

# Security **ADVISOR**

MIDDLE EAST



## **CYBER RESILIENCE: THE KEYSTONE OF MODERN CYBERSECURITY**

SECURITY ADVISOR ME EXAMINES THE RELEVANCE OF CYBER RESILIENCE IN AN AGE WHERE DIGITAL TECHNOLOGY UNDERPINS EVERY FACET OF OUR LIVES.



tahawultech.com

# CISO50 AWARDS 2024

19<sup>th</sup> September 2024

The Ritz-Carlton, JBR, Dubai

#CISO50FSA2024 | #tahawultech

## UNITING CYBERSECURITY LEADERS: CISO 50 FORUM & AWARDS 2024

Celebrating leadership excellence and innovation in cybersecurity

In an era where cyber threats continue to evolve rapidly, the role of Chief Information Security Officers (CISOs) has never been more crucial. **CPI Media Group** is delighted to announce the **CISO 50 Forum & Awards**, a prestigious event dedicated to recognizing and celebrating the leaders who are at the forefront of cybersecurity.

### Event Highlights:

- **Keynote Sessions:** Hear from industry leaders and visionaries who are shaping the future of cybersecurity. Gain insights into the latest trends, strategies, and technologies that are driving innovation and protecting organizations globally.
- **Panel Discussions:** Engage with top CISOs and security experts in dynamic discussions about the challenges and opportunities in the ever-changing landscape of cybersecurity.
- **Awards Ceremony:** Celebrate the achievements of the top 50 CISOs who have demonstrated outstanding leadership, innovation, and dedication to securing their organizations. These awards honor those who have set benchmarks in the industry and inspire others to follow in their footsteps.
- **Networking Opportunities:** Connect with peers, thought leaders, and solution providers. This is your chance to build relationships, exchange ideas, and explore potential collaborations in an exclusive setting.

### Why Attend:

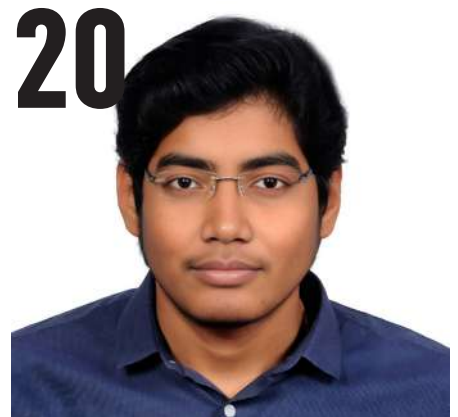
The **CISO 50 Forum & Awards** is more than just an event; it's a movement towards a more secure and resilient digital world. By attending, you will:

- **Gain Valuable Insights:** Learn from the experiences and success stories of top CISOs and cybersecurity professionals. Discover new approaches and strategies to enhance your organization's security posture.
- **Stay Ahead of Trends:** Understand the latest developments in cybersecurity technology and practices. Equip yourself with the knowledge to tackle emerging threats and leverage new opportunities.
- **Be Inspired:** Celebrate the success stories and draw inspiration from exceptional achievements. Recognize the impact of effective leadership and innovative thinking in driving cybersecurity excellence.
- **Expand Your Network:** Meet and connect with like-minded professionals who are passionate about cybersecurity. Build relationships that can lead to new opportunities and collaborations.

Don't miss your chance to be part of this landmark event. Whether you are a seasoned CISO, an aspiring cybersecurity leader, or a stakeholder invested in the security domain, the **CISO 50 Forum & Awards** offers a unique platform to learn, share and celebrate.

Mark your calendar for **September 19<sup>th</sup>, 2024**, and be prepared to immerse yourself in a day of knowledge, recognition, and inspiration. Together, let's celebrate the pioneers who are safeguarding our digital future.

For more details about the event and nomination, please visit [www.tahawultech.com/ciso50-fsa/2024](http://www.tahawultech.com/ciso50-fsa/2024)



**6** News from the security industry in the region and beyond

**10** Darren Thomson, VP and Field CTO, EMEAI, Commvault, explains how Commvault is transforming into a comprehensive cyber resilience provider for organizations.

**20** Attackers exploit URL protection services to conceal malicious links in phishing attacks: Barracuda

**22** Sujoy Banerjee, Associate Director of ManageEngine Sales, MEA region discusses the latest trends in Security Information and Event Management (SIEM).

# Solar Powered Camera

## No network cable required

Powered by solar energy, this kit sets up without any electrical wiring.

## Easy installation

Easy set up without mechanical equipment-reducing the installation costs and time.

## Can withstand bad weather

Prone to extreme weather such as strong wind and rainstorms.



**2MP**  
@ 30 fps



**40W**



**20 Ah**  
lithium



**4G**



Beaufort  
scale **12**



**IP67**



Scan to Learn More



HIKVISIONMENA



HIKVISION-MENA



HIKVISIONMENA



HIKVISIONMENA

**HIKVISION**<sup>®</sup>

# EDITOR'S NOTE



Talk to us:  
E-mail:  
anita.joseph@  
cpimediagroup.com

Anita Joseph  
Editor

## TRUST NOTHING

In an era where digital transformation is accelerating, the landscape of cybersecurity is undergoing rapid evolution. The proliferation of interconnected devices, cloud computing, and remote work has expanded the attack surface, making traditional security models increasingly inadequate. It is within this context that the Zero Trust framework has emerged as a pivotal paradigm shift in cybersecurity.

Zero Trust, a concept popularized by Forrester Research, operates on the foundational principle that no entity, whether inside or outside the network, should be trusted by default. Unlike conventional security approaches that rely heavily on perimeter defenses, Zero Trust advocates for continuous verification of all users and devices attempting to access resources, irrespective of their location.

The necessity for Zero Trust arises from the growing sophistication of cyber threats. The traditional "trust but verify" approach has proven insufficient in mitigating risks associated with insider threats and lateral

movement within networks. Zero Trust, on the other hand, enforces stringent access controls, ensuring that trust is never implicit and always validated through multifactor authentication, identity verification, and real-time monitoring.

Implementing a Zero Trust architecture requires a holistic overhaul of existing security practices. It demands granular visibility into user activities, robust identity and access management (IAM) systems, and seamless integration across various security tools and platforms.

### THE RISE OF ZERO TRUST

This transition, though challenging, promises enhanced resilience against breaches and a more robust security posture.

As we navigate through an increasingly digital world, the adoption of Zero Trust represents a proactive step towards safeguarding critical assets. Zero Trust is not merely a trend but a necessary evolution in the pursuit of comprehensive cybersecurity. As threats continue to evolve, so too must our defenses, with Zero Trust leading the charge towards a more secure digital future.

#### EVENTS



FOUNDER, CPI  
Dominic De Sousa  
(1959-2015)

Published by **CPI**

ADVERTISING  
Group Publishing Director  
Kausar Syed  
kausar.syed@cpimediagroup.com

EDITORIAL  
Editor  
Anita Joseph  
anita.joseph@cpimediagroup.com

PRODUCTION AND DESIGN  
Designer  
Prajith Payyapilly  
prajith.payyapilly@cpimediagroup.com

DIGITAL SERVICES  
Web Developer  
Adarsh Snehan  
webmaster@cpimediagroup.com

Publication licensed by  
Dubai Production City, DCCA  
PO Box 13700  
Dubai, UAE

Tel: +971 4 5682993

Publishing Director  
Natasha Pendleton  
natasha.pendleton@cpimediagroup.com

Online Editor  
Daniel Shepherd  
daniel.shepherd@cpimediagroup.com

Sales Director  
Sabita Miranda  
sabita.miranda@cpimediagroup.com

© Copyright 2024 CPI  
All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

## ESET RESEARCH DISCOVERS EVILVIDEO: TELEGRAM APP FOR ANDROID TARGETED BY ZERO-DAY EXPLOIT SENDING MALICIOUS VIDEOS

**ESET researchers discovered a** zero-day exploit, which targets the Telegram app for Android, that appeared for sale for an unspecified price in an underground forum post from June 2024. Using the exploit to abuse a vulnerability that ESET named "EvilVideo," attackers could share malicious Android payloads via Telegram channels, groups, and chats, and make them appear to be multimedia files.

"We found the exploit being advertised for sale on an underground forum. In the post, the seller shows screenshots and a video of testing the exploit in a public Telegram channel. We were able to identify the channel in question, with the exploit still available. That allowed us to get our hands on the payload and test it ourselves," explains ESET researcher Lukáš Štefanko, who discovered the Telegram exploit.



ESET Research analysis of the exploit revealed that it works on Telegram versions 10.14.4 and older. The reason might be that the specific payload is most likely crafted using the Telegram API, since it allows developers to upload specially crafted multimedia files to Telegram chats or channels programmatically. The exploit seems to rely on the threat actor being able to create a payload that displays an Android app as a multimedia preview and not as a

binary attachment. Once shared in chat, the malicious payload appears as a 30-second video.

By default, media files received via Telegram are set to download automatically. This means that users with this option enabled will automatically download the malicious payload once they open the conversation where it was shared. The default automatic

download option can be disabled manually — in that case, the payload can still be downloaded by tapping the download button of the shared video.

If the user tries to play the "video," Telegram displays a message that it is unable to play the video and suggests using an external player. However, if the user taps the Open button in the displayed message, they will be requested to install a malicious app disguised as the aforementioned external app.

## IFS STRENGTHENS SAUDI OPERATIONS WITH NEW REGIONAL HEADQUARTER IN RIYADH

**IFS, the global cloud enterprise** software company, has announced the inauguration of its regional headquarters in Riyadh. The strategic move reiterates IFS' commitment to strengthen its position in the region and accelerate the Kingdom's ongoing digital transformation journey.

"Establishing our regional headquarters in the largest economy in the MENA region reinforces our commitment to support the region's growth by providing industrial technologies to key sectors here. We look forward to building a strong foundation with our partners and expand our footprint in Saudi

Arabia and the neighboring countries, driving innovation and excellence. This achievement symbolizes our dedication to becoming an integral part of the Kingdom's ambitious vision and dynamic future." said Vincent Carvalho, Regional President, APJ, ME&A, IFS.

The regional headquarter establishment reaffirms IFS' focus on optimizing local resources and driving sustainable industrial innovations in the kingdom through its latest digital solutions. It will help local key industry players benefit from the latest technological advancements as IFS continues to innovate and drive operational efficiency in business processes.



---

## EXABEAM AND LOGRHYTHM COMPLETE MERGER AND ANNOUNCE NEW COMPANY DETAILS

---

### In a strategic move set to define

the future of the cybersecurity landscape, Exabeam, delivering industry-leading AI and automation for accelerated threat detection, investigation, and response (TDIR), and LogRhythm, renowned for its high-integrity, trusted data ingestion, today announced the successful completion of their previously announced merger. The merger combines unparalleled technological innovation with reliable data to create an AI-driven security operations platform that delivers the most efficient and accurate security information and event management (SIEM) and user and entity behavior analytics (UEBA) solutions in the industry.

Moving forward, the company will leverage the best of both organizations to create a best-of-breed cybersecurity



vendor relentlessly focused on empowering security analysts, security engineers, and CISOs with the tools, intelligence, and guidance needed to safeguard their organizations against cyberthreats. The company will retain the Exabeam name and refresh the visual brand to represent the merging of two industry leaders and honor the legacy of the long-established LogRhythm brand.

Exabeam has also unveiled its product roadmap and strategy, highlighting the proven, cloud-native AI-driven Exabeam Security Operations Platform that will serve as the foundation of its future product offerings. On-premises LogRhythm SIEM customers will benefit from the powerful analytics offered through the Exabeam platform to combat sophisticated and credential-based attacks. The company remains committed to quarterly launches to its cloud-native and on-premises SIEM offerings as demonstrated by LogRhythm since July 2022. By integrating AI-driven automation with reliable data, this strategy aims to streamline security operations and accelerate TDIR, empowering security teams to focus on quickly and effectively mitigating complex threats.

---

## CLOUDERA UNVEILS NEW OBSERVABILITY OFFERINGS FOR ON-PREMISES AND PUBLIC CLOUD DATA CENTERS

---

**Cloudera, the hybrid platform for data, analytics, and AI,** announced two new offerings for Cloudera Observability Premium designed to simplify and automate platform administration. These premium tier features provide a single source of observability across all cloud-based and on-premises data centres, even for the most secure enterprises.

With the increasing demand for strategic insights from technologies like GenAI and the rise of data privacy and security regulations, there is an increasing need for full visibility into enterprise data sources and workflows. Cloudera's expanded Cloudera Observability suite empowers enterprises with highly secure networks to operate observability entirely within their data centres or on the public cloud.

Cloudera's two new solutions in its Cloudera Observability suite include:



- Cloudera Observability Premium On-Premises allows customers with highly secure networks to run observability entirely within their data centres. This solution ensures optimal monitoring, troubleshooting, financial governance, data

observability, and automated actions, even in air-gapped configurations.

- Cloudera Observability Premium for Public Cloud Data Hub extends all the advanced premium capabilities to public cloud users, including real-time monitoring, advanced financial governance, automated actions, and data observability.

With the addition of both these offerings, enterprises can now leverage high-value features such as real-time monitoring for Data Hub clusters, jobs, and queries, financial governance with new cost factors and capacity forecasting, workload views, alerts, and automated actions, along with data observability with hot and cold table analysis. These features aim to maximise investment, streamline self-service troubleshooting, and enhance visibility into resource costs and usage.

## JUNIPER NETWORKS INTRODUCES INDUSTRY'S FIRST OPS4AI LAB AND VALIDATED DESIGNS TO MAXIMIZE AI WORKLOAD PERFORMANCE

**Juniper Networks, a leader in secure, AI-Native Networking,** has announced the first and most comprehensive multivendor lab for validating end-to-end automated AI Data Center solutions and automated operations with switching, routing, storage and compute solutions from leading vendors, as well as new Juniper Validated Designs (JVDs) that accelerate the time-to-value in deploying AI clusters. In addition, Juniper is releasing new key software enhancements that optimize the performance and management of AI workloads over Ethernet. Through these Operations for AI—Ops4AI—initiatives, Juniper is collaborating closely with a broad range of infrastructure ecosystem partners to enable the best AI workload



performance via the most flexible and easiest-to-manage data center infrastructures.

As a key element of Juniper's AI-Native Networking Platform, the existing Networking for AI solution consists of a spine-leaf data center architecture with a foundation of AI-optimized 400G and 800G QFX Series Switches and PTX Series Routers. The solution is secured via high

performance firewalls with industry-leading effectiveness, and managed via Juniper Apstra

data center assurance software and the Marvis Virtual Network Assistant (VNA). Juniper Apstra and Marvis provide key Ops4AI capabilities, such as intent-based networking, multivendor switch management, application / flow / workload

awareness, AIOps proactive actions and a GenAI conversational interface. With Juniper's full Networking for AI solution, customers and partners can lower AI training Job Completion Times (JCTs), reduce latency during inferencing and increase GPU utilization while decreasing deployment times by up to 85 percent and reducing operations costs by up to 90 percent in some instances.

## SENTINELONE AND AON COLLABORATE TO ENHANCE STRATEGIC CYBER SERVICES FOR INSUREDS

**SentinelOne, a global leader in AI-powered security,** and Aon plc, a leading global professional services firm, announced a strategic collaboration through which Aon will leverage SentinelOne's Singularity Platform to help gather internal security data from SentinelOne's clients to more effectively profile and mitigate cyber risk.

SentinelOne will team with Aon in both its cyber brokerage process, which is facilitated by its global eSubmission and self-attestation patented platform Cyber Quotient Evaluation (CyQu), and through its industry-leading Stroz Friedberg global Incident Response service. This effort will serve to enhance the client value proposition of making better data-driven decisions and help organizations

manage and mitigate cyber risk by providing more visibility into insurability drivers and cyber exposures.

Combining SentinelOne's cutting-edge Singularity Platform with Aon's incident response prowess, organizations will now have access to a comprehensive suite of tools and services to proactively defend against, detect and swiftly respond to cyber incidents of all magnitudes.

"This alliance fortifies the shared capabilities of two leaders in the cybersecurity space and marks a significant milestone in our collective mission to combat evolving cyber threats with unparalleled expertise and innovative solutions," said Christopher Bruno, Head of Strategic Alliances, Cyber Solutions, Aon. "Bringing together SentinelOne's



AI-powered threat detection and response technology with Aon's extensive experience in managing and guiding clients through the most complex of breaches, will empower clients to navigate the challenging threat landscape with confidence and resilience."

The combined solution will enhance the placement process with more verifiable risk data that helps to prioritize remediation activities and enhance the organization's security posture.





tahawultech.com

# FUTURE SECURITY AWARDS 2024

19<sup>th</sup> September 2024

The Ritz-Carlton, JBR, Dubai

#CISO50FSA2024 | #tahawultech

## CELEBRATE CYBERSECURITY INNOVATION: FUTURE SECURITY AWARDS 2024

### Applauding Vision and Innovation in Cybersecurity

In a world where cyber threats are ever-evolving, the need for cutting-edge security strategies and visionary leaders has never been more critical. **CPI Media Group** is delighted to announce this year's edition of the **Future Security Awards**, an exceptional event dedicated to honoring innovation, vision, and strategic excellence in cybersecurity.

#### Why Attend:

**The Future Security Awards** is more than just an awards ceremony; it's a celebration of the pioneering spirit and strategic foresight that drive the cybersecurity industry forward. By attending, you will:

- **Gain Insightful Knowledge:** Hear from leaders who are pioneering new approaches to cybersecurity. Learn about the innovations and strategies that are making a significant impact in the industry.
- **Stay Ahead of the Curve:** Understand the latest trends and technological advancements in cybersecurity. Equip yourself with the knowledge and tools to navigate and mitigate emerging threats effectively.
- **Celebrate Excellence:** Recognize and celebrate the achievements of peers and organizations that are leading the way in cybersecurity innovation. Draw inspiration from their successes and contributions.
- **Expand Your Professional Network:** Meet and connect with like-minded professionals and industry leaders. Build relationships that can lead to new opportunities, collaborations, and partnerships.

Don't miss your chance to be part of this landmark event. Whether you are a cybersecurity professional, a visionary leader, or a stakeholder (vendor, distributor, reseller or systems integrator) in the security domain, the **Future Security Awards** offers a unique platform to learn, share, and celebrate.

Mark your calendar for **September 19<sup>th</sup>, 2024**, and prepare to immerse yourself in an evening of recognition, inspiration, and forward-thinking. Together, let's celebrate the innovators and strategists who are shaping the future of cybersecurity.

For more details about the event and nomination, please visit [www.tahawultech.com/ciso50-fsa/2024](http://www.tahawultech.com/ciso50-fsa/2024)

# DRIVING CYBER RESILIENCE

**DARREN THOMSON**, VP AND FIELD CTO, EMEA, COMMVault, TELLS ANITA JOSEPH THAT COMMVault IS TRANSFORMING INTO A COMPREHENSIVE CYBER RESILIENCE PROVIDER FOR ORGANIZATIONS

**C**ommvault has been a leader in data protection and information management for many years. How do you define cyber resilience, and what key elements differentiate it from traditional data protection strategies?

Cyber resilience is defined as an organization's ability to prepare for, withstand, recover, and rebuild from cyberattacks. It encompasses having a comprehensive strategy that goes beyond just protecting data. Traditional data protection strategies focus on backing up data so it can be restored in case of a disaster.

However, cyber resilience acknowledges the evolving threat landscape and focuses on proactively mitigating risks and ensuring business continuity even during an attack. Key elements that differentiate cyber resilience from traditional data protection strategies include understanding digital risks, where organizations need to identify and assess the potential threats they face and recognize the critical data that needs protection.

Integrated cybersecurity is essential, embedding cybersecurity into all aspects of business operations rather than treating it as a separate IT function.



Regular testing of incident response plans and having a clean room environment for isolated data recovery are crucial for ensuring a swift and effective response to cyberattacks.

Awareness of AI's potential dangers, such as its use in reconnaissance and fraudulent activities, while also leveraging its benefits for threat detection, is vital. Strong executive leadership is necessary to build a culture of cybersecurity awareness and allocate resources for cyber resilience initiatives.

**Can you share how emerging technologies like artificial intelligence and machine learning are being integrated into Commvault's cyber resilience and recovery solutions? How do these technologies enhance threat detection and response?**

Commvault has integrated Artificial Intelligence (AI) and Machine Learning (ML) through partnerships with industry leaders. These collaborations strengthen Commvault Cloud's offerings by providing advanced security features, improved data analysis, and advanced threat detection. For instance, the partnership with Avira delivers AI-powered threat protection, while the integration with CyberArk bolsters Zero Trust security by reducing the risk of compromised credentials. Additionally, Commvault's collaboration with Darktrace offers proactive threat defense through AI-powered insights, and the integration with Databricks allows AI-driven searches for better data governance. These are just a few examples, and Commvault also partners with other security leaders to further enhance its cloud platform's response times and overall effectiveness.

**What are some best practices that Commvault recommends for organizations to build a comprehensive cyber resilience strategy?**

Based on the Commvault 2024 Cyber Recovery Readiness Report, Commvault recommends five key capabilities, or resiliency markers, for organizations to



build a comprehensive cyber resilience strategy:

- Security tools that enable early warning about risk, including insider risk.
- A known-clean dark site or secondary system in place.
- An isolated environment to store an immutable copy of the data.
- Defined runbooks, roles, and processes for incident response.
- Specific measures to show cyber recovery readiness and risk.

**Looking ahead, what are the major trends and innovations in cyber resilience and recovery?**

Here are the major trends and innovations in cyber resilience and recovery according to the Commvault report "Overcoming Data Protection Fragmentation for Cyber-Resiliency":

**Increased Collaboration Between**

**ITOps and Security Teams:** The report highlights a breakdown of silos between IT operations (ITOps) and security teams. This fosters collaboration for a more holistic approach to cyber resilience, considering both security and recovery practices.

**AI-powered Security:** Artificial Intelligence (AI) is seen as a major innovation with 68% of respondents expecting it to improve security efforts. AI can automate tasks, enhance user authentication, and expedite threat detection and response.

**Overcoming Data Fragmentation:**

Fragmented data protection solutions using various tools create management complexities and hinder cyber resilience. The report suggests adopting modern platforms that consolidate data protection and streamline recovery processes.

**How do you see the role of Commvault evolving to help organizations stay ahead of future cyber threats?**

Commvault's role is evolving beyond just data protection and disaster recovery. It is transforming into a comprehensive cyber resilience provider for organizations. This shift is driven by the need for a layered approach to security, where organizations implement more than just a few basic measures. Commvault can offer solutions and guidance to help support this.

Additionally, disaster recovery planning is no longer sufficient on its own. Commvault recognizes the importance of frequent testing specifically designed for cyber recovery scenarios, suggesting they may be developing improved testing tools or incorporating them into their existing platform.

In addition, the findings from our recent study with GigaOm show a gap between perceived preparedness and cyber threats. We are constantly innovating and working on new ways to bridge this gap and ensure organizations have a realistic understanding of their cyber resilience. 📌

# HOW ENTERPRISES CAN RAISE THEIR CYBER SECURITY READINESS BY GOING THROUGH 3 STAGES OF PREPARATION

It is now well established that regional enterprises, small, medium or large, need to manage the eventuality of when they will be breached rather than, if they will be breached. Reacting to a cyber incident plunges an enterprise into a damage control mode and the extent to which the enterprise reacts depends on the severity of the cyber incident.

The more rigorous is the preparation of the enterprise to manage the cyber incident the more likely that it will be able to combat the cyber threat. While defending against any cyber incident requires skill, expertise and technology, it can be managed, and everything depends on the preparation efforts made by the enterprise.

Enterprises need to prepare, assess, and practice a cyber incident response plan that concludes with a recovery process. In the absence of this, well-rehearsed and practised, cyber security incident response plan, a Chief Security Officer would find it challenging to explain to the board, top executives and customers, why the organisation was not prepared to defend itself.

Corporate compliance around disclosure of cyber incidents means that publicity of the incident will eventually

take place in media. It is for this reason that regulators, auditors, and stakeholders expect enterprises to have a well-established cyber incident response in place to protect the impact on the corporate brand's reputation, as well as the impact on employees, customers and shareholders.

According to the 2023 Thales Data Threat Report, 51% of global organizations did not have a ransomware incident response plan. The imperative for enterprises is therefore to prepare a well-documented and well-rehearsed response plan for various types of incidents.

There are three primary stages for developing a cyber incident response plan.

## 1. Building a response process

The response process for a cyber incident should be documented and described in detail. This process will name a coordinator to ensure the process is rolled out sequentially, a grading of severity, and escalation paths in case of delays or failures.

Grading the incident by severity is an important part of this process and can use the area of impact as a guide, including whether the incident can impact

safety, privacy, finance, reputation, data, operations. Cyber security administrators may use internal levels of severity such as low, medium, high and whether it is a crisis or not.

Each of these category levels generates a unique process for response and a minimum escalation path. They also define the stakeholders who need to be informed and the service level agreements that need to be in place for remediation. Documenting the process with stakeholders and end users helps to build a joint team effort towards containment of the incident.

## 2. Detailed response plans

While building a generic response process to manage any type of cyber incident based on its severity is useful, it is also important to develop detailed response processes for specific types of incidents. Ransomware is a typical such incident that is commonly prevalent and capable of disrupting operations and is therefore a high impact and severe cyber incident.

The most important criteria here is to identify the point of attack and reduce the amount of time from the moment of attack to the point of containment, while limiting the disruption to business



**SINCE REGIONAL ENTERPRISES ARE CONTINUOUSLY FACING THE POSSIBILITY OF CYBER SECURITY INCIDENTS AND BREACHES, IT IS IMPORTANT FOR THEM TO RAISE THEIR LEVELS OF READINESS AND PREPARATION THROUGH WELL-DEFINED PLANS AND PROCESSES.**

operations, through well-built recovery and fail-over operations.

A typical cyber incident response plan for ransomware will identify and isolate the breached end points, will reset breached end user credentials, will analyze the incident and classify the ransomware attack and malware, and finally catalogue and document all indications of the breach.

Ransomware impacts the enterprise horizontally and vertically and the Chief Security Officer needs to collaborate with all stakeholders to build specific business and operations recovery plans.

### **3. Scenario simulations**

The last stage is to realistically simulate a cyber incident and get all end users and stakeholders to react as per the detailed response processes and operations that have been documented and made available. These simulations must include decision makers and top executives.

During the simulation, end users are alerted that a cyber incident has occurred, and its impact is simulated, for example loss of access to data or networks or specific applications or group of end users. As the simulation progresses, the various stakeholders and end users are alerted to the progress of the incident and are meant to react as per the defined processes and operations.

No advance information is provided to the end users and stakeholders about how the simulated crises will unfold and this uncertainty and their ability to take charge and react towards incident containment, begins to match typical real-life scenarios.

Real life cyber incidents are characterised by high levels of uncertainty and a continuously evolving situation that is best tackled by well-defined processes, responsibilities, and enterprise wide, group simulations. Better the preparation, the more likely that the incident response plan will progress satisfactorily. 📌



**IN THE ENTIRE YEAR OF 2023, THE COMPANY MITIGATED 14 MILLION DDOS ATTACKS, AND HALF WAY THROUGH 2024, IT HAS ALREADY MITIGATED 60% OF LAST YEAR'S FIGURE.**

# CLOUDFLARE REPORT HIGHLIGHTS DDoS ATTACK TRENDS IN Q2 2024

**C**loudflare, Inc., the security, performance, and reliability company helping to build a better Internet, has announced its 2024 Q2 DDoS report. This report includes insights and trends about the DDoS threat landscape — as observed across the global Cloudflare network, which is one of the largest in the world. With a 280 terabit per second network located across over 230 cities worldwide, serving 19% of all websites, Cloudflare holds a unique vantage point, which enables the company to provide valuable insights and trends to the broader Internet community.

## Threat actor sophistication fuels the continued increase in DDoS attacks

In the first half of 2024, Cloudflare mitigated 8.5 million DDoS attacks: 4.5 million in Q1 and 4 million in Q2. Overall, the number of DDoS attacks in Q2 decreased by 11% quarter-over-quarter, but increased 20% year-over-year.

For context, in the entire year of 2023, the company mitigated 14 million DDoS attacks, and half way through 2024, it has already mitigated 60% of last year's figure.

Cloudflare successfully mitigated 57 petabytes of network-layer DDoS attack traffic, preventing it from reaching its customers' origin servers..

## Ransom DDoS attacks

In May 2024, the percentage of attacked Cloudflare customers that reported being threatened by a DDoS attack threat actor, or subjected to a Ransom DDoS attack reached 16% – the highest it's been in the past 12 months. The quarter started relatively low, at 7% of customers reporting a threat or a ransom attack. That quickly jumped to 16% in May and

slightly dipped in June to 14%.

Overall, ransom DDoS attacks have been increasing quarter over quarter throughout the past year. In 2024 Q2, the percentage was 12.3%, slightly higher than the previous quarter (10.2%) but similar to the percentage of the year before (also 12.0%).

## Threat actors

75% of respondents reported that they did not know who attacked them or why. These respondents are Cloudflare customers that were targeted by HTTP DDoS attacks.

Of the respondents that claim they did know, 59% said it was a competitor who attacked them. Another 21% said the DDoS attack was carried out by a disgruntled customer or user, and another 17% said that the attacks were carried out by state-level or state-sponsored threat actors. The remaining 3% reported it being a self-inflicted DDoS attack.

## Top attacked countries and regions

In the second quarter of 2024, China was ranked the most attacked country in the world. This ranking takes into consideration HTTP DDoS attacks, network-layer DDoS attacks, the total volume and the percentage of DDoS attack traffic out of the total traffic.

After China, Turkey came in second place, followed by Singapore, Hong Kong, Russia, Brazil, and Thailand.

## Most attacked industries

The Information Technology & Services was ranked as the most targeted industry in the second quarter of 2024. In second, the Food & Beverages was the most attacked, following the Telecommunications, Services Providers and Carrier sector. Consumer Goods came in third place.

## Largest sources of DDoS attacks

Libya was ranked as the largest source of DDoS attacks in the second quarter of 2024. Indonesia followed closely in second place, followed by Netherlands in third.

## DDoS attack duration

The vast majority of DDoS attacks are short. Over 57% of HTTP DDoS attacks and 88% of network-layer DDoS attacks end within 10 minutes or less. This emphasizes the need for automated, in-line detection and mitigation systems. Ten minutes is hardly enough time for a human to respond to an alert, analyze the traffic, and apply manual mitigations. Approximately a quarter of HTTP DDoS attacks last over an hour, and almost a fifth last more than a day. On the network layer, longer attacks are significantly less common. Only 1% of network-layer DDoS attacks last more than 3 hours.

Commenting on the report, Bashar Bashaireh, Managing Director & Head of Sales - Middle East and Türkiye at Cloudflare, "The majority of DDoS attacks are small and quick. However, even these attacks can disrupt online services that do not follow best practices for DDoS defence. Threat actor sophistication is increasing, perhaps due to the availability of Generative AI and developer copilots, resulting in attack code that delivers DDoS attacks that are harder to defend against. Even before the rise in attack sophistication, many organizations struggled to defend against these threats on their own. But they don't need to. Cloudflare is here to help. We invest significant resources – so you don't have to – to ensure our automated defences, along with the entire portfolio of Cloudflare security products, can mitigate emerging threats." 🔑





# CYBER RESILIENCE: THE KEYSTONE OF MODERN CYBERSECURITY

SECURITY ADVISOR ME EXAMINES THE RELEVANCE OF CYBER RESILIENCE IN AN AGE WHERE DIGITAL TECHNOLOGY UNDERPINS EVERY FACET OF OUR LIVES.

In an age where digital technology underpins nearly every facet of our lives, the importance of cybersecurity has never been more pronounced.

However, as cyber threats grow in both number and sophistication, merely having defensive measures in place is no longer sufficient. To truly safeguard against the multifaceted dangers of the digital world, organizations must adopt a comprehensive cyber resilience framework. This approach not only emphasizes the prevention of cyberattacks but also ensures a robust strategy for recovery and continuity in the face of inevitable breaches.

#### The Evolving Threat Landscape

The cyber threat landscape is continually evolving, with attackers employing increasingly sophisticated tactics. Traditional methods such as malware and phishing are now

supplemented by advanced persistent threats (APTs), ransomware, and zero-day exploits. These attacks target vulnerabilities across the entire digital infrastructure, from endpoints and servers to cloud services and IoT devices. In such a dynamic environment, a static security posture is inadequate.

#### Understanding Cyber Resilience

Cyber resilience goes beyond conventional cybersecurity, encompassing the ability of an organization to prepare for, respond to, and recover from cyber incidents. It is a holistic approach that integrates

cybersecurity, business continuity, and risk management into a unified strategy. The key components of a robust cyber resilience framework include:

- 1. Risk Assessment and Management:** Identifying and evaluating potential threats and vulnerabilities is the first step. This involves continuous monitoring and analysis to understand the evolving risk landscape.
- 2. Preventive Measures:** Implementing robust security

DEVELOPING A CYBER RESILIENCE FRAMEWORK  
REQUIRES A HOLISTIC APPROACH,  
INTEGRATING CYBERSECURITY EFFORTS  
ACROSS ALL LEVELS OF THE ORGANIZATION.

controls such as firewalls, intrusion detection systems, and encryption to protect against known threats. Regular updates and patches are crucial to mitigate vulnerabilities.

**3. Detection and Response:** Developing capabilities for rapid detection of and response to cyber incidents. This includes real-time monitoring, incident response plans, and the deployment of security information and event management (SIEM) systems.

**4. Recovery and Continuity:** Establishing procedures for data backup, disaster recovery, and business continuity to ensure that operations can be quickly restored following a cyber incident.

**5. Training and Awareness: Educating** employees on cybersecurity best practices and the importance of their role

**TO TRULY SAFEGUARD AGAINST THE MULTIFACETED DANGERS OF THE DIGITAL WORLD, ORGANIZATIONS MUST ADOPT A COMPREHENSIVE CYBER RESILIENCE FRAMEWORK.**

in maintaining the organization's security posture. This includes regular training sessions and simulated phishing attacks to test readiness.

**The Strategic Importance of Cyber Resilience**

**Mitigating Impact of Breaches:** While preventing every cyberattack is unrealistic, a strong cyber resilience framework minimizes the impact of breaches. Effective incident response and recovery strategies ensure that business operations can continue with minimal disruption.

**Protecting Reputation and Trust:**

Data breaches can severely damage an organization's reputation and erode customer trust. Demonstrating a commitment to cyber resilience reassures stakeholders that the organization is well-prepared to handle cyber threats, maintaining confidence and loyalty.

**Compliance and Regulatory**

**Requirements:** Many industries are subject to stringent regulations regarding data protection and cybersecurity. A robust cyber resilience framework





helps ensure compliance with these regulations, avoiding potential fines and legal repercussions.

**Financial Stability:** Cyber incidents can result in significant financial losses due to operational downtime, data loss, and remediation costs. By minimizing the impact of these incidents, organizations can protect their financial health and stability.

#### **Building a Cyber Resilience Framework**

**Holistic Approach:** Developing a cyber resilience framework requires a holistic approach, integrating cybersecurity efforts across all levels of the organization. Collaboration between IT,

operations, and executive leadership is essential.

**Continuous Improvement:** Cyber resilience is not a one-time effort but a continuous process. Regularly updating and testing security measures, conducting drills, and staying informed about the latest threats and technologies are critical to maintaining a robust defense.

**Leverage Technology:** Advanced technologies such as artificial intelligence, machine learning, and automation can enhance threat detection and response capabilities. Investing in these technologies provides a proactive defense against emerging threats.

**Third-Party Partnerships:** Collaborating with cybersecurity experts and service providers can augment internal capabilities. These partnerships provide access to specialized knowledge and resources, enhancing the overall resilience of the organization.

#### **Conclusion**

In conclusion, building a strong cyber resilience framework is essential for navigating the complex and ever-changing cyber threat landscape. It is not just about preventing attacks but ensuring that organizations can withstand and quickly recover from them. By adopting a comprehensive, proactive approach to cybersecurity, organizations can protect their assets, maintain trust, and secure their future in the digital age. Cyber resilience is the foundation upon which modern cybersecurity must be built, offering a path to sustained security and operational continuity in an increasingly hostile digital world. 🛡️

→ **WHILE PREVENTING EVERY CYBERATTACK IS UNREALISTIC, A STRONG CYBER RESILIENCE FRAMEWORK MINIMIZES THE IMPACT OF BREACHES.**

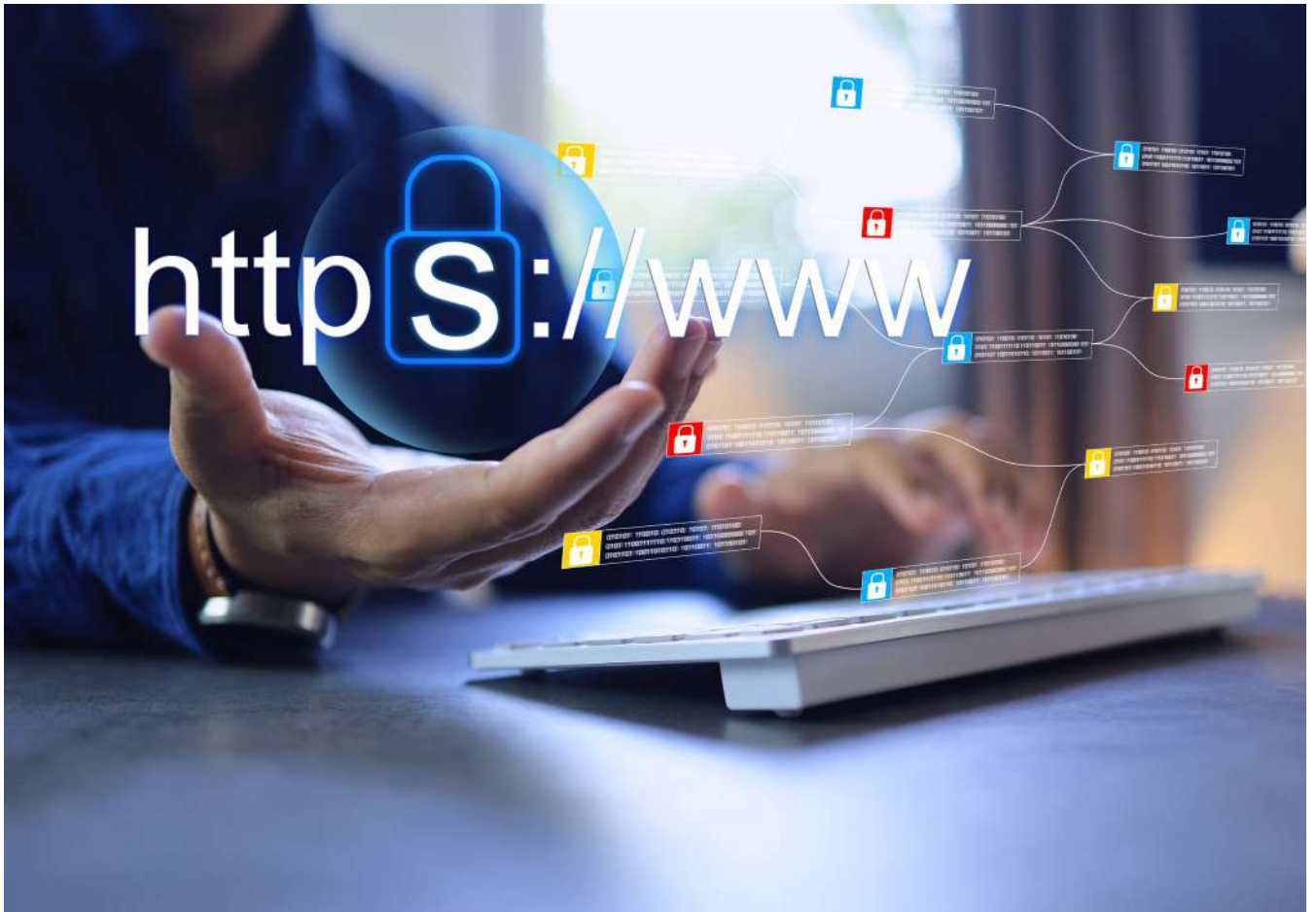
# ATTACKERS EXPLOIT URL PROTECTION SERVICES TO CONCEAL MALICIOUS LINKS IN PHISHING ATTACKS: BARRACUDA



In a novel attack technique, cybercriminals are abusing legitimate URL protection services to hide malicious URLs in phishing emails, according to a new Threat Spotlight from Barracuda Networks.

From mid-May 2024 onwards, Barracuda researchers observed phishing attacks taking advantage of three different URL protection services to mask their phishing URLs. The services are provided by trusted, legitimate brands. To date, these attacks have targeted hundreds of companies, if not more.

URL protection services work by copying URL links found in emails, rewriting them, and then embedding the original within the rewritten one, rather like a wrap. When the email recipient



clicks on the link, it triggers an email security scan of the original URL. If the scan is clear, the user is redirected to the URL. In the attacks seen, the users were redirected to phishing pages designed to steal sensitive information.

Barracuda researchers believe it is likely that the attackers initially gained entry to the URL protection services after compromising the accounts of legitimate users.

Once the attacker had taken over an email account, they could impersonate the owner, and infiltrate and examine their email communications, also known

as business email compromise (BEC) or conversation hijacking. Links in emails connected to the account, or in the user's email signature, would have shown whether a URL protection service was being used, and which one.

Using the compromised account to send themselves a phishing email carrying their malicious link, the attackers would have been able to get the protection URL they needed for their phishing campaigns.

"This inventive tactic helps attackers to evade security detection, and the abuse of trusted, legitimate security

brands means that recipients are more likely to feel safe and click on the malicious link," said Saravanan Mohankumar, Manager, Threat Analyst at Barracuda. "The URL protection provider may not be able to validate whether the redirect URL is being used by a customer or by an intruder who has taken over the account. Phishing is a powerful and often successful threat, and cybercriminals will continue to evolve their tools and techniques to maintain this. Security teams need to be prepared."

Barracuda recommends a multilayered, AI-powered approach to defence, which can detect and block unusual or unexpected activity, however complex. These security measures should be complemented by active and regular security awareness training for employees on the latest threats and how to spot and report them. 📌

**THE URL PROTECTION PROVIDER MAY NOT BE ABLE TO VALIDATE WHETHER THE REDIRECT URL IS BEING USED BY A CUSTOMER OR BY AN INTRUDER WHO HAS TAKEN OVER THE ACCOUNT.**

# MANAGEENGINE SHIELD 2024: REVOLUTIONIZING IAM AND IT SECURITY



**T**he ManageEngine Shield 2024 seminar, held in the UAE, marked a pivotal moment in the identity and access management (IAM) and IT security sectors. This landmark event convened industry experts, thought leaders, and key stakeholders to explore and address the rapidly changing security landscape.

ManageEngine showcased its deep understanding of industry trends and the evolving security environment. Recognizing the critical role of identities in the era of cloud adoption, ManageEngine provides state-of-the-art solutions that empower enterprises to adopt an identity-driven security approach. These cutting-edge solutions enable organizations to navigate the difficulties of identity access and security, providing both strong protection and streamlined operations. Shield 2024 offered invaluable insights and solutions to tackle these challenges, delivering substantial value to all attendees.

Anita Joseph caught up with Sujoy Banerjee, Associate Director of ManageEngine Sales, MEA region to discuss the latest trends in Security Information and Event Management (SIEM), how organizations in the UAE are adapting to the rising complexity of

data breaches, and the best practices for implementing SIEM solutions.

### **What are the latest trends in SIEM that organizations in the UAE should be aware of?**

In the realm of SIEM, several notable trends are emerging that organizations in the UAE should be keenly aware of. Firstly, there's a significant shift towards integrating artificial intelligence (AI) and machine learning (ML) within SIEM solutions. These technologies are revolutionizing how threats are detected and responded to by providing advanced analytics, predictive capabilities, and automated threat hunting.

Another trend is the increasing adoption of cloud-based SIEM solutions. As more organizations in the UAE move their operations to the cloud, they seek SIEM tools that can seamlessly integrate with their cloud environments. This not only ensures better scalability but also enhances real-time monitoring and incident response across hybrid infrastructures.

Lastly, we are seeing a push towards simplifying the complexity of SIEM systems. Vendors are developing more user-friendly interfaces and dashboards that provide actionable insights without requiring extensive expertise. This trend is particularly beneficial for organizations that may not have large, specialized IT security teams.

### **What are the primary challenges that UAE organizations face regarding data breaches and cybersecurity?**

One of the foremost issues that UAE organizations face with respect to cybersecurity is the rapidly evolving threat landscape. Cyber attackers are becoming more sophisticated,

employing advanced techniques such as ransomware, phishing, and zero-day exploits. Keeping pace with these evolving threats requires continuous vigilance and adaptation of security strategies.

The complexity of IT environments in the UAE also poses a challenge. Many organizations operate in hybrid settings with a mix of on-premise, cloud, and IoT devices. Ensuring comprehensive security across such diverse environments can be daunting and requires integrated, holistic SIEM solutions.

There's also the issue of regulatory compliance. As data protection laws and regulations become stricter, organizations must navigate a complex web of compliance requirements. Failing to comply can result in hefty fines and damage to reputation, adding pressure on organizations to implement robust security measures.

Lastly, insider threats remain a persistent challenge. Whether intentional or accidental, insider actions can lead to significant data breaches. Organizations must implement stringent access controls, continuous monitoring, and effective training programs to mitigate these risks.

### **How do local regulations and compliance requirements impact the adoption of SIEM solutions in the UAE?**

With the introduction of data protection laws such as the UAE's NESA, ISR, organizations are mandated to ensure the security and privacy of personal data. SIEM solutions play a critical role in helping organizations achieve and maintain compliance by providing comprehensive monitoring, logging, and reporting capabilities.

These regulations often require

**AS MORE ORGANIZATIONS IN THE UAE MOVE THEIR OPERATIONS TO THE CLOUD, THEY SEEK SIEM TOOLS THAT CAN SEAMLESSLY INTEGRATE WITH THEIR CLOUD ENVIRONMENTS.**

organizations to maintain detailed records of all security incidents, breaches, and access logs. SIEM solutions facilitate this by automatically collecting and storing the necessary data, making it easier for organizations to generate compliance reports and demonstrate adherence to regulatory requirements during audits.

Furthermore, the threat of substantial fines and legal repercussions for non-compliance drives organizations to adopt advanced SIEM solutions that can provide real-time alerts and automated responses to potential breaches. This proactive approach not only helps in meeting regulatory requirements but also in minimizing the risk of data breaches and mitigating their impact when they occur.

Overall, local regulations and compliance requirements act as a catalyst for the adoption of SIEM solutions in the UAE, pushing organizations to invest in robust security measures to protect sensitive data and maintain regulatory compliance.

### **What is ManageEngine's vision for UAE for 2025?**

ManageEngine's vision for the UAE in 2025 is centered on empowering organizations to leverage technology for

**OVERALL, LOCAL REGULATIONS AND COMPLIANCE REQUIREMENTS ACT AS A CATALYST FOR THE ADOPTION OF SIEM SOLUTIONS IN THE UAE**



driving efficiency, innovation, and growth. We aim to significantly reduce manual tasks and enhance operational efficiency through automation. A key aspect of our vision is creating a secure digital ecosystem that prioritizes the protection of critical assets and data. With the rapid adoption of cloud technology in the UAE, we are committed to ensuring the robust protection of data and applications in cloud environments. Adhering to both local and international regulations is paramount, and we strive to foster partnerships between the government, private sector, and academia to collectively address the evolving cybersecurity challenges.

**How has the cybersecurity landscape in the UAE evolved in recent years, and how has your company adapted to these changes?**

The UAE has undergone a rapid digital transformation in recent years, positioning itself as a global tech hub. To mitigate the associated risks, the government has implemented stricter cybersecurity regulations and compliance standards. Protecting essential services

like energy, transportation, and healthcare has become a top priority. Additionally, with data becoming a valuable asset, safeguarding personal information has gained significant importance. The use of AI, machine learning, and automation in cybersecurity has accelerated to counter evolving threats. In response, ManageEngine has invested in robust threat intelligence platforms and developed tailored cybersecurity solutions for specific sectors such as finance, healthcare, and government. We also assist organizations in achieving compliance with local and international regulations and invest

**MANY ORGANIZATIONS OPERATE IN HYBRID SETTINGS WITH A MIX OF ON-PREMISE, CLOUD, AND IOT DEVICES.**

in training and certifications to build a skilled cybersecurity workforce.

**How do you see the future of cybersecurity in the UAE, and what is your company's role in shaping that future?**

Looking ahead, cybersecurity in the UAE will become a core business function, evolving from a reactive to a proactive strategy. Data privacy regulations will intensify, and AI and automation will play a critical role in threat detection, incident response, and predictive security. The demand for skilled cybersecurity professionals will continue to grow. ManageEngine is poised to be a trusted cybersecurity partner, providing comprehensive solutions tailored to the unique needs of UAE organizations. We are heavily investing in research and development to stay ahead of emerging threats and develop cutting-edge technologies. Furthermore, we are committed to building cybersecurity awareness and resilience through training and education initiatives, ensuring that organizations are well-prepared to face future challenges. 🛡️





# CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD  
CLEANROOM™ RECOVERY



Visit [commvault.com](https://www.commvault.com) to Learn More



## CHINESE HOTPAGE BROWSER INJECTOR OPENS SYSTEM TO OTHER VULNERABILITIES: ESET

**E**SET Research has discovered a sophisticated Chinese browser injector: a signed, vulnerable, ad-injecting driver from a mysterious Chinese company. This threat, which ESET dubbed HotPage, comes self-contained in an executable file that installs its main driver and injects libraries into Chromium-based browsers. Posing as a security product capable of blocking advertisements, it actually introduces new ads. Additionally, the malware can replace the content of the current page, redirect the user, or simply open a new tab to a website full of other ads. The malware introduces more vulnerabilities and leaves the system open to even more dangerous threats. An attacker with a non-privileged account could leverage the vulnerable driver to obtain SYSTEM privileges or inject libraries into remote processes to cause further damage, all while using a legitimate and signed driver.

At the end of 2023, ESET researchers stumbled upon an installer named "HotPage.exe" that deploys a driver capable of injecting code into remote processes, and two libraries capable of intercepting and tampering with browsers' network traffic. The installer was detected by most security products as an adware component. What really stood out to ESET researchers was the embedded driver signed by Microsoft. According to its signature, it was developed by a Chinese company named Hubei Dunwang Network Technology Co., Ltd.

According to available information, the business scope of the company includes technology-related activities such as development, services, and consulting – but also advertising activities. The principal shareholder is currently Wuhan Yishun Baishun Culture Media Co., Ltd., a very small company that looks to be specialized in advertising and marketing. Due to the level of privileges needed to install the driver, the malware might

have been bundled with other software packages or advertised as a security product.

Using Windows' notification callbacks, the driver component monitors new browsers or tabs being opened. Under certain conditions, the adware will use various techniques to inject shellcode into browser processes to load its network-tampering libraries. Using Microsoft's Detours hooking library, the injected code filters HTTP(S) requests and responses. The malware can replace the content of the current page, redirect the user, or simply open a new tab to a website full of gaming ads. On top of its obvious mischievous behavior, this kernel component leaves the door open for other threats to run code at the highest privilege level available in the Windows operating system: the SYSTEM account. Due to improper access restrictions to this kernel component, any process can communicate with it and leverage its code injection capability to target any non-protected processes. 🔒

# OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT sets new standard in cybersecurity with first-ever

# 100%

rating in SE Labs CDR [content disarm & reconstruction] test.



**Talk to one of our experts today or book a demo**

[opswat.com/get-started](https://opswat.com/get-started)

**Read the full SE Labs report**

[selabs.uk/reports](https://selabs.uk/reports)



# Transform

**Your Network**  
*with Smart Managed Switches*

**5**  
YEARS  
WARRANTY



Full-duplex networking  
with 10G SFP+ fiber  
uplink ports



Easy-to-use  
management interface



Advanced Web Smart  
managed features



Upgrade to the latest generation of switches from D-Link for unparalleled performance and flexibility. With advanced features and seamless integration, the DGS-1250 Series ensures your business network operates at peak efficiency.

## Experience the future of networking today

### Advanced Features:

Benefit from features like loopback detection, cable diagnostics, and VLAN support for efficient network maintenance.

### Green Technology:

Save energy and reduce costs with power-saving features like link status detection and system hibernation.

### Easy Management:

Enjoy intuitive management with D-Link Network Assistant utility and Full CLI support.



**IPv6 Ready**

PoE and non-PoE Options

Layer2 Series

10G Fiber uplinks

Connect to more...