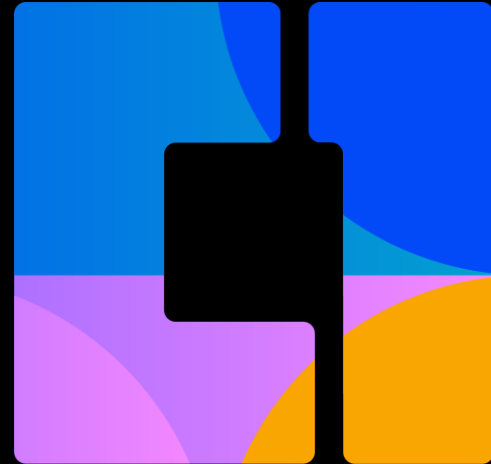


Defending Education in the Age of AI Threats: Zero Trust vs. AI Super Hackers

HASSAN KASSIH, VP C1 CAPABILITIES, C1



C1 by the Numbers

2,600+

Engaged Team Members

800+

Specialized Engineers

7,000+

Technical Certifications

4,762

Projects delivered
annually

300+

Trusted Partnerships

250,000+

Devices services annually

47,000 sq. ft

Secure depots &
Warehousing

3,000+

Devices customized daily

4,762

Implementation Partner
Network to deliver
anywhere

5,000+

Valued Customers

300+

Multinational Customers

60%

of the Fortune 10

40%

of the Fortune 100

120+

Countries Supported

31

Locations, Worldwide

12

Data Centers

4

Customer Success
Centers



Select California K-12 Partners



Select California K-12 Partners



Managed
Services

C1 TC

Technical
Services

C1 MDM

Integration &
Deployment Services

C1 PS

Collaboration
Security

C1 MDR

Human
Intelligence

C1 AIIM

Collaboration
Solutions

UC,CX, C1 Products



Managed
Services

C1 IMS

Technical
Services

C1 MDM

Integration &
Deployment Services

C1 PS

Infrastructure
Intelligence

C1 AIIM

Infrastructure
Security

C1 MDR

Infrastructure
Solutions

EN, DC, CS



IT LifeCycle Services

Secure, Consistent, Depot Services

Secure

inventory & storage

80,000 sq. ft.

warehouse space in California,
New Jersey, Minnesota

Depot/LAB Configuration

Configuration | Remote | Access
Asset tagging | Laser Etching | Kitting

Onsite Deployment

Onsite user installation
and migration

Retrieval and Redeployment

Re-Inventory | Asset disposition/
e-wasting | Re-inventory and cycling

Repair and Warranty Servicing

In Warranty repairs | Out of Warranty
repairs | Seamless RMA processing





Zero Trust vs AI Super Hackers: How to Win the Battle for the Cybersecurity Future



Top 5 Most Commonly Cited Emerging Risks

in Q3 2024

| Risk Score | Risk Name | Risk Category | Risk Rank in 2024 |
|------------|--|---------------|-------------------|
| 1 | AI-Enhanced malicious attacks | 80% | 1 |
| 2 | AI-Assisted misinformation | 66% | New |
| 3 | Escalating political polarization | 66% | New |
| 4 | Globally consequential | 61% | 4 |
| 5 | Misaligned organizational talent profile | 60% | 5 |

Source: Gartner (November 2024)

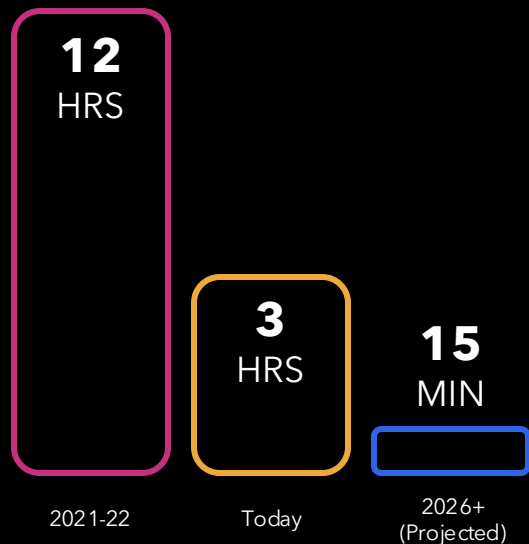




Asked only of respondents whose organizations have adopted AI in at least 1 function. For both risks considered relevant and risks mitigated, n=913.
Source: McKinsey Global Survey on AI, 1,684 participants at all levels of the organization at all levels of the organization, April 11-21, 2023

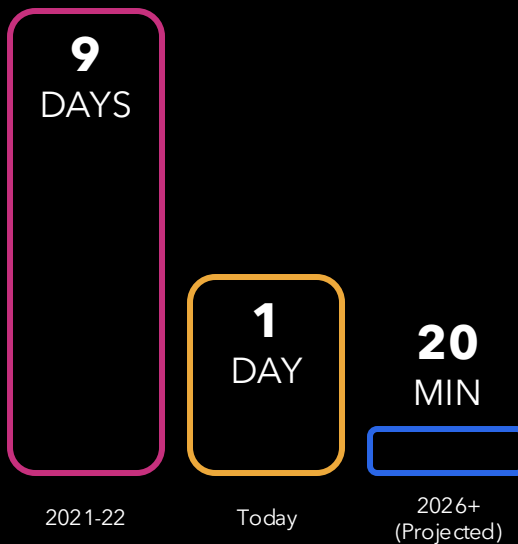
AI is Turbocharging the Speed and Scale of Attacks

BUILD RANSOMWARE



\$2B IMPACT FROM ATTACK ON A US HEALTH INSURER IN 2024

COMPROMISE & EXFILTRATE



15 MILLION USERS' PII AND CONFIDENTIAL DATA EXFILTRATED IN JAN 2024

EXPLOIT VULNERABILITY



500+ ORGANIZATIONS AND 35+ MILLION PEOPLE AFFECTED BY MOVEIT VULNERABILITY



Initial access (attack vector)

Lateral movement

Privilege escalation

The Five Stages of a Cyber Attack

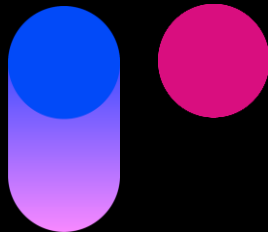
Data exfiltration

Ransomware deployment

Zero Trust Architecture

Never Trust, Always Verify:

WHO, WHEN, WHAT, WHY, WHERE



Identity and Access Mg.

Least Privilege Access

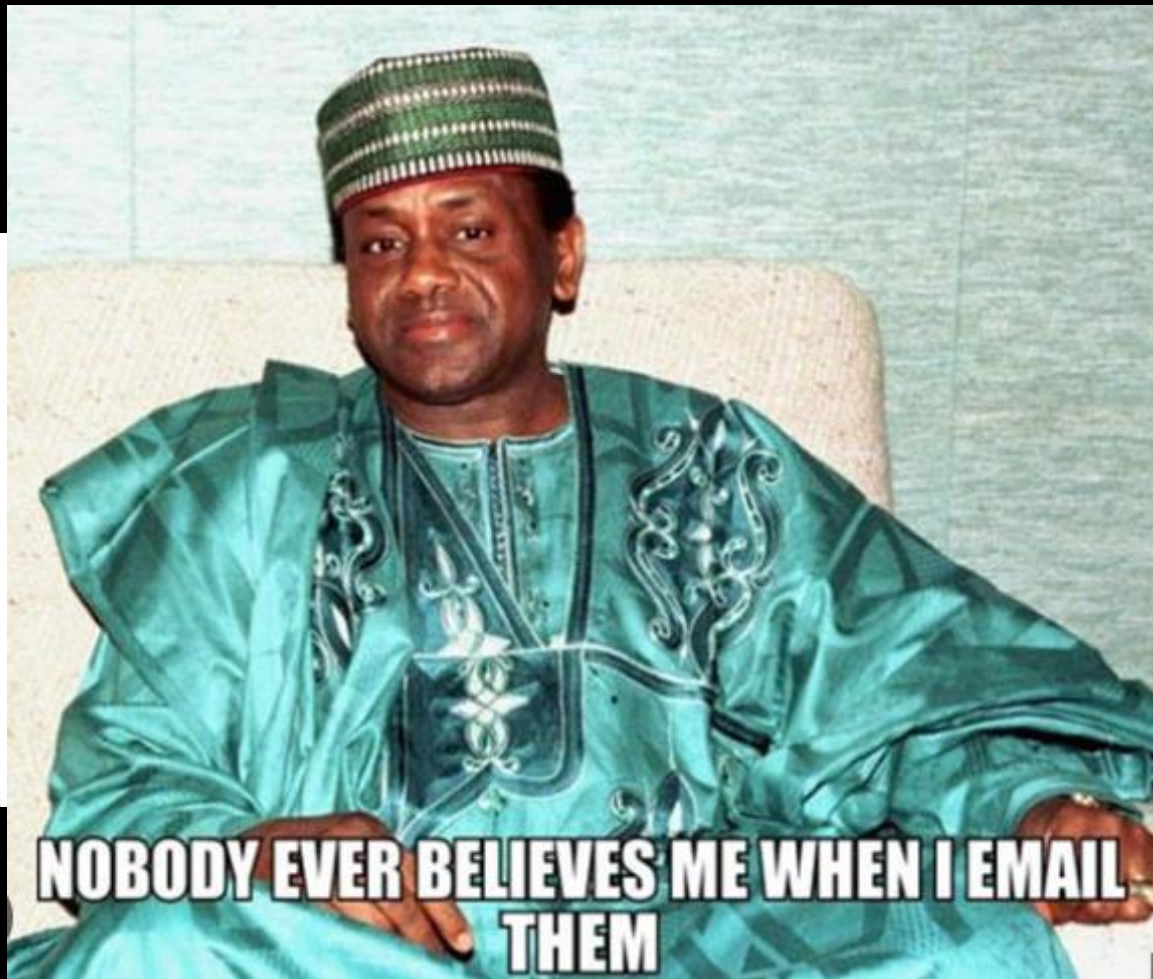
Micro Segmentation

Continuous Monitoring

Encryption

1: Social Engineering At Scale







Emily family photo.pdf
3 MB



From: François

Sent: Saturday, November 16, 2024, 8:14 AM

To: Emily

Subject: your son photo from Paris trip

Bonjour Emily,

As promised, attached is the picture I took for your son—he seemed so excited about it during your visit.

This version is complimentary, but if you'd like to have a high-resolution version, it's available for just €10. Let me know, and I'll be happy to provide it.

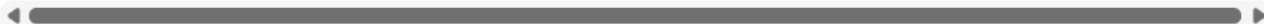
Wishing you and your family all the best!

Au revoir,

François

Paris Pictures Corp.

P.S. Paris is always ready to welcome you back—perhaps with even more memories to capture!





Fraudsters Deepfake Entire Meeting, Swindle \$25.5M

Hong Kong Company Scammed After Criminals Used Deepfake Technology to Imitate CFO

Jayant Chakravarti (@JayJay_Tech) • February 5, 2024



Share



Tweet



Share



Credit Eligible



Get Permission



Image: Shutterstock

A group of fraudsters used deepfake technology to trick an employee at a Hong Kong-based multinational company to transfer \$25.57 million to their bank accounts, Hong Kong Police said Sunday.

Massive Reach

Hyper-Personalization

Emotional Manipulation

Social Engineering At Scale

Authority Impersonation

Multi-Channel Attacks

Overwhelms Defenses

High Success Rates



**Zero Trust Identify Management
(Three-Factor Authentication)**

**Zero Trust Access Management
(Context-Based Authorization)**

**Apply Zero Trust Principles to
verify all communications**

The Counterattack Strategy

**Zero Trust AI-Powered
Behavioral Analytics**

**From EDR to XDR to
MDR**

**Educate and Train
Users**

**Zero Trust Browser
Security**

Industry Insight with Ashish Khanna

No sales pitch, just the straight scoop from the leaders whom institutions bank on for security solutions.



Governance & Risk Management, Remote Workforce, Zero Trust

Why Browser-Based Security Is Vital to Zero Trust Operations

Browser Isolation Protects Access Points as Remote Work Expands Attack Surface

Ashish Khanna • March 12, 2025

Share Tweet in Share Get Permission



Image: Shutterstock

Enterprises depend on web browsers as a primary gateway to critical resources, especially given the rise of remote and hybrid work.

See Also: [Financial & Banking Services: Cybersecurity Trends from Expel's 2025 Annual Threat Report](#)

Verizon's 2024 Mobile Security Index shows that 92% of organizations support some form of remote connectivity. While browsers have evolved into essential access points, they have become prime targets for cyberattacks.

GET DAILY EMAIL UPDATES

Covering topics in risk management, compliance, fraud, and information security.

Email address

Submit

By submitting this form you agree to our [Privacy & GDPR Statement](#).



RESOURCES



AI, Automation, and Compliance: The New Frontier in Banking Risk Management



[Whitepaper](#)
Future-Proof Your Business: A Comprehensive Guide to Application Modernization and Development for Public and Private Sectors



How to Get the Most Out of Your Security Tech Stack



Live Webinar | Reimagining Risk Modelling and Decisioning: Balancing Compliance and Automation for Competitive Advantage



[Whitepaper](#)
A Defender's Cheat Sheet: MITRE ATT&CK in AWS

2: AI-Driven Lateral Movement and Privilege Escalation



AI-Driven Lateral Movement and Privilege Escalation

Reconnaissance at Scale

Credential Harvesting

Privilege Escalation

Automated Propagation



The Counterattack Strategy

Zero Trust Network Access (ZTNA)

Zero Trust SSE/SASE

Zero Trust Security Zones (Segmentation, MicroSegmentation)

Strict Privileged Access Management (PAM)

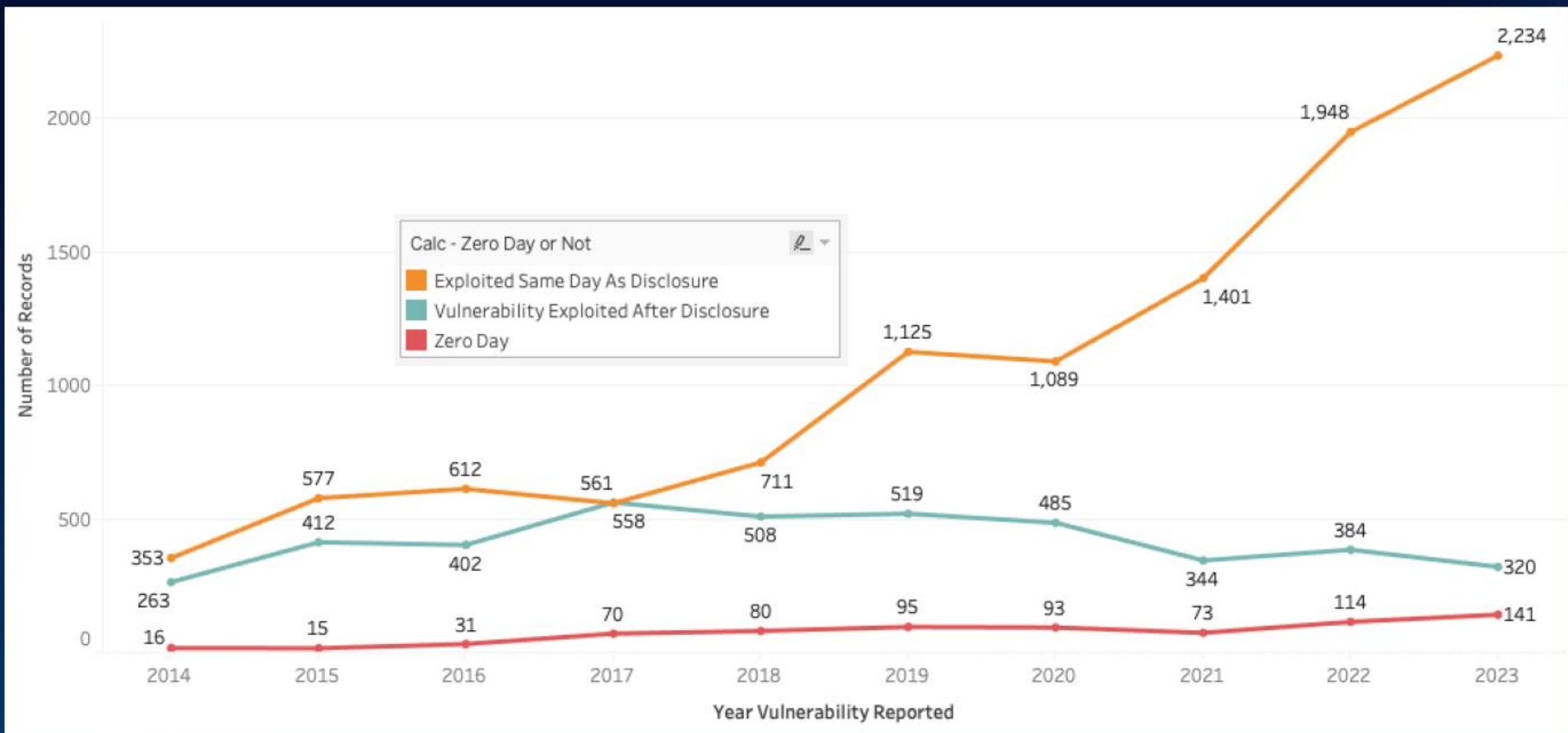
Behavioral Monitoring

Rapid Incident Response



3: Automated Vulnerability Scanning and Exploitation





Source: IBM X-Force/Analysis: Gartner Research



Automated Vulnerability Scanning and Exploitation

**Automated
Exploit Kits**

**Weaponized
Zero-Days**

**Unmatched Speed
and Massive Scale**

**Real-Time
Adaptive Precision**

**Accessibility for
Unexperienced Attackers**



The Counterattack Strategy

**Zero Trust AI Threat
Detection and Response**

**Real Time Asset
Discovery and Validation**

**Enhanced Vulnerability
and Patch Management**

**Harden Systems and Applications
(Minimize the Attack Surface)**



4: Data Exfiltration and Manipulation at Scale



Data Exfiltration and Manipulation at Scale

- Automated Data Harvesting
- Stealthy Exfiltration Techniques
- User Behavior Imitation
- Fragmented File Transfer
- Exfiltration-as-a-Service

The Counterattack Strategy



Identify and Classify sensitive Assets
Role Based and Attribute Based Access Control
Certificate based Authentication (Devices,
Servers, Applications, workloads, and APIs)
AI-Based Data Loss Prevention (DLP)
Real-time monitoring and Analytics
Time-Bound Access

5: AI-Augmented Ransomware and Destructive Attacks



AI-Augmented Ransomware and Destructive Attacks

Identify and encrypt critical data faster

Disable backups and recovery mechanism

Hard to detect



The Counterattack Strategy

Zero Trust Cyber Recovery Solution

Zero Standing Privileges (ZSP)

Behavioral Analysis

Incident response

Master your environment



How C1 Can Help

**AI-Security Risk
Assessments**

**AI-Security
Solutions & Controls**

**Zero Trust Architecture
Deployments**

**Infrastructure
and Data Security**

**Vulnerability
Management**

**Users and
Devices Security**


**Cyber Recovery
Solutions**

**Managed Detection
and Response**

**Attack Surface
Management**

**GRC Advisory
Services**





Connecting Every Learner, Everywhere

Supporting over 8 Million Students

**Proven Track
Record**

**Deep Education
Expertise**

**Local Focus with
National Scale**

**Innovative
Learning Solutions**

**Safe Schools
Initiatives**

**IT LifeCycle
Services**

**Experts in E-Rate
Funding**

**Trusted Partner
Ecosystem**

**Dedicated Leadership
in K-12 Community**

**Community
Investment**



Top Concerns in the CoSN 2023 State of EdTech Leadership Survey

81%

of districts cite insufficient
funding as their biggest
challenge

59%

report concern over the
increasing sophistication
of threats

58%

are concerned about the lack of
documented cybersecurity
processes



K-12 IS THE #1 TARGETED SECTOR FOR RANSOMWARE

"Many of our schools across the nation are, what we call, **'target rich and cyber poor'** in that they are often a frequent target for ransomware and other cyberattacks due to the extensive data kept on school networks, often without the proper protection."

Cybersecurity & Infrastructure Security Agency (CISA)

Join the Discussion: Scan to Connect





Powering Student Outcomes
through Technology