beamsec

SOLUTION BRIEF

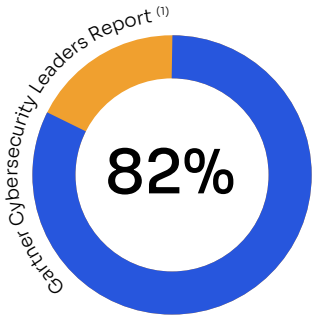
Build a rock-solid human firewall!

Introduction

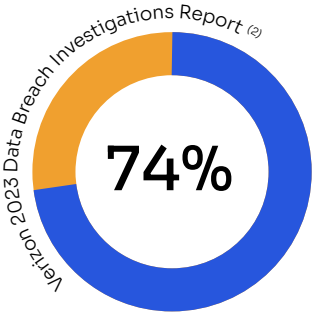
Cybersecurity threats have become increasingly sophisticated, with the capacity to adapt, hide their source, and precisely exploit vulnerabilities. They pose significant threats to organizations worldwide, more so than ever before, resulting in substantial financial losses, compromised sensitive information, disrupted operations, reputational damage, and even legal liabilities.

At BeamSec, we understand that the most significant battleground in cybersecurity is often the human element. Most security breaches begin not with a failure of technology, but with a well-crafted deception - a phishing email that appears legitimate enough to fool even the most vigilant employee. This is where BeamSec steps in. We don't just provide tools; we empower organizations to build a 'human firewall' - a workforce that is as aware and responsive to cyber threats as any technological solution.

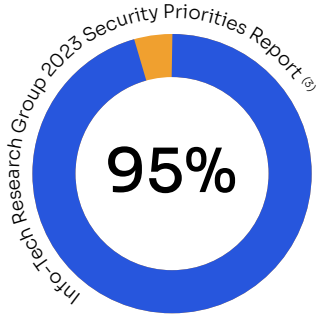
Our solution transcends traditional cybersecurity measures. We focus on fortifying the first line of defense - your employees. By equipping them with the knowledge and tools necessary to identify and counteract email threats effectively, we turn what is often seen as the weakest link in cybersecurity into its most robust asset. BeamSec's approach is comprehensive, combining cutting-edge technology with in-depth training and awareness programs to create a culture of cybersecurity resilience.



82% of data breaches were due to unsecure employee behavior



74% of data breaches include human element through error, misuse, stolen credentials or social engineering



95% of all security incidents investigated recognized human error as a contributing factor

(1) Gartner- 4 Ways to Achieve Secure Employee Behaviors **https://www.gartner.com/en/publications/employee-behaviors**
(2) Verizon - 2023 Data Breach Investigations Report **https://www.verizon.com/business/resources/reports/dbir/**
(3) Info-Tech - Security Priorities 2023 **https://www.infotech.com/research/ss/security-priorities-2023**

Key Challenges

1 The Rising Tide of Phishing Attacks

Phishing attacks remain a widespread threat, representing both the most frequent and damaging initial attack vectors. From an attacker's point of view, the technical barrier of phishing attacks is low; they can easily scale their operations and reach a global audience. Even a small success rate among millions of phishing emails can grant attackers access to your organization's network, bypassing all advanced security tools.

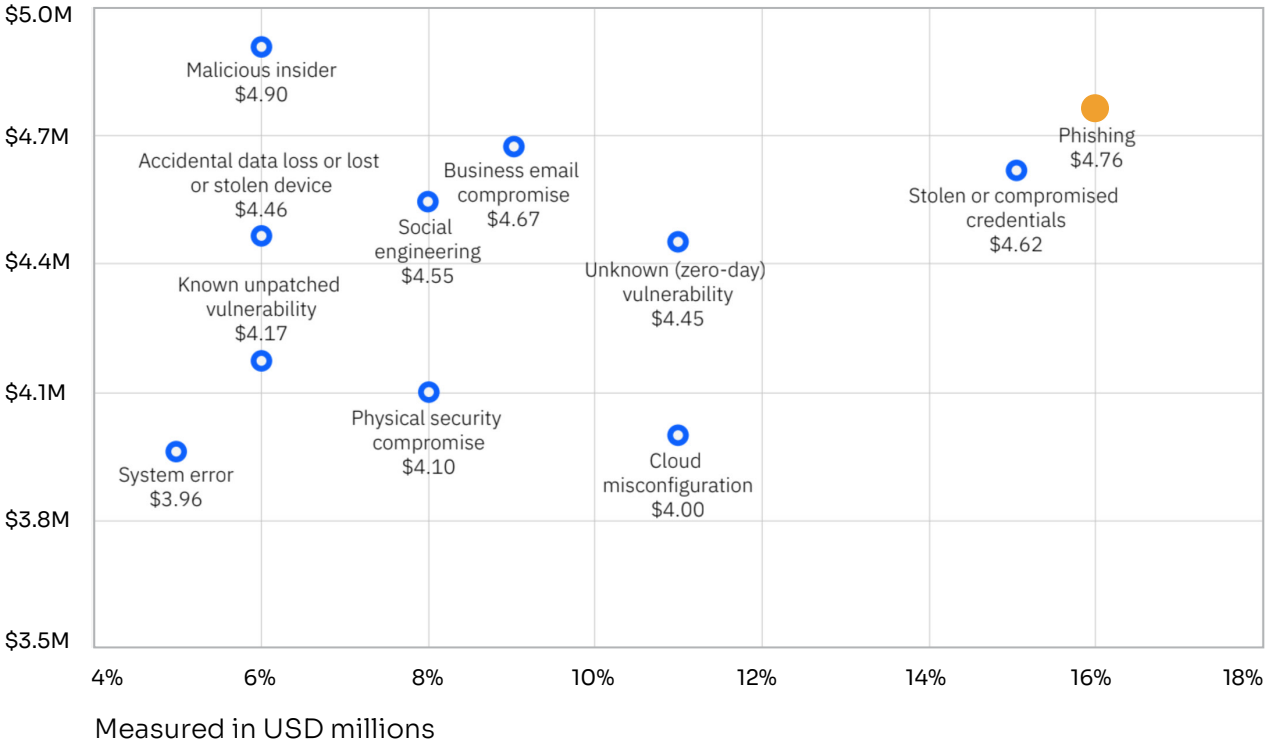
2 The Human Factor in Cybersecurity

Cybercriminals employ various manipulative tactics exploiting human psychology. They use social engineering tactics to trick employees into divulging confidential information or performing unsafe actions. Employees often struggle to identify phishing emails, rendering them susceptible to clicking malicious links or downloading harmful attachments.

3 Consequences of Security Breaches

Successful attacks can lock files, halt operations, and lead to substantial financial losses. Unauthorized access to sensitive data can result in significant data breaches, with long-lasting reputational damage and legal consequences, especially under regulations like GDPR and CCPA.

Cost and frequency of a data breach by initial attack vector (3)



Measured in USD millions

(3) IBM – Cost of Data Beach Report 2023

Discover the BeamSec Advantage

The Premier Partner to Elevate Your Cybersecurity to New Heights
BeamSec stands at the forefront of cybersecurity innovation, offering advanced solutions to safeguard against sophisticated email-based threats. Our proactive approach ensures our clients are always one step ahead.

What Sets BeamSec Apart

- **Accredited Cyber Security Lab**
Our state-of-the-art lab has received top accreditations, reflecting our commitment to excellence in product testing, security assessments, and managed services.

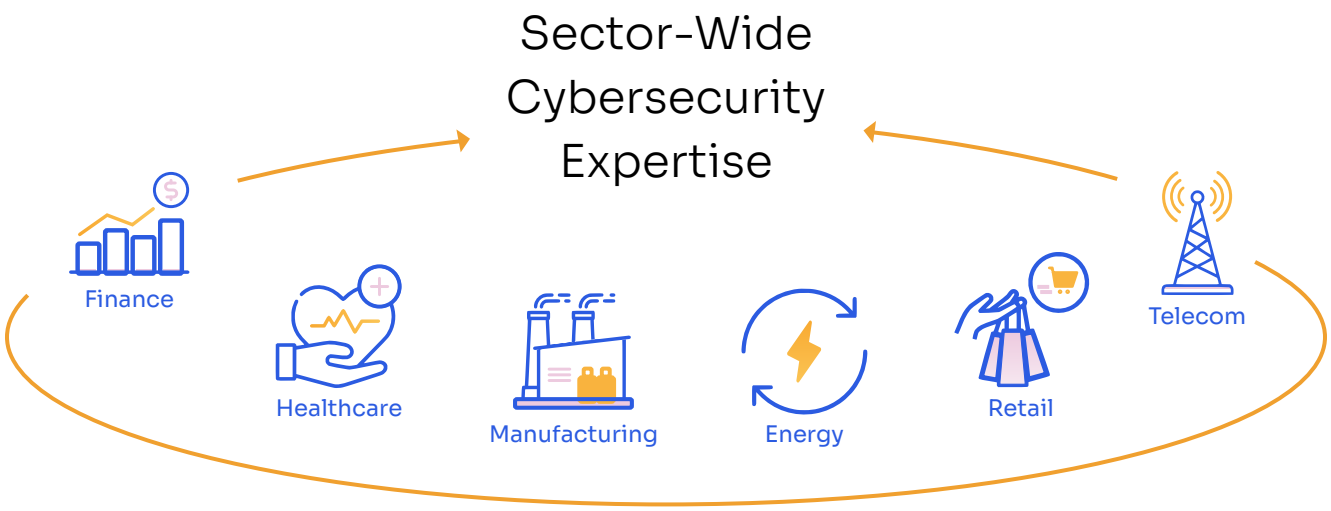
- **Industry Expertise**
Our experience spans hundreds of products and applications, enabling us to offer unparalleled insights into cybersecurity challenges across various industries.

- **Hybrid Deployment Model**
BeamSec's Hybrid Deployment Model offers the perfect balance of on-premises security and cloud flexibility, tailored to meet the specific needs of any organization.

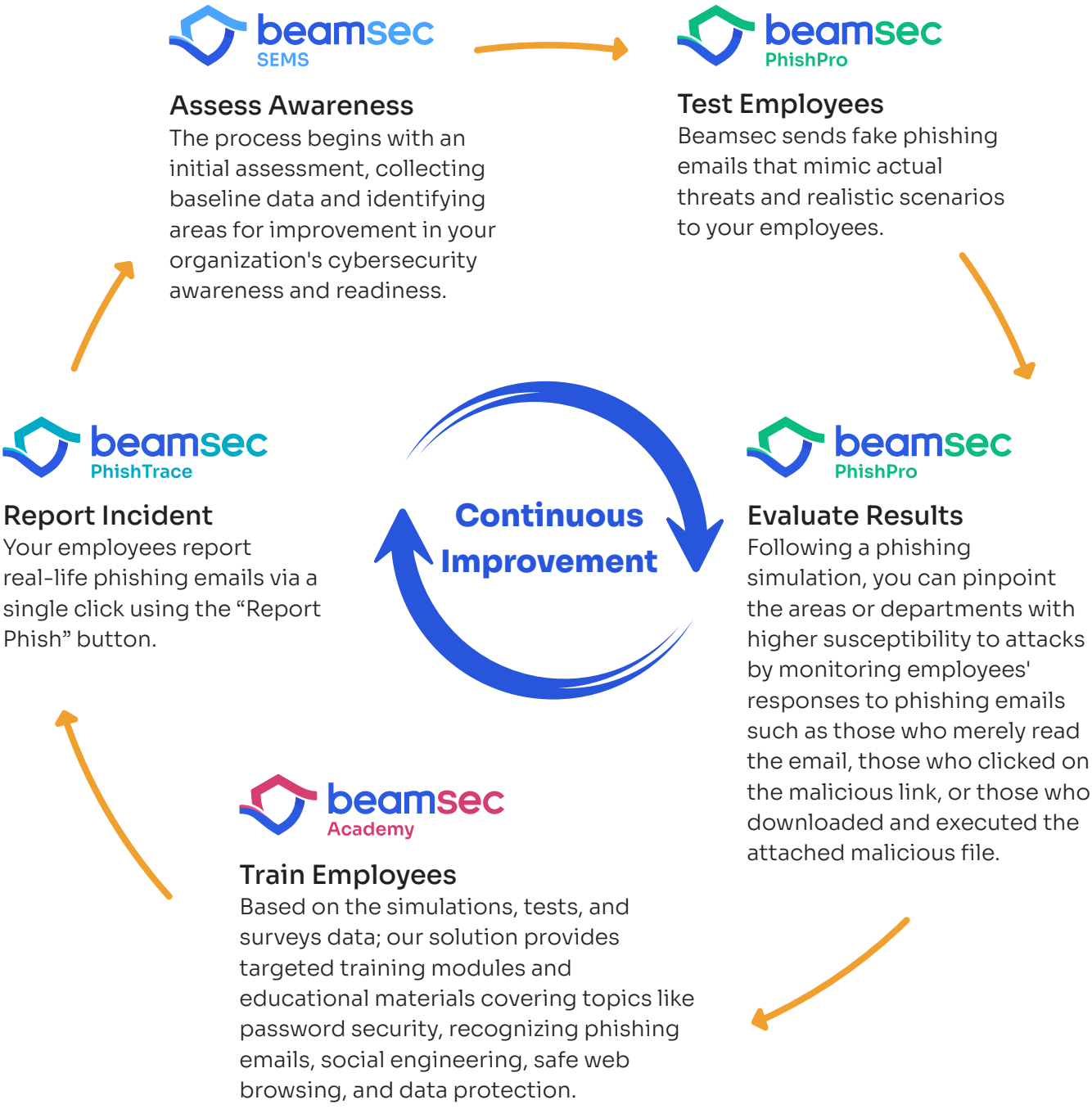
- **Scalable Solutions**
BeamSec's flexible solutions cater to organizations of all sizes, from SMEs to large enterprises, with seamless integration on-premises or via cloud services.

- **Inbound & Outbound Email Security**
We specialize in both inbound and outbound email protection, equipping your workforce with the knowledge and tools necessary for comprehensive email threat defense.

For more information on how BeamSec can transform your cybersecurity strategy, contact us.



How does it work?



Continuous Improvement

The process is iterative. Monitoring employee performance in training modules and simulations helps identify areas for improvement and measure the overall effectiveness of the training program. Ongoing awareness campaigns, including regular communication through newsletters, posters, and other materials, reinforce security best practices to keep cybersecurity at the top of your employees' minds. We provide updates to training materials and simulations to address emerging threats and vulnerabilities.

Benefits

Email security solutions in the market today all together have the capacity to identify and stop up to 92% of email attacks, implying that at least 8% of potentially harmful emails manage to reach your employees' inboxes. BeamSec's innovative approach to cybersecurity offers a range of tangible benefits that significantly enhance the security posture of organizations. Here's how partnering with BeamSec benefits our clients:

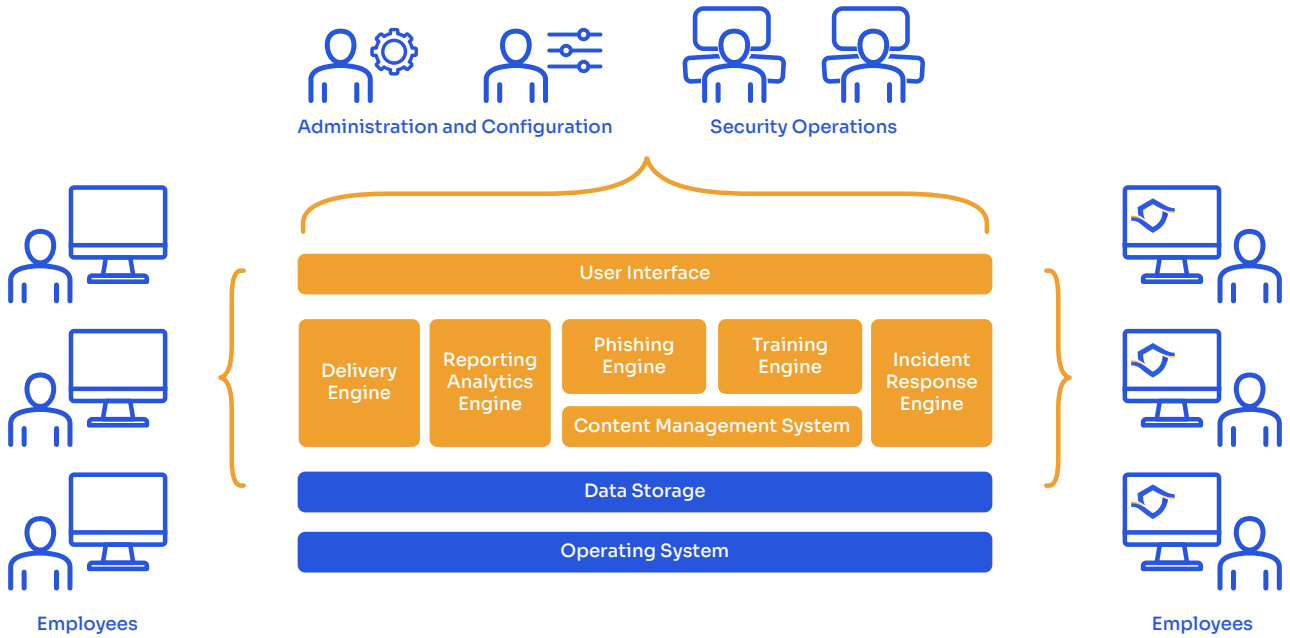
- **From Liability to Proactive Defense:** BeamSec transforms employees from perceived risks to vital assets in cybersecurity, actively contributing to threat detection and prevention. One of our government customers, after six months of training and phishing simulations, detection rates surged by 140%, showcasing an elevated awareness to identify suspicious emails.

- **Creating a Cybersecurity-Aware Workforce:** BeamSec training and simulations cultivate a culture of alertness, knowledge, and readiness to combat cyber threats. The employees of one of the leading regional Financial Institutes reported over 80% of phishing emails that reached their inboxes.

- **Compliance with Data Privacy Regulations:** BeamSec simplifies adherence to stringent regulations like GDPR and CCPA, ensuring many of our clients meet their legal obligations regarding data protection. Our clients used out-of-the-box reports simplifying the audit and compliance process.

High-Level Architecture

The high-level architecture of Beamsec Security Awareness and Training Solution involves various components and subsystems that work together to provide a comprehensive and effective product. Here's an overview of the key architectural elements:



Reporting and Analytics Engine

Collects data on user performance, simulation results, and incident reports. It provides administrators with insights into training effectiveness and areas for improvement.

Content Management System (CMS)

Content management system is used to create, manage, and deliver training and phishing simulation materials. Beamsec provides content updates to address emerging threats and allows you to adapt them as needed.

Incident Response

Enables your employees to report real-life phishing/suspicious emails with a single click to your organization's security operations team where they are analyzed, quarantined or deleted from all employees' inboxes if needed.

Delivery Engine

Delivery Engine manages the distribution of phishing simulations and training content to your employees.

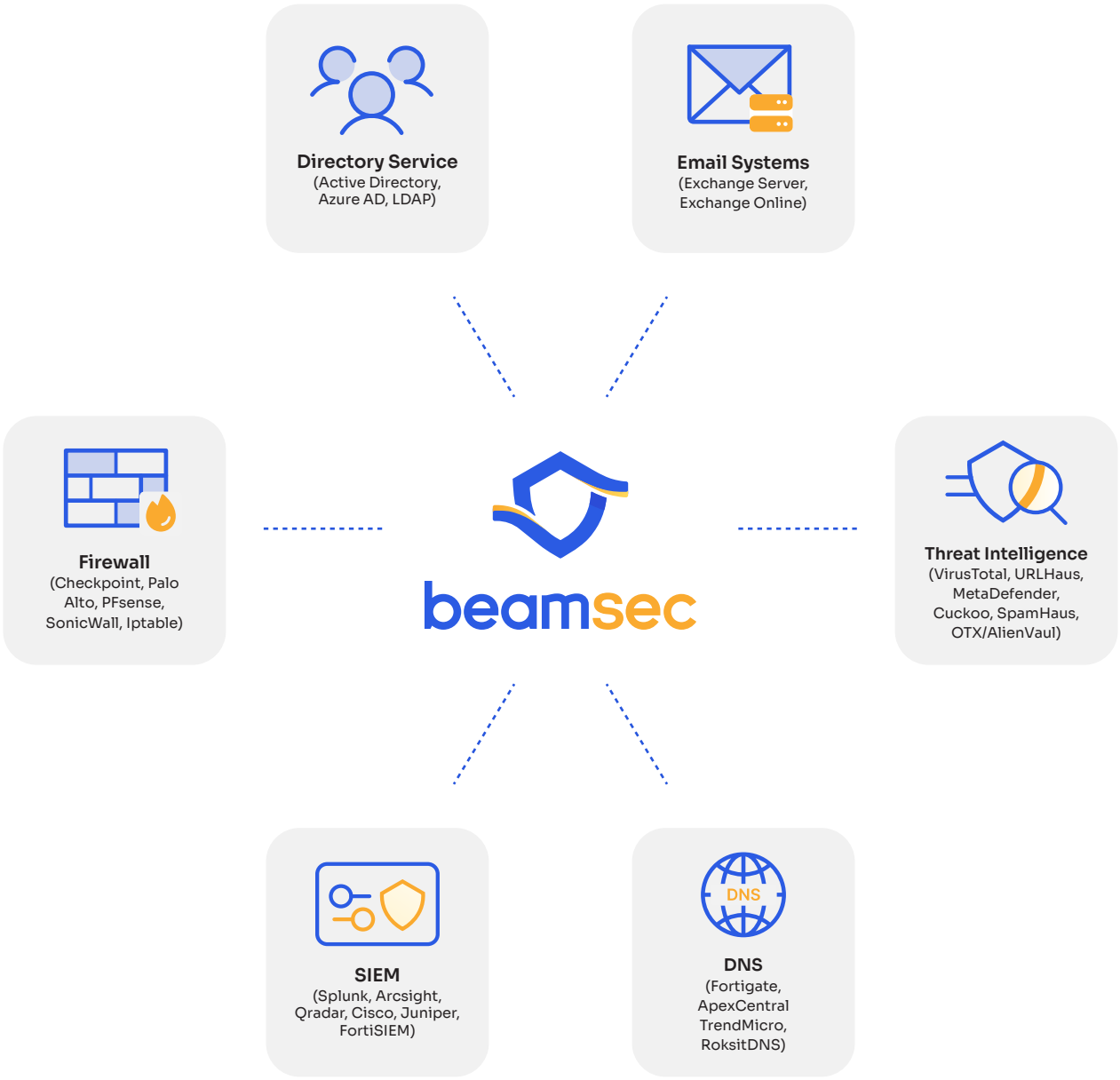
Training Engine

Training Engine manages and tracks training content including videos, games, quizzes, and written materials.

Phishing Engine

This component generates and manages phishing simulations, including the creation of realistic phishing emails and tracking employee responses.

Integrations:
Streamlining Cybersecurity Across Your Digital Ecosystem



BeamSec's integrations are meticulously designed to enhance your cybersecurity infrastructure seamlessly. By integrating with a variety of key systems and services, BeamSec offers a unified and fortified cybersecurity posture, ensuring that all components of your digital ecosystem work together to protect against threats.

Key Integration Benefits

Directory Service Integration

Streamlined User Management: Integrates with Active Directory, Azure AD, and LDAP for seamless user access control, ensuring that security training is targeted and relevant.
Automated Role-Based Training: Assigns tailored training materials and phishing simulations automatically based on user roles, enhancing the effectiveness of security education.

Email Systems Integration

Real-Time Training Delivery: Synchronizes with email systems like Exchange Server and Exchange Online to deliver training content and feedback promptly, reinforcing learning immediately following simulated phishing attacks.
Incident Response and Reporting: Enables employees to report phishing attempts with ease, facilitating quick action by the security team to isolate threats.

Firewall Integration

Enhanced Network Security: Compatible with various firewall solutions (e.g., Checkpoint, Palo Alto), BeamSec enhances your organization's defense mechanisms against external threats, creating a robust barrier against cyber attacks.

Threat Intelligence Integration

Comprehensive Threat Awareness: By linking with threat intelligence tools (e.g., VirusTotal, MetaDefender), BeamSec ensures that your cybersecurity measures are informed by the latest threat data, maintaining a proactive stance against potential attacks.

SIEM Integration

Advanced Monitoring and Analysis: BeamSec's collaboration with SIEM tools (e.g., Splunk, Arcsight) provides deep insights and analytics, enabling sophisticated threat detection and response.

DNS Integration

Proactive Web Defense: Partners with DNS services (e.g., FortiGate, TrendMicro) to preemptively block access to malicious sites, safeguarding your network before threats can materialize.

Deployment Models: Seamlessly Integrating BeamSec into Your Operations

The high-level architecture of Beamsec Security Awareness and Training Solution involves various components and subsystems that work together to provide a comprehensive and effective product. Here's an overview of the key architectural elements:

Software as a Service (SaaS)

Instant Activation:
Upon subscription, BeamSec's SaaS model is ready to 'plug and play' with your current systems, offering immediate protection with no installation delays.

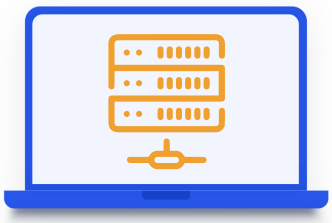
Integrated Functionality:
Works cohesively with the integrations outlined in our solution, such as directory services and email systems, providing a seamless transition and immediate enhancement to your cybersecurity capabilities.

What 'Immediate' Means:
The term 'immediate' refers to the swift enablement of BeamSec's features upon deployment. Users can expect to start utilizing BeamSec's tools and services without the lengthy setup times typically associated with new software integration.

Deployment in Action

Rapid Deployment:
Whether it's the SaaS model with its cloud-based agility or the on-premises solution with its in-depth customization, both deployment models are engineered for quick setup and immediate action.

Operational Readiness:
BeamSec ensures that the deployment process is as straightforward as possible, with comprehensive support and guidance, so that your cybersecurity is up and running with full functionality without unnecessary downtime.



Self-Managed (On-Premises)

Full Control:
The on-premises model places BeamSec within your own network infrastructure, offering you complete control over the deployment and management of the cybersecurity solutions.

Tailored Integration:
This model allows for a customized setup that aligns with your specific IT environment and integrates with existing SIEM, DNS, and Threat Intelligence platforms as depicted in the provided visual diagram.

Clarifying 'Works Immediately':
In the context of on-premises deployment, 'works immediately' signifies that once the setup is complete, the system is ready for instant use, with all integrations active and operational to support your cybersecurity measures from day one.

Ensuring Integration Harmony

BeamSec's deployment models are crafted to align with the array of integrations detailed earlier. Each model is designed to capitalize on BeamSec's central role as the nexus of your cybersecurity strategy, ensuring that regardless of the chosen model, the integrations function cohesively to fortify your organization's cyber defenses.

About BeamSec:
Transforming Cybersecurity Awareness and Email Security

At BeamSec, we're more than just a cybersecurity solutions provider; we're your strategic partner in navigating and neutralizing the ever-evolving landscape of email-based cyber threats. Our holistic approach transcends traditional defense mechanisms, focusing on empowering your organization's greatest asset in cybersecurity: its people.

Why BeamSec Stands Apart

A Holistic Approach
We believe that a comprehensive cybersecurity strategy involves more than just technological solutions. It's about creating a culture of awareness and resilience, where every employee is equipped with the tools and knowledge to act as a first line of defense against cyber threats.

Innovation and Expertise
As a subsidiary of BEAM Teknoloji, an accredited Cyber Security Testing and Evaluation Laboratory, we bring a wealth of expertise and a track record of excellence in cybersecurity. Our services range from formal product certification and security assessment to penetration testing and managed security services, catering to a wide array of industries.

Commitment to Continuous Learning
The heart of our innovation lies in our dedicated Research Lab. Here, we're relentlessly exploring and decoding the latest threat vectors and attack strategies used by malicious entities. This commitment ensures that our suite of products is not only up-to-date but also anticipatory of emerging threats.

Our Mission

Our mission is to transform the way organizations perceive and handle email security. We aim to shift the narrative from viewing cybersecurity as a technical challenge to recognizing it as a fundamental aspect of organizational culture and human resource empowerment. By doing so, we seek to elevate the overall security posture of organizations, turning potential vulnerabilities into robust defenses.

Our Vision

BeamSec envisions a digital landscape where organizations can communicate freely, securely, and with complete confidence. We're dedicated to creating solutions that not only protect against current threats but also adapt and evolve to meet future challenges, ensuring that our clients are always one step ahead in the cybersecurity game.

Our Commitment

We are committed to delivering excellence and innovation in every aspect of our services. From the initial assessment to continuous training and improvement, our focus is on providing not just tools, but comprehensive solutions that empower organizations to effectively defend against and mitigate cyber threats.

beamsec

Contact Us

To learn more about how BeamSec can revolutionize your organization's cybersecurity, contact us.

BEAMSEC LIMITED
Britannia House, 11 Glenthorne Road, London,
United Kingdom, W6 0LH

hello@beamsec.com

https://www.linkedin.com/company/beamsec/