



Hunt Down Human Risk

Powerful Insights for a
Minimized Attack Surface

February 28, 2024



What is Human Risk Management (HRM)?

Forrester Definition, Q1 2024:

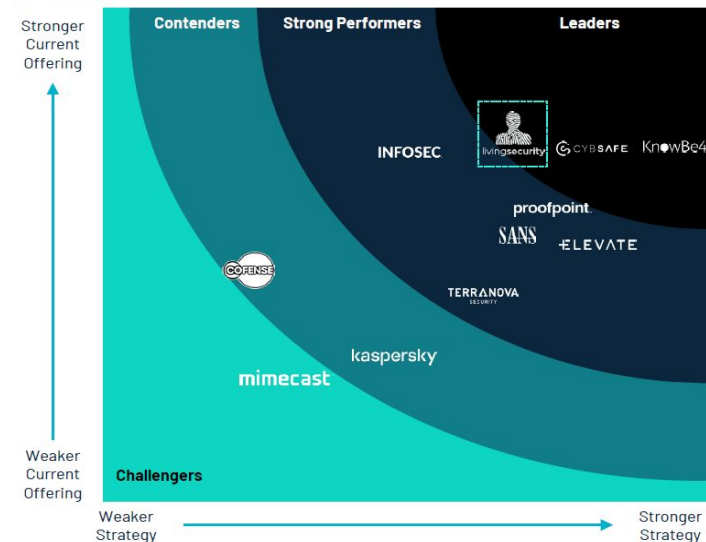
Solutions that manage and reduce cybersecurity risks posed by and to humans through:

1. Detecting and measuring human security behaviors and quantifying the human risk
2. Initiating policy and training interventions based on the human risk
3. Educating and enabling the workforce to protect themselves and their organization against cyberattacks
4. Building a positive security culture

Industry Leading HRM Solution

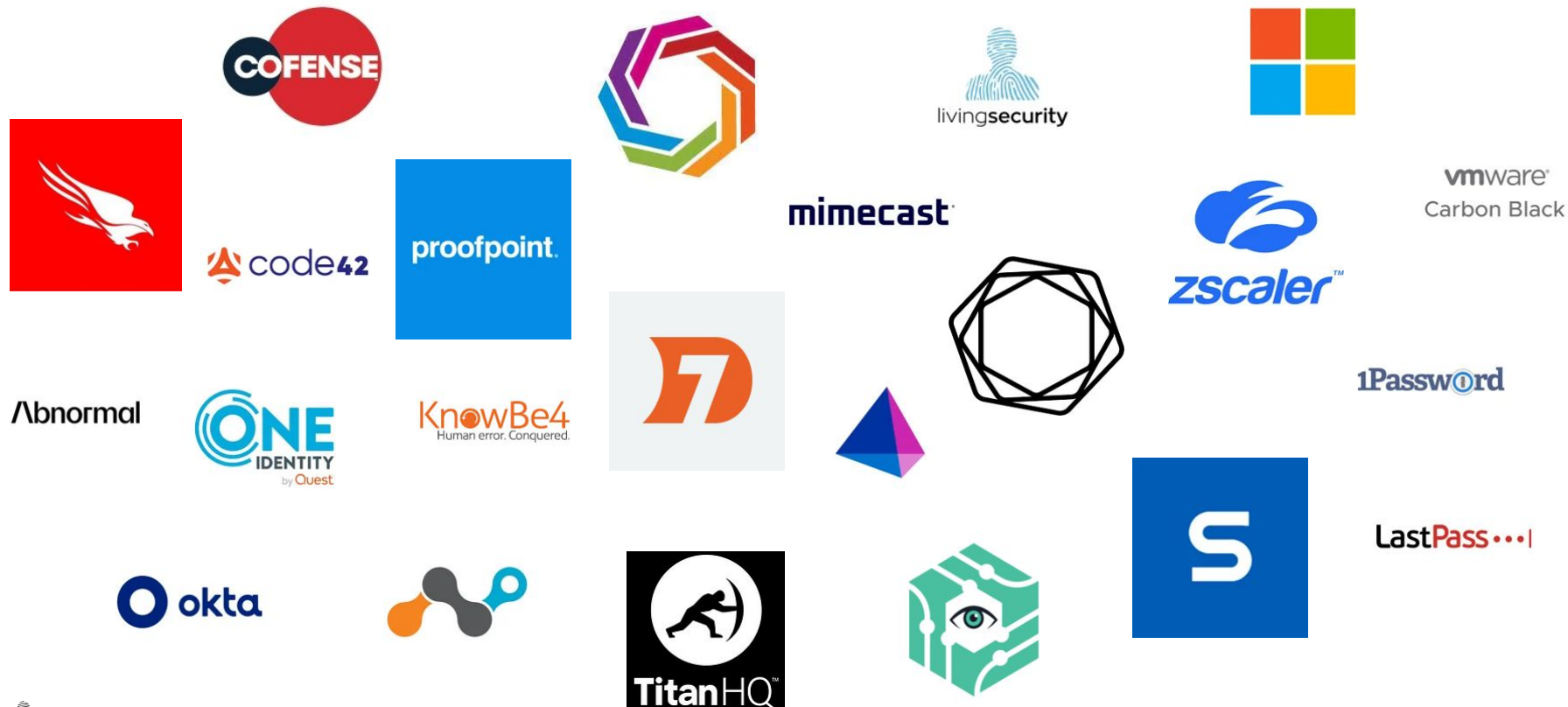
Differentiated Approach To Risk Management.

The Forrester Wave, Q1 2022



Source: The Forrester Wave™: Security Awareness And Training Solutions, Q1 2022.
1. Denotes current offering score, excludes strategy & current market presence.

Integrations for Identifying Risk



Defining Risk

$$\text{Risk} = (\text{Threat}) \times (\text{Vulnerability}) \times (\text{Impact})$$



(Heavily targeted employees) x (Repeat clickers) x (Privileged Access User)

Risk is not:

- Clicked on a link
- Overdue on training
- Reused passwords, etc.

These are risky activities, but standalone activities do not mean exposure to risk.

Hunters vs. Gatherers

Hunting

Seek out risk outliers in data to identify who and what affects your organization's human risk index

Gathering

Create Lenses, pin Power Insights, Behaviors, and Events that your organization cares about the most



Identify

Protect

Report

Social Engineering

Phishing is a type of social engineering attack often used to steal user data. Attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money.

TIME FRAME

30 days

SEGMENTS

Select segments...

BUSINESS RISK

Phishing & Email Vulnerabi...

IMPACT MODIFIERS

Select impact modifiers...

29,308 identities matched (of 29,308 for organization)

☐ Show insights without detections

Pinned Power Insights

POWER INSIGHT	IDENTITIES DETECTED	% ORG	DETECTIONS	RELATIVE IMPACT
> Repeat Phishing Offenders	37	0.13%	65	■■■■■ -302
> Simulated Phish Risk	869	3%	996	■■■■■ -274
> Phishing Targeted and Click	296	1%	371	■■■■■ -208
> Phishing Reporting Adoption	45	0.15%	90	■ +46

Insights

☐ Show inactive

☐ Pinned only

Download

Search insights...

INSIGHT	IDENTITIES DETECTED	DETECTIONS	RELATIVE IMPACT
> Simulated Phish Clicked	869	873	■■■■■ -202
> Simulated Phish Action	164	181	■■■■■ -150
> Phish Clicked	74	84	■■■■■ -130

Phishing Vigilance by Worker Type

Identify

Contractors are demonstrating proper phish reporting practices less than FTEs (*19% Cont. vs. 33% FTE*)

Protect

1. Improve Contractor onboarding documentation
2. Targeted outreach to current Contractors

Report

Track & report on metrics over next 30 days and after next simulation

Entire Organization Employees

Insights

VERIFIED ACTIVE Change identity settings

Power Insights Behavior & Event Insights

TIME FRAME: 30 days SEGMENTS: Select segments... BUSINESS RISK: All Business Risks IMPACT MODIFIERS: Select impact modifiers...

110,365 identities matched (of 110,365 for applied lens)

Pinned Power Insights

POWER INSIGHT	IDENTITIES DETECTED	% APPLIED LENS	DETECTIONS
Repeat Phishing Offenders	564	0.51%	564
Phishing Targeted and Click	756	0.68%	1684
Simulated Phish Risk	2727	2%	2732
Phishing Reporting Adoption	36625	33%	46779

Entire Organization Contractors

Insights

VERIFIED ACTIVE Change identity settings

Power Insights Behavior & Event Insights

TIME FRAME: 30 days SEGMENTS: Select segments... BUSINESS RISK: All Business Risks IMPACT MODIFIERS: Select impact modifiers...

26,890 identities matched (of 26,890 for applied lens) ☐ Show insights without detections

Pinned Power Insights

POWER INSIGHT	IDENTITIES DETECTED	% APPLIED LENS	DETECTIONS	RELATIVE IMPACT
Repeat Phishing Offenders	100	0.37%	100	■■■■■ -336
Simulated Phish Risk	369	1%	370	■■■ -174
Phishing Targeted and Click	35	0.13%	55	■■ -93
Phishing Reporting Adoption	4994	19%	5864	■■■■ +148

Narrowing the Focus of Targeted Phishing Training

Identify

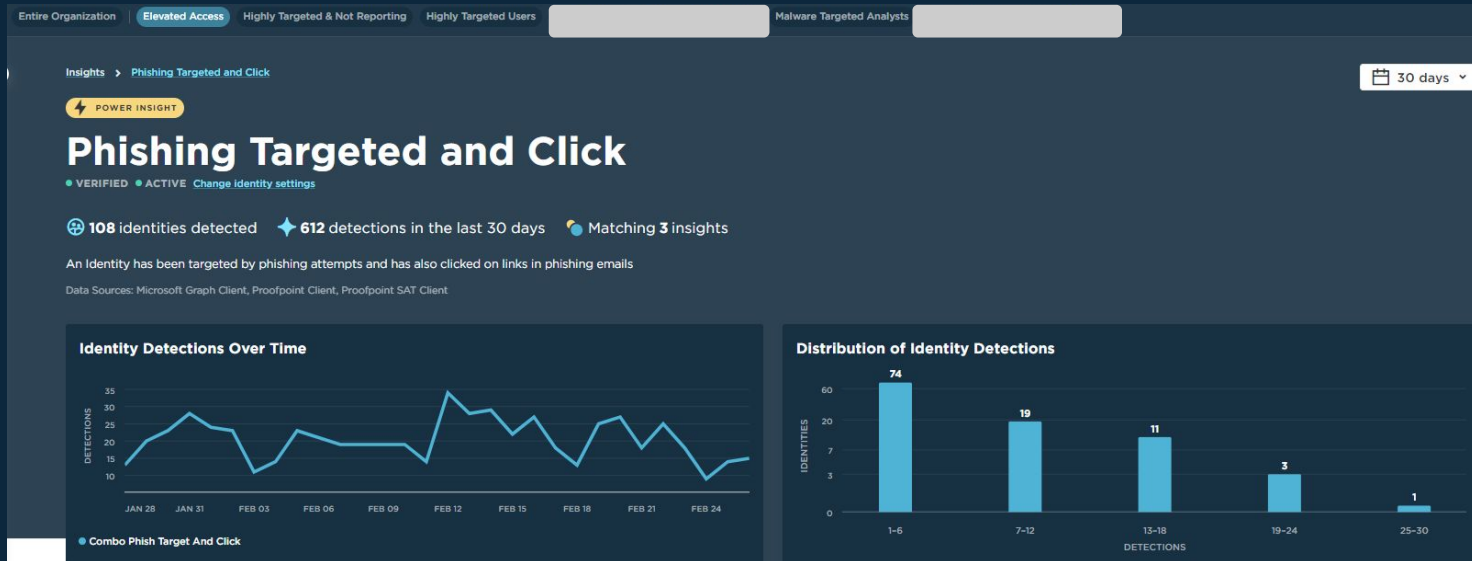
Seek out targeted, elevated access individuals that have demonstrated poor hygiene on simulations

Protect

Assign targeted training RE: heightened role & phishing best practices
Alternative: Customized spear-phish

Report

73% completed optional remediation training
12% reported a real phish within the next 30 days



Account Compromise

A form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials.

TIME FRAME	SEGMENTS	BUSINESS RISK	IMPACT MODIFIERS
30 days ▾	Select segments... ▾	Account Compromise ▾	Select impact modifiers... ▾

12,111 identities matched (of 12,111 for organization) ☐ Show insights without detections

Pinned Power Insights

POWER INSIGHT	IDENTITIES DETECTED	% ORG	DETECTIONS	RELATIVE IMPACT
> Password Manager Adoption ⚡	4262	35%	5667	■■■ +45
> MFA Adoption ⚡	11051	91%	180754	■■■■■ +93

Insights ☐ Show inactive ☐ Pinned only Download

INSIGHT	IDENTITIES DETECTED	DETECTIONS	RELATIVE IMPACT
> Simulated Phish Clicked	382	386	■■■■■ -197
> IDP Suspicious Activity	1	1	■■■■■ -159
> Simulated Phish Action	72	84	■■■■■ -147
> Phish Clicked	74	84	■■■■■ -130
> Simulated Phish Clicked Multiple Times	1	20	■■■■■ -119
> IDP Account MFA Bypass Attempt	59	227	■■■■ -104

MFA Policy Change

Identify

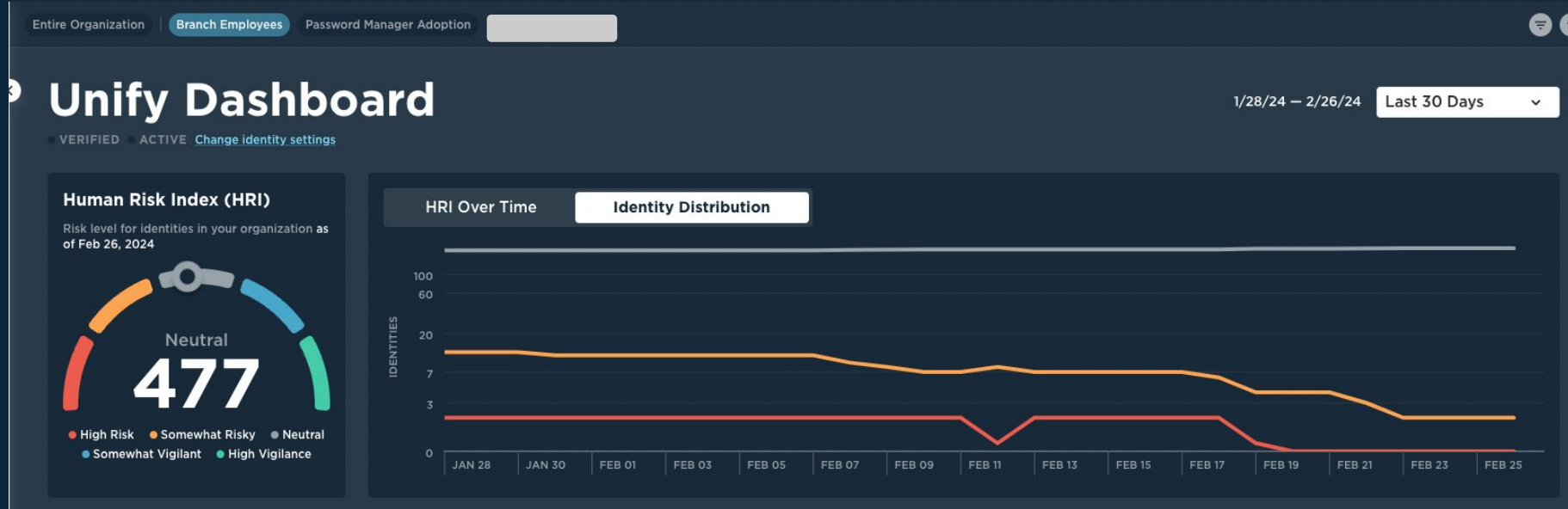
Branch employees failing or bypassing MFA more often than non-branch groups

Protect

Investigated reason for MFA failure and determined need to adopt 1Password org-wide

Report

Report adoption of 1Password and impact on security posture



Malicious Attempts Against Executives

Identify

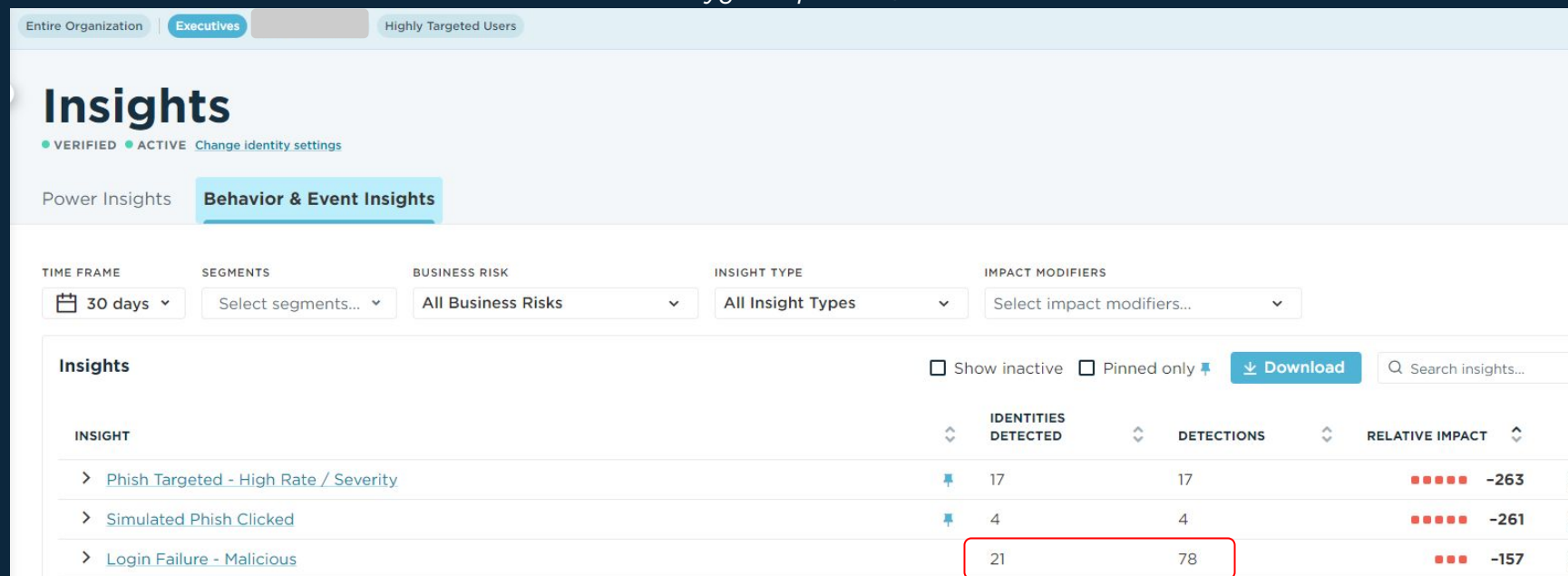
Monitoring Executives for risky behaviors and Malicious Login attempts were highly prevalent (18% of Execs)

Protect

Develop business justification case for CISO approval to provide role-based training
Alternative: Consider other credential hygiene policies/tools

Report

Track vigilant actions of Executives and provide quarterly risk report to CISO



Entire Organization | **Executives** | Highly Targeted Users

Insights

● VERIFIED ● ACTIVE [Change identity settings](#)

Power Insights | **Behavior & Event Insights**

TIME FRAME: 30 days | SEGMENTS: Select segments... | BUSINESS RISK: All Business Risks | INSIGHT TYPE: All Insight Types | IMPACT MODIFIERS: Select impact modifiers...

Insights ☐ Show inactive ☐ Pinned only [Download](#)

INSIGHT	IDENTITIES DETECTED	DETECTIONS	RELATIVE IMPACT
> Phish Targeted - High Rate / Severity	17	17	■■■■■ -263
> Simulated Phish Clicked	4	4	■■■■■ -261
> Login Failure - Malicious	21	78	■■■ -157

Malware & Unsafe Browsing

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.”

TIME FRAME

SEGMENTS

BUSINESS RISK

IMPACT MODIFIERS

📅 30 days

Select segments...

Malware

Select impact modifiers...

29,308 identities matched (of 29,308 for organization)

☐ Show insights without detections

📌 Pinned Power Insights

POWER INSIGHT	IDENTITIES DETECTED	% ORG	DETECTIONS	RELATIVE IMPACT	
> Unsafe Browsing and Malware	6	0.02%	9	■■■■■ -78	⋮
> Unsafe Browsing Habits	2175	7%	3537	■ -14	⋮

INSIGHT	IDENTITIES DETECTED	DETECTIONS	RELATIVE IMPACT	
> Malware Detected	25	36	■■■■■ -83	⋮
> Malware Targeted	175	252	■■■■■ -74	⋮
> Phish with Malware Targeted	53	67	■■■■■ -67	⋮
> Malware Blocked	33	56	■■■ -40	⋮
> Malicious Data	22	25	■■■ -34	⋮
> Website Blocked	2173	3535	■ -14	⋮

Mitigating Behaviors of High Risk Users

Identify

Pinpoint most impactful risky behavior across High Risk Users

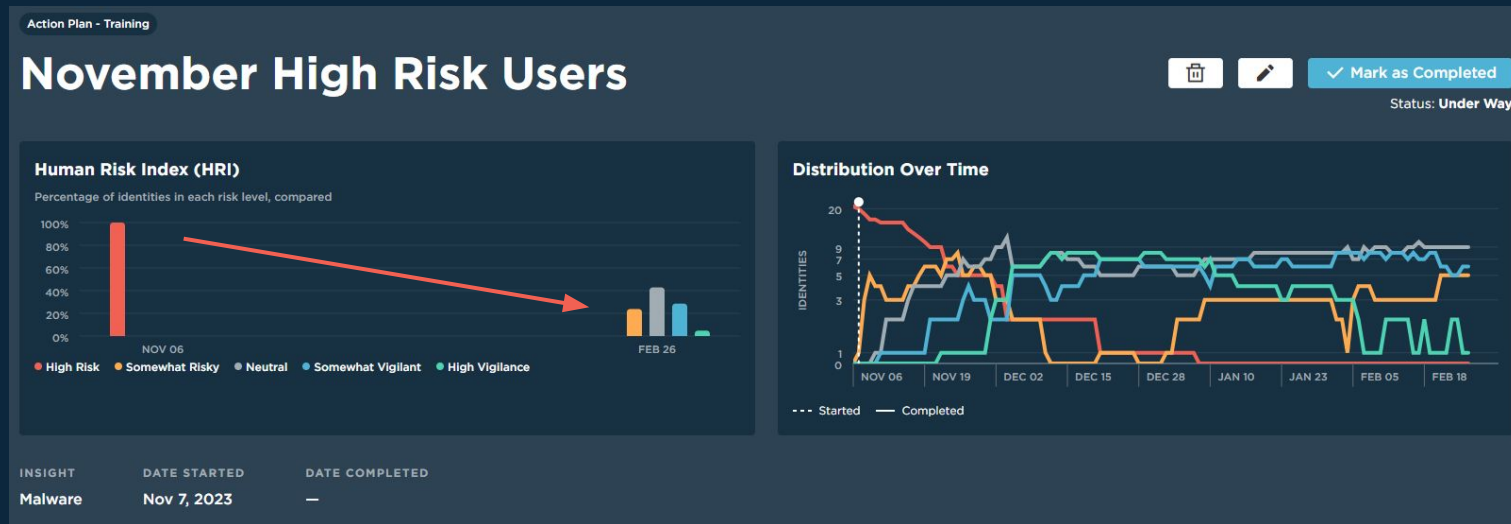
Protect

1. Assign targeted training focusing on specific behavior
2. Send targeted communication to reinforce vigilant behavior

Report

100% reduction of High Risk Users

47% of targeted users became Vigilant



Web Browsing Threat by Employee Level

Identify

High percentage of senior employees are detected with unsafe browsing

Protect

1. Targeted, role-specific communication sent to MD level employees
2. Review web access policies

Report

Monitor for change in browsing habits of MDs vs. other employees

Insights > Unsafe Browsing Habits

⚡ POWER INSIGHT

Unsafe Browsing Habits

● VERIFIED ● ACTIVE [Change identity settings](#)

🔍 144 identities detected ⚡ 183 detections in the last 30 days 🔗 Matching 4 insights

An Identity has exhibited a pattern of unsafe browsing habits

Data Sources: Zscaler Client

Identity Detections Over Time



● Combo Unsafe Browsing

Identities Segments Composition

TIME FRAME: 30 days SEGMENT TYPE: Job Level

Segments [Download](#)

SEGMENT	TYPE	IDENTITIES DETECTED	IDENTITIES TREND %	% SEGMENT	RISK SCORE
Managing Director - [REDACTED]	Job Level	1	+0%	9%	280
Managing Director - [REDACTED]	Job Level	2	+0%	8%	218
Managing Director	Job Level	11	-1%	6%	240
Senior Director	Job Level	23	-0.57%	4%	267
Director	Job Level	27	-0.42%	3%	315
Associate Director	Job Level	32	-0.15%	2%	319
Analyst [REDACTED]	Job Level	23	-0.09%	2%	342
Associate Analyst [REDACTED]	Job Level	25	-0.09%	1%	363

Rows 10 per page

Page 1 out of 1

Data Loss Prevention

Data Loss is when data is somehow removed from your system completely and cannot be recovered or has left your controlled environment through unauthorized access and malicious intent.

TIME FRAME

30 days

SEGMENTS

Select segments...

BUSINESS RISK

Data Loss

IMPACT MODIFIERS

Select impact modifiers...

29,308 identities matched (of 29,308 for organization)

☐ Show insights without detections

Pinned Power Insights

POWER INSIGHT	IDENTITIES DETECTED	% ORG	DETECTIONS	RELATIVE IMPACT
> Sharing Sensitive Information	226	0.77%	341	■■■■■ -183

Insights

☐ Show inactive ☐ Pinned only [Download](#)

INSIGHT	IDENTITIES DETECTED	DETECTIONS	RELATIVE IMPACT
> Sensitive Data Uploaded	18	18	■■■■■ -340
> Blocked Attempted Data Transfer	189	304	■■■ -173
> Data Downloaded in Bulk	19	19	■■ -134
> Unusual Location	158	174	■ -54
> Impossible Location	25	30	■ -43
> Training Overdue - Data Security & Privacy	14	14	■ -38
> Anonymous IP Address	66	111	■ -17



Preventing Data Loss by Contractors

Identify

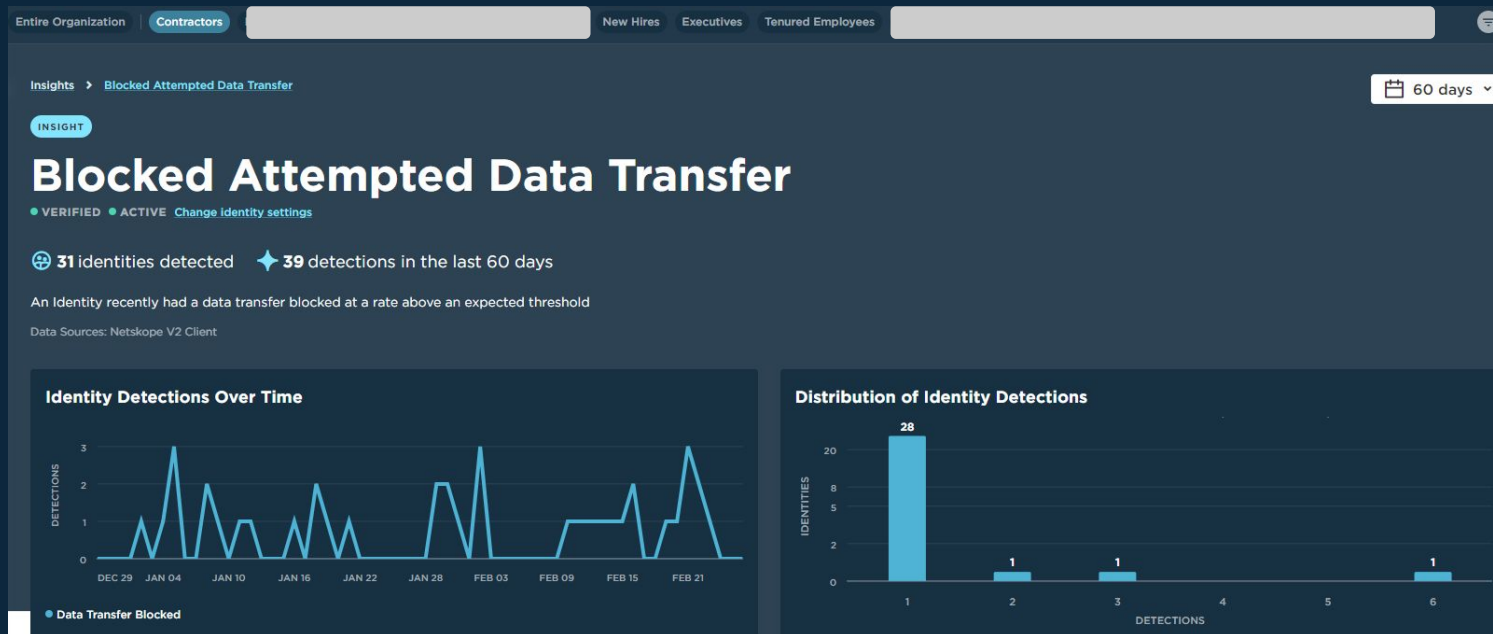
Contractors attempting data transfers, some several times

Protect

1. Review DLP policies for each worker type
2. Send notice to all Contractors re: approved file sharing tool

Report

Track usage in file sharing system and identify persistent violators





livingsecurity

Questions?