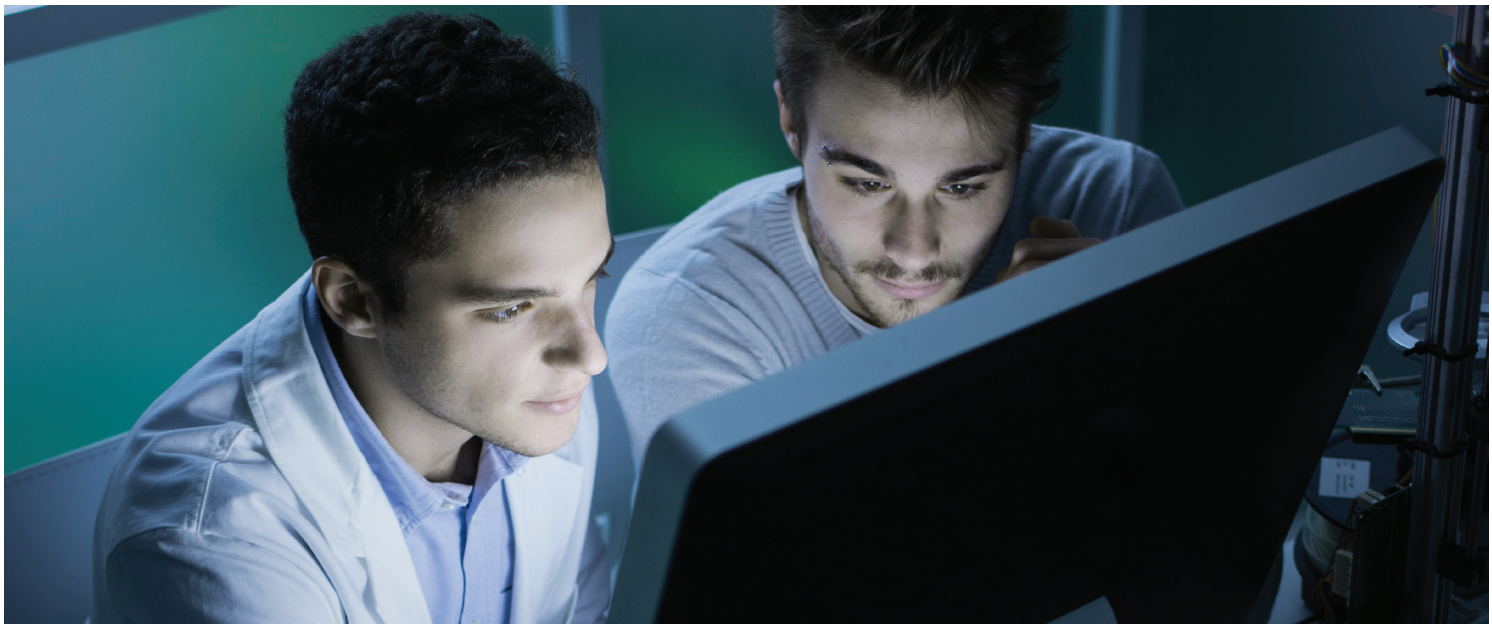
esentire®



Microlearning: Small Bites, Big Cybersecurity Impact

Six Must-Haves Every Organization Needs to Move the Security Awareness Training (SAT) Needle

An eSentire White Paper

Table of Contents

The times they are a-changin'

There's a major shift happening in the business world that will—and should—turn corporate Learning & Development inside out. In an era where businesses are subject to an increasing volume of cyber attacks, they must move from simply "training" employees to ensuring employees have the cybersecurity knowledge they need to do actually protect the business.

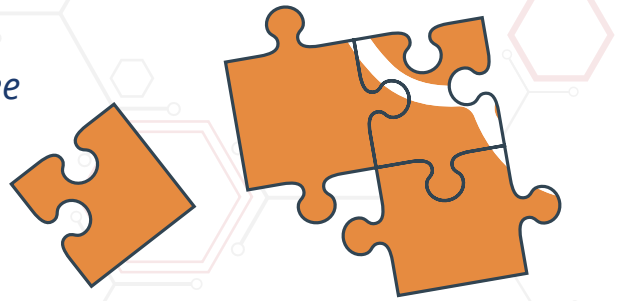
Traditional training approaches—whether in the classroom or via eLearning—have been providing lukewarm results for years. This just isn't good enough and it's showing: according to a recent report by Aberdeen Group[1], 49% of organizations say their main employee learning challenge is ensuring that what is taught is actually understood and can be applied. In the cybersecurity context, the ability for employees to apply knowledge gained in the day-to-day business workflows is critical to protect the organization from attack.

However, there have been huge strides made in both brain science and technology, resulting in a wealth of techniques and solutions that provide more impactful methods for improving employee knowledge.

Axonify, the platform upon which eSentire Training Day was built, has been delivering successful microlearning to organizations like Bloomingdale's, Walmart and Ethicon (division of Johnson & Johnson). This experience gives them the unique insight into what microlearning is, what it can be, and the opportunities it presents for your organization when it comes to arming your employees with the cybersecurity knowledge to protect themselves and your business.

When employees don't have the appropriate knowledge or can't recall what they've learned, they'll continue to fall victim to spear-phishing and social engineering attacks that could cost a business millions of dollars in damages.

One of the most important advances in employee knowledge approaches is microlearning —a technique that will totally change the face of cybersecurity awareness training in the corporate environment.



A quick look at the importance of Security Awareness Training

According to leading research analyst firm Gartner, security education is a rapidly growing market driven by increased regulations and a higher volume and diversity of threats targeting individuals. There is an increasing recognition that internal security departments are rarely able to produce effective security education or behavior management programs. The combination of increased risks and a lack of internal expertise pushes many IT leaders and Compliance Officers to seek Security Awareness Training solutions in the market that are capable of producing measurable improvements in employee security behavior. In order to support security objectives, employees require skills, knowledge and motivation. Security education focuses on developing secure employees who, in turn, enable security performance and regulatory compliance[9].

Despite extensive use of cybersecurity prevention technology such as firewalls, anti-virus and others to secure the organization, the reported number of successful breaches due to successful phishing and social engineering attacks continue to grow at an alarming rate.

Employees of an organization remain a significant vulnerability within most organizations. Phishing attacks are well researched, planned and targeted. Even skeptical users within an organization can fall victim to an attack if they aren't fully up to date on current tactics, and many more of the most senior employees in an organization don't realize they are a target. In fact, when we look at the results of hundreds of phishing campaigns that we've conducted across thousands of users almost 19% either clicked or opened an attachment contained in a spear-phishing attempt. A great deal of this can be overcome with a successful training program. However, training itself runs into a common set of problems when delivered via traditional methods. It is difficult to raise the priority on cybersecurity training when employees have never fallen victim, don't believe they're being targeted or they are too busy on a day to day basis to dedicate time to training. Therefore, the most common delivery model – either a face-to-face session, or Computer-Based Training (CBT) course – typically fail to reach enough employees because they don't attend, can't attend or they are remote mobile employees. For the employees that it does reach, the ability to recall the lessons learned decay over time – information goes into short term memory, and without use, doesn't make it to long term memory (use it or lose it). Within 30 to 60 days, employees lose all the knowledge they gained and will once again represent a vulnerability within their organization.

eSentire phishing campaign data reveals that 19% of employees either clicked or opened an attachment contained in a spear-phishing attempt.

Today's cybersecurity solutions don't address the biggest vulnerability – human nature, and the way humans learn. Well planned attacks not only know this, but count on it.

By understanding the principles behind knowledge retrieval and spaced repetition for learning, organizations can eliminate the problems associated with traditional approaches for security awareness training solutions and ensure that employees retain the knowledge they gain and can apply them in the real world to protect the business.

What is Microlearning?

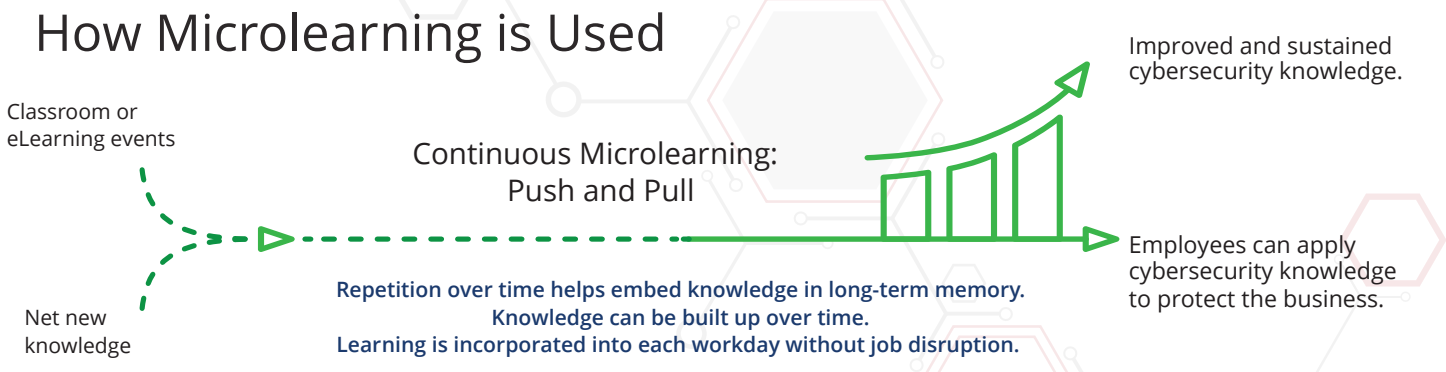
Microlearning is a technique of delivering learning content in short, bite-sized bursts (from three to five minutes), several times per week, or even daily. Neuroscientists have determined that we can only absorb four to five pieces of information into short-term memory at any given time, so by breaking it into short chunks, it's easier to understand and assimilate.

But this doesn't mean that microlearning is simply about creating 1-minute videos or putting short pieces of content into an LMS. For microlearning to work, it needs to:

- Include proven techniques for reinforcing content so that employees remember it and can apply it in practice
- Provide personalized and adaptive learning experiences
- Offer gamification to engage employees in ongoing cybersecurity learning
- Include modern social elements for collaborative learning
- Be accessible from multiple devices, including mobile
- Offer reporting and analytics that measure cybersecurity knowledge growth and effectiveness

When microlearning is delivered in a consistent, ongoing way, you have the ability to **drive continuous learning, build up knowledge over time**, and **produce real behavior change** that results in embedded human layer of security protection across every part of the business. Smart organizations understand this: Aberdeen Group's Best-in-Class companies are 60% more likely to consider microlearning to be effective for employee development[1].

How Microlearning is used

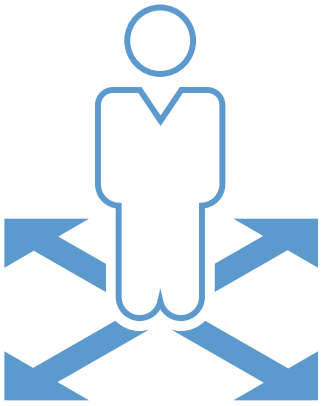


Why is Microlearning essential to Security Awareness Training?

Over the past few years, there has been a convergence of circumstances that have made organizations—and employee learning—ripe for change. Changing business requirements and a constantly evolving security landscape have altered what businesses need from their workforce to protect intellectual property, client information and critical data and assets. At the same time, employees are dramatically changing the ways in which they work and learn.

Increasing knowledge demands

All employees (whether they work in an office setting, retail floor or warehouse) must know more information than ever before to keep up with the growing number of attacks, risk and compliance requirements and more—this requires constant learning, but using existing training methods is proving to be cost and time-prohibitive and that's why today's security training solutions fail.



The failure of the LMS

While Learning Management Systems (LMSs) and other Computer Based Training (CBT) cybersecurity training solutions can deliver training to large groups of employees, they are ineffective. They simply replicate this flawed model of pushing maximum volumes of information at learners in the shortest possible time, which pretty much guarantees that employees won't learn and retain the material.

Traditional "one and done" training sessions—whether in the classroom or via eLearning— have proven largely ineffective in helping employees retain the knowledge they need. Traditional security and awareness training solutions like these are good enough to meet cybersecurity compliance regulations but are not good enough to protect your business from attack. Single-event training is highly susceptible to the "forgetting curve[3]," a proven cognitive science concept that has identified up to 90% of knowledge is quickly forgotten, unless reinforced.

Learning & Development specialists have also realized that traditional training—designed for long periods of concentration—doesn't have a hope of competing for the attention of today's modern learners whose attention spans are becoming shorter and shorter[4].

Changing needs to knowledge workers

Today's modern knowledge workers are a different breed: they have their hands full with deadlines, rapidly shifting roles and responsibilities and almost constant interruption. They're usually just too overwhelmed, distracted and impatient to sit through lengthy training sessions that could be mostly irrelevant. Instead they need learning that is current, easy to digest and accessible when and where they need it.

Based on Bersin's Modern Learner profile[2].
Today's knowledge workers are vastly different than they were even ten years ago, yet learning & development still largely focuses on that old profile.

Why you should adopt Microlearning to protect your business

Microlearning can be delivered to the desktop, on smartphones and tablets—in small chunks, where and when it makes sense for employees: on the job, at home, or while travelling. But microlearning offers far more than that:

- It adapts to the pace of today's business and meets the needs of your modern learners,
- Providing cybersecurity learning in short bites that are fast and easy to absorb. And because it's fast and easy, employees are more receptive to learning.
- Microlearning's short, fast bursts are highly suited to mobile environments, making it the preferred mode of learning for today's highly mobile workforce.
- It's far less disruptive to job performance: microlearning can be delivered in short daily bursts, which means employees don't need to spend hours away from their jobs to learn.
- Microlearning lets you use advanced learning techniques that help employees retain more of what they learn over the long term. This also has the benefit of enhancing the value of in-class or eLearning sessions by ensuring employees don't forget the cybersecurity knowledge that they learn.
- It helps reduce cognitive overload by delivering information in short, easy-to-understand chunks.
- Because microlearning breaks a topic into granular chunks, cybersecurity learning can be highly focused on what the employee needs to know, eliminating the need for people to sit through irrelevant training.

Six components of an ideal Microlearning platform for Security Awareness Training

While technologies exist for distributing and aggregating microlearning, they are not created equal. You can truly increase employee cybersecurity knowledge and achieve results by adopting a platform that not only delivers the proper cybersecurity microlearning content, but also employs techniques to ensure that the learning is effective and has a direct impact on your security posture.

1. Uses proven information retention techniques to ensure the most effective learning

The ideal microlearning platform should be based on proven neuroscience techniques that can have a dramatic impact on how much knowledge employees learn, plus how much of that knowledge they retain over the long term. Techniques should include:

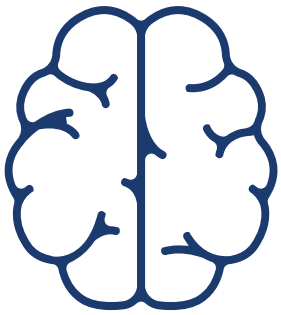
- **The Spacing Effect.** The spacing effect6 is the process of repeating information over time with specific time gaps between each repetition, which strengthens long-term knowledge retention.

- **Retrieval Practice.** Retrieval practice[5] is the act of quickly learning a concept, being tested on recall, refreshing the knowledge, and again being tested on recall. Research has proven that retrieval practice produces superior learning over conventional studying such as cramming, repeated studying, concept mapping and other study methods.

- **Confidence-Based Learning.** Research has shown that it's the combination of knowledge plus confidence that leads to appropriate behavior and empowers people to act—critical in areas like decision-making skills, as an example, when assessing an email to determine if it's a spear-phishing attack. Based on a 2-dimensional assessment model developed by Dr. James Bruno[6], confidence-based learning asks

employees to rate their confidence in the correctness of their answer, helping evaluate not only knowledge, but confidence in knowledge. With this deeper insight, organizations can more closely identify areas of learning employees should focus on, to achieve true mastery of cybersecurity knowledge and skills.

2. Embeds personalized and adaptive learning techniques for tailored learning



The ideal microlearning platform should provide for personalized learning where learning content can be customized for employees based on prior learning or benchmark knowledge, and methods of delivery. It should offer adaptive learning, which is a sophisticated learning technology that ensures employees are always progressing towards subject mastery along their own unique learning path. Adaptive learning:

- Continuously evaluates information from the learner during learning sessions (such as test and quiz answers, topics re-taken, and knowledge confidence levels, if tracked).
- Compares the learner data to initial benchmark information plus target knowledge levels programmed into the system.
- Adapts the learning path with modifications being made on the fly to subject matter and level of difficulty.

Aberdeen Group's Best in Class Companies plan ahead for employee knowledge transfer: 91% assess current knowledge/skill competency levels to determine gaps, versus all other companies at 39%[1]

3. Includes gamification for increasing employee engagement

Your microlearning platform should employ gamification techniques, which make learning more engaging and enjoyable for people of all ages. It should offer a variety of game interfaces for delivering learning, plus offer incentives such as leaderboards, reward points and team scores that encourage participation and achievement.

4. Offers modern social elements for collaborative learning

Because modern learners not only appreciate, but also expect a social learning environment, your microlearning platform should facilitate collaborative learning using a variety of social elements, such as user-generated and curated content, newsfeed, team competitions and surveys.

5. Supports multiple devices, including mobile, to ensure employee have access to learning

Learning should be accessible when and where it makes sense for employees—in the office, home office, or on the train.—via a desktop, shared terminal, or mobile device.

With the overall adoption of mobile learning growing by 20% since 2013, and up to 85% of people carrying smartphones[7], mobile learning is essential, allowing employees to gain cybersecurity knowledge where and when they desire. Aside from providing access over the Internet, your platform should also leverage a purpose-built app for smartphones and tablets, which meets today's modern learner preferences for speed, convenience and ease of use.

6. Provides a way to measure learning effectiveness and tie it to business results

Without the ability to measure learning, you can't determine if it's working. The ideal microlearning platform needs to incorporate the ability to track and measure cybersecurity knowledge growth, identify if knowledge is being applied and identify gaps to help employees become cybersecurity masters. This is the only way leaders can

determine if learning is having a direct impact on business.

When done properly, Microlearning works

Employees prefer microlearning

Employees prefer microlearning to traditional methods and voluntarily participate more frequently than traditional learning— especially when the learning is gamified. Estimates of traditional LMS participation are less than 20%, whereas the platform on which Training Day was built achieves participation rates of more than 80%. In addition, 80% of employees who use microlearning stated that they enjoyed learning this way and that they found it to be an effective way to learn[8].

Employees become more knowledgeable through microlearning

Employees who are learning on the platform see an average knowledge lift of 20% to 79%. In surveys, they've also indicated that the platform helped them in their job. The knowledge sticks.

Microlearning in action

While the term and the hype may be fairly recent, the technique of microlearning— delivering learning content in short, bite-sized bursts multiple times per week—isn't entirely new. The following innovators have been using microlearning to augment eLearning or deliver net new learning for the past three years. Although these organizations weren't using the platform in a cybersecurity training context, these examples point to the efficacy of microlearning in the corporate environment and serve to underscore the benefit of adopting this model to deliver cybersecurity training.

Microlearning at Bloomingdale's

Retail giant Bloomingdale's made the shift to microlearning in 2012 as a way to reduce safety incident rates, improve compliance, drive consistency of knowledge across the organization and improve learner motivation. They wanted a solution that was:

- Engaging for their four generations and multiple cultures.
- Integrated into the workday, which would leverage employee downtime and wouldn't take employees off the floor for long stretches of time.
- Measurable, identifying participation levels, knowledge growth, and impact on safety and retail shrink.

Since implementing microlearning, Bloomingdale's has seen a dramatic lift in employee confidence and has experienced a claim reduction of 41%, an annual savings of $2.2 million per year. The company has also discovered that associates who are not using the platform are three times more likely to have a worker's compensation claim than those who are using the system.

According to Chad McIntosh, VP of Loss Prevention & Risk Management at Bloomingdale's, ***"We have four different generations in Bloomingdale's—33% of which are millennials—so personalization is a huge factor for engaging our employees in learning. We've seen knowledge lifts of up to 20% in some subjects, and have achieved a dramatic decrease in preventable safety claims."***

Microlearning at Ethicon

A subsidiary of J&J, Ethicon is the world leader in the manufacturing of surgical sutures and wound closure devices. Like many organizations in the healthcare industry, the company was experiencing several challenges related to knowledge retention that impacted the performance of its sales team. Issues around increased product complexity, intensified customer demands and additional compliance requirements were negatively impacting both rep confidence and sales.

The company felt that microlearning was the best way to keep knowledge top of mind over the long term, monitor knowledge gaps, increase sales reps confidence in their knowledge, adjust to strategic priorities on the fly, and balance the need to learn with the need to sell. It supported their environment of constant change, with multiple generations and a mobile workforce.

As a result of implementing microlearning, Ethicon has achieved the following results:

- 90% voluntary participation
- 13% knowledge lift
- 81% of reps indicated they prefer the platform to other forms of learning
- 70% stated that they've increased their confidence in selling

According to John Knoble, Worldwide Director of Learning at Ethicon, being able to continuously reinforce major learning events to drive product knowledge every day has fundamentally changed the effectiveness of knowledge delivery to its sales professionals. ***"Not only are we seeing gratifying knowledge lifts, but we've found the sales reps' knowledge confidence increase, which is significant when it comes to selling our products."***

Microlearning at Walmart Logistics

Walmart Logistics, the distribution network for Walmart's global organization, wanted to take a fresh approach to safety awareness training that achieved high levels of voluntary participation and resulted in an improved safety culture and reduced incidents. They chose microlearning as the best way to accomplish these objectives and rolled it out to over 75,000 logistics employees.

Microlearning provided Walmart Logistics with a way to drive employee knowledge, while meeting several key requirements:

- Daily learning bursts to keep safety top of mind and to enhance learning retention
- A variety of learning games to appeal to multiple generations and keep the learning fun and fresh
- Fast and easy learning to avoid time away from work
- Personalized learning so that each learner could progress along a unique learning track
- Customizable learning modules to address safety issues at each Distribution Centre

No one in Walmart Logistics was expecting the types of results that the platform would provide. The company achieved a voluntary participation rate of more than 80%, a 54% decrease in incidents, along with a noticeable cultural shift.

According to Ken Woodlin, Vice President Logistics - Compliance, Safety and Asset Protection at Walmart, ***"We have seen tremendous improvement as a result of our associates' ownership and engagement in our safety programs, as well as leadership commitment to the program. Metrics like Lost Times have been reduced by over 50% in the past 3 years, and Incident Rates and DART rates are now well below industry average. Feedback about the system has been phenomenal, and we believe the process has been a significant contributing factor to our improved performance and engaged associate base".***

The eSentire Training Day difference

Training Day is the new approach to security awareness training that actually protects your business because it's built upon proven microlearning brain science.

	Face-2-Face	Traditional Online	TRAINING DAY
Meets cybersecurity compliance	✓	✓	✓
Works for busy corporate schedules	✗	✗	✓
Fun and engaging	✗	✗	✓
Improve and apply knowledge	✗	✗	✓
Automatically adapts	✗	✗	✓

Sources

[1] Aberdeen Group, December 2015.

[2] The Modern Learner: https://twitter.com/josh_bersin/status/542080404115947521

[3] Forgetting Curve definition: https://www.trainingindustry.com/wiki/entries/forgetting-curve.aspx

[4] Attention Span: http://www.statisticbrain.com/attention-span-statistics/

[5] Retrieval Practice Produces More Learning than Elaborative Studying with Concept Mapping, Jeffrey D. Karpicke and Janell R. Blunt. Science 20 January 2011

[6] Confidence Based Learning: http://www.uwex.edu/disted/conference/Resource_library/proceedings/09_20559.pdf

[7] Smartphone use: http://www.pcmag.com/image_popup/0,1740,iid=371072,00.asp

[8] Axonify end user survey, 2014

[9] Gartner Inc., 2015 Magic Quadrant for Security Awareness Computer-Based Training

About eSentire Training Day

eSentire® Training Day™ is a new adaptive, gamified, and fully-mobile Security Awareness Training (SAT) solution that uses small bursts of cybersecurity knowledge to more effectively arm your employees from the latest social-engineering, spear-phishing attacks and more. Training Day brings together best-in-class cybersecurity curriculum developed from attacks and techniques observed by eSentire's front line security analysts with the industry's most powerful knowledge-building platform, to transform your employees into a human layer of security protection.

About eSentire

eSentire® is a proven industry leader, keeping mid-sized organizations safe from constantly evolving cyber attacks that traditional security defenses simply can't detect. eSentire combines people, process and technology to deliver an unmatched, premium level service that detects, remediates, and communicates sophisticated cyber threats in real-time, 24x7. Protecting more than $3 trillion in Assets under Management (AuM), eSentire is the award winning choice for security decision-makers in mid-size enterprises. eSentire has received multiple accolades for exceptional service, including the HFM (Hedge Fund Manager) Service Provider award (2013, 2014, 2015, 2016). In 2015, eSentire was named to Deloitte's Technology Fast 50TM and Fast 500TM lists, and included in the 2015 "Cool Vendors in Cloud Security Services" report by Gartner, Inc.

The Axonify Platform

The cloud-based SaaS Axonify Platform is a unique approach to improving the knowledge and performance of employees. Axonify can complement your existing eLearning solution to dramatically improve knowledge retention and tie employee knowledge to on-the-job behaviors and performance; or function as a completely standalone knowledge and learning ecosystem.

Accessible using a web browser or the Axonify App, your employees have access to the learning and knowledge they need to do the job via a variety of media including video, audio, presentations and text. Supervisors and leaders can access individual or team results to provide critical coaching and support. Business managers and L&D professionals can quickly and easily access intelligence needed to establish learning program success and link specific learning programs directly to business results. Employee knowledge. Anytime. Anywhere. With any media. With Axonify, you have the ability to create a continuous learning ecosystem that drives sustainable knowledge and performance improvements.

Move beyond compliance - turn every employee into a cybersecurity ninja.

Contact eSentire today
North America: 1.866.579.2200
United Kingdom: 0800 044 3242
International: 1.519.651.2200
Email: info@eSentire.com

Learn more about Training Day: www.eSentire.com/training-day