Elevate Security

Elevate Security for Account Compromise

The Problem

The 2021 Verizon Data Breach Incident Report paints a clear picture of the root cause of thousands of incidents and breaches. For the past decade, the tactics used by attackers have remained largely unchanged.

A recent research study by Cyentia Institute revealed the following:

- The current approaches of training and phishing simulations for protecting employees **have made little impact**
- While a single individual may not be have had their account compromised, at a department and organizational level, there is a **100% likelihood it will happen**

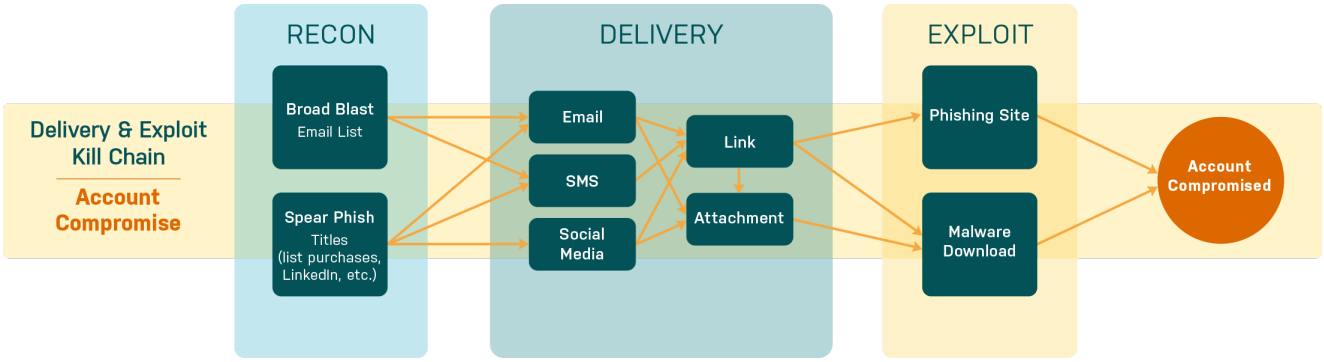
This leaves industries as diverse as Technology, Finance and Biotech equally at risk. Corporate firewalls are no longer adequate protection from the threats of stolen customer data, financial losses, or IP theft. Identity is the new perimeter.

With this sobering insight, it's clear that enterprises like yours should **extend Zero Trust beyond just your networks, but also your employees and other end users**.

How can you know which end users are the largest security risks and which are not? How can understanding of your riskiest users help in provisioning or revoking identity & access privileges? Can you measure the level of human risk inherent in your remote WFH workforce?

Elevate Security

The Account Compromise Kill Chain



To understand how to defend your end users against these attacks, we first need to understand how an attacker works to get to their ultimate goal.

The account compromise kill chain follows some typical steps:

1 Recon

The attacker identifies their targets. This can be broad blasts to a list they've purchased or spear phishing of specific names

2 Delivery

The attacker chooses how to deliver their attack to their victim(s); this could be through an email, SMS, or website, compromised or not). Inside the delivery is typically a link to a website or an executable with an enticing reason to download it

3 Exploit

If the victim clicks the link to the phishing site or executes the malware, the attacker can take over that user's account

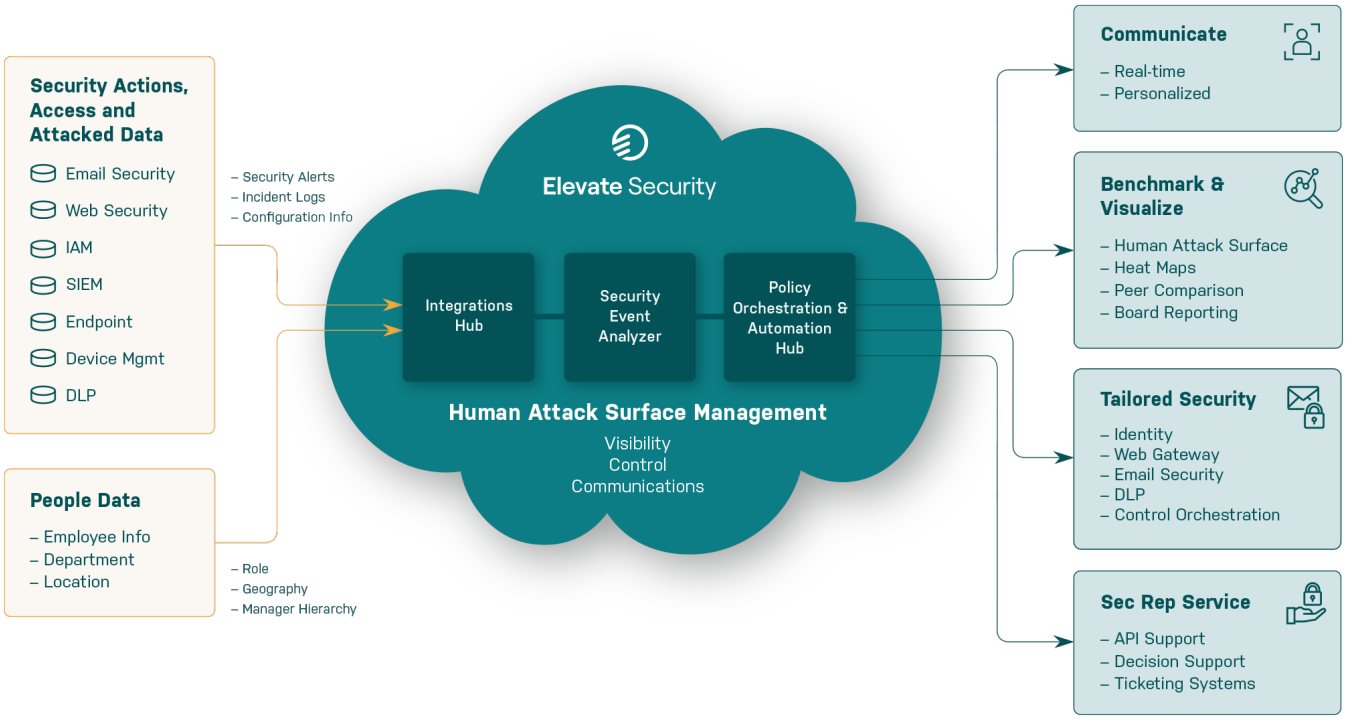
Enterprises typically have technology in place to defend against these steps, yet breaches still occur. Attackers circumvent your email security tools, web security gateways, endpoint security solutions, and identity platforms. Clearly bad actors have figured out how to bypass these safeguards and compromise your last line of defense–your users. This is where Elevate can help.

Elevate Security

The Solution

Elevate Security Platform: A Solution for Account Compromise

Elevate Security Platform helps your organization to defend itself against account compromise.



Our solution delivers visibility and control over your human attack surface, which is the sum total of user actions, access, and security controls that put your organization at risk. Your security team will understand which users are at greatest risk and most likely to fall for an account compromise attack. We help you to disrupt the likelihood of account compromise success, keep all necessary controls up to date automatically, and actively manage your account compromise posture over time. Think of it as Zero Trust for your end users. Everyone receives the right level of protection commensurate with their risk

Elevate Security

Elevate Security Platform Guards Against Account Compromise with 5 Key Functions:

Visibility

We build individual risk profiles of every user in your extended enterprise and their likelihood to fall for an account compromise attack, giving you the power to determine where Zero Trust implementations are most needed.

Employee Feedback & Executive Communication

Automated notifications warn your riskiest, targeted users to be on the lookout for phishing or malware attacks, so they can stay on their toes and receive direct feedback when they've made a mistake.

Control Orchestration

We automate the workflow of creating risk-appropriate profiles for targeted individuals. Tailored Security Controls can be tightened or loosened by Elevate pushing updates to email, web gateways, endpoints or identity solutions as needed.

Decision Support

The Incident Response team, Helpdesk, and security analysts receive insights into human risk to make educated and defensible decisions.

Continuous Improvement

You can re-evaluate your account compromise risk posture continuously, tracking the effectiveness of your tool and technology investments.

Protect your risky, targeted end users... while relaxing security around the best. Zero Trust for employees.

About Elevate Security

Elevate Security, the leader in human attack surface management, was founded in 2017 by two former Salesforce security executives to address one of cybersecurity's biggest unsolved problems – human error. The Elevate Security Platform offers an intelligent, customized and automated platform that ingests the entirety of an organization's security data to gain benchmarked visibility into human risk, enabling customers to proactively tailor security controls and create 'safety nets' around the riskiest employees. Armed with the insights and controls from the Elevate Security platform, CISOs are in a much better position to support high-growth initiatives within the enterprise while securing and defending the human attack surface. Elevate Security counts leading enterprises in industries – from financial services to technology and healthcare – as customers.

For more information, visit: https://elevatesecurity.com/

Elevate Security