

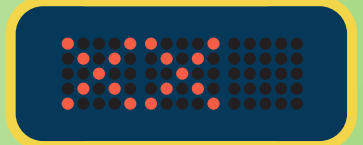
# Clearedin

PHISHING SECURITY



Five Unique Advantages over Existing SEGs and Simulated Attacks to Field a Complete Layered Defense

**\$1.6M** Average Cost of a Single Spear Phishing Attack



Over **60%** of Breaches Target Privileged Enterprise Credentials

according to 2020 Verizon Research

## 2. Dynamic blacklists and whitelists

### SOLVES: PROTOCOL-SPECIFIC LIMITATION

Clearedin's unique Identity Trust Graph stops or vastly limits phishing far beyond - 15% or better - typical SEG batting average. Protocol-specific, contextual guidance is used during the moment of the actual attacks providing end users information on the exact next pitch before the ball leaves the pitcher's hand.

**95%** of All Enterprise Attacks Include Successful Spear Fishing

## 3. Real-time, user-specific protection across increasingly popular chat, video, file collaboration

### SOLVES: ARTIFICIALLY HIGH SENSE OF ENTERPRISE PROTECTION

Protocol dependency is akin to a SEG-style batter offering one-dimensional single hits. Unfortunately, the enterprise lacks protection across increasingly popular Chat, Video, File Collaboration. Clearedin solves these SEG shortfalls and scales across email plus all popular collaboration channels like Teams, Zoom and Google Workspace.



**50%** Increase in Microsoft Teams Usage in 2020: 115 Million Users

## 1. Deep User Behavior Analytics (UEBA) bench offers enterprises a learning model

### SOLVES: NO VISIBILITY TO SUPPLY CHAIN IMPERSONATION

Supply Chain Impersonation is often invisible to SEGs. Vendor-compromised domains are often "on deck" as ATO common phishing origins. SEGs fail to go deep into the dangerous phishing line up. In contrast, Clearedin's Deep User Behavior Analytics (UEBA) bench offers enterprises a hands-on learning model. Enterprises gain Clearedin's platform capabilities of more intelligent and incisive learning.

Phishing Pinpointed in **81%** of Social and Malware Attack Vectors

according to 2020 Verizon Research

Only **3%** of Users Report Phishing Emails

## 4. Eliminate SOC fatigue and help enterprises prevent multi-collaboration phishing

### SOLVES: AUTOMATION MAKING SEGs DIFFICULT TO INSTALL, LEARN OR CONFIGURE FOR ENTERPRISE CUSTOM ROUTING TABLES AND NETWORKS

SEGs are difficult to install, require constant training that is often ignored, and often takes months to properly configure for enterprise custom routing tables and network configurations. Clearedin takes a cloud-native approach and installs in hours using server-side API integration. Automation and an identity trust graph prevents phishing attacks from reaching home.



## 5. Customizable banner with context to all email, collaboration

### SOLVES: STATIC REPORTING OF PHISHING ATTEMPTS BY SEGs

By knowing the velocity of an attack, Clearedin offers a dynamic banner with context to all email, collaboration and is fully customizable, including:

- Impersonation protection
- New domain coverage
- Geo-insight including sender IP from wrong locations or domains
- Company logo replacement
- Protection against an entire attack team of Spear phishing, Whaling, Catphishing and Clone phishing



*Clearedin delivers major league collaboration phishing security!*