CLOUDFLARE

EXECUTIVE GUIDE

Unified risk posture:

A CISO’s guide to reducing risk and complexity

Content

Beyond risk management: Unified risk posture

As a CISO, you own cybersecurity and risk management. Yet, you do not always "own" all the technologies and digital assets that create risk for your business, such as:

- The Internet-connected applications, devices, clouds, and networks used by your employees and third-parties
- The data being created, stored, and shared by your workforce and customers
- The code and APIs built and used by your developers

Over time, organizations accumulated many point solutions, trying to extend protections across increasingly distributed IT environments. But too often, these tools operate in silos with limited interoperability to build a holistic view of risk, and the data they generate can be overwhelming to security staff. Altogether, managing this fragmentation has required too much manual effort, time, and expertise to prioritize risk effectively.

This complexity leads to danger. For example, according to a survey from TechTarget's Enterprise Strategy Group, **three-fourths (76%) of organizations have experienced a cyberattack due to an unknown, unmanaged, or poorly managed Internet-facing asset.**

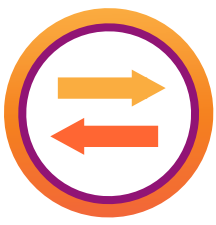
Improving your cybersecurity posture across today's distributed environment requires change. As attack surfaces expand, organizations should explore a more unified, more integrated approach to risk posture management in order to:

- **Mitigate** risk more effectively — with less effort
- **Optimize** what can be done with existing tools and risk signals
- **Adapt** faster to meet evolving risks
- **Automate** more security workflows

"Unified risk posture: A CISO's guide to reducing risk and complexity" will explain the benefits, use cases, and a three-stage framework (below) to think about risk management. Read on to learn more.

3-stage framework

Evaluate risk throughout IT environments



...by exchanging risk indicators between tools for a more holistic view

...to enforce risk controls and protect the business.

What is unified risk posture management?

Many component pieces — one holistic goal

At a high level, risk management requires three key jobs:

1. Evaluating risk throughout IT environments with dynamic first-party risk scoring models
2. Exchanging risk indicators – meaning sharing data between tools – to build a more comprehensive view of risk
3. Enforcing controls based on what you have learned – in automated, consistent ways

Unifying risk posture simplifies this process by accomplishing these steps in as few security systems as possible — ideally with one platform. Bringing together dynamic first-party risk scoring, integrations to share context between security tools, and automated security measures in this way equips organizations with a stronger center of gravity to assess, prioritize, and mitigate risk.

This approach becomes more powerful the more you can extend visibility and controls across your attack surface, including to protect people, apps, data, and networks.

Plus, by converging these risk management jobs into one platform, you can reduce reliance on point solutions, do more with the risk signals within your existing IT ecosystem, and apply protections everywhere.

Unifying risk posture management helps you adapt to evolving internal and external risks across vectors, including:

User risks

- Phishing
- Ransomware
- Remote access
- Mobile devices / BYOD
- Third parties / supply chain
- ...and more

Data risks

- Data loss / exposure
- Data theft / breach
- Privacy violations
- Compliance violations
- Data tampering
- ...and more

Application risks

- Denial of service
- Zero-day exploits
- SQL injection
- Cross-site scripting
- Account takeovers
- Shadow IT — including shadow APIs
- ...and more

Benefits of unified risk posture management

Unifying these evaluation, exchange, and enforcement stages helps organizations manage risk posture across their attack surface with less effort and complexity.

Benefits	Sample metrics
Reduce effort in SecOps with less manual policy building & greater agility in responding to incidents	• Increase # of automated workflows • Reduce # of clicks to build policies • Reduce mean time to detect (MTTD) • Reduce mean time to detect (MTTD)
Reduce cyber risk with automated and dynamic risk posture enforcement across your attack surface	• Reduce # of critical incidents • Increase # of threats blocked automatically

Security technologies and their role in unifying risk posture

Security service edge (SSE) platforms enable organizations to secure access, defend against threats, and protect data across the web, SaaS, and private app environments. This broad reach equips SSE platforms with unique visibility into user activity across IT environments, which enriches models to identify risky and suspicious behavior in real-time. Moreover, the cloud-delivered SSE approach to network security helps centralize policy building and enforcement throughout an organization.

If SSE is largely about defending an organization's internal IT infrastructure, web application and API security **(WAAP)** is about defending its public-facing attack surface. This means guarding against a wide-range of risks, including vulnerability exploits, bots, unauthorized access, fraud, abuse, and denial-of-service.

Converging SSE and WAAP capabilities with a single platform can help organizations extend risk management across the key areas of people, apps, and data.

Other well-established technologies complement SSE and WAAP security platforms:

- **Security information and event management (SIEM) and extended detection and response (XDR)** platforms aggregate logs and risk information across environments to enable monitoring, analysis, and reporting. Many enterprises rely on these tools to investigate and respond to incidents and to support compliance.
- Enterprises also often rely on endpoint security to secure devices and identity and access management tools to authenticate users. As additional layers of security, these tools provide rich intelligence on device and user activity, which can then be shared across security platforms.

Alone, any of the technologies listed above have some limitations on how far they can extend visibility and controls over your attack surface. However, **tapping into the capabilities and intelligence of your entire security ecosystem is foundational to more effective risk posture management.**

Step 1: Evaluate Risk

Simplify risk scoring across users with SSE

User and entity behavior analytics (UEBA) models play a powerful role in helping organizations adapt to evolving risks. Often using machine learning, UEBA models detect unusual or dangerous activity among users, devices, and other entities and then alert security teams to take action. This saves significant manual analysis and helps security keep up with threats.

In practice, however, deploying UEBA models can still be inefficient. For example, these models are often used within SIEM and XDR tools, which then require fine tuning and customization to avoid inaccuracy that can be unsustainable at scale, even for well-resourced SOCs.

Instead, embedding risk scoring directly within an SSE platform helps with consistent logging and rules across web, SaaS, and private apps. This avoids the complexity of using UEBA models exclusively within SIEMs/XDRs. SSE platforms can quickly 'close the loop' between detecting risky behavior and enforcing policies (e.g. blocking traffic) across network security environments.

User risk scoring examples

User risk scoring — a component of UEBA — examines user activity for suspicious and unsafe actions. More dangerous actions yield higher scores, representing likelihood of compromise, an insider threat, or other risks. User risk scoring is common within SSE platforms, which have direct visibility across network activity.

For example, users can be scored in real-time as high risk by:

- **Impossible travel:** When a user completes a login from two different locations within an unreasonably short timeframe (e.g. an employee logs in from New York City and then a few minutes later logs in from Sydney)
- **Repeated data loss prevention (DLP) violations:** When sensitive or confidential information is moved, shared, or access in ways that go against company policy or regulations (e.g. developer attempts to upload proprietary source code into a third-party AI chatbot)
- **Repeated use of risky devices:** When devices are deemed unsafe or in violation of company policies (e.g. lack latest OS updates; have unpatched vulnerabilities)

Bringing together risk evaluation across users and apps

SSE platforms are an increasingly popular modern foundation to detect user-level risk with UEBA models. But with today's focus on IT consolidation, organizations are looking for ways to extend risk evaluation further to cover threats to public-facing apps, sites, and APIs.

Converging SSE and web application and API security capabilities onto one platform equips business with visibility, controls, and shared intelligence across users and apps, representing a significant percentage of a typical organization's attack surface.

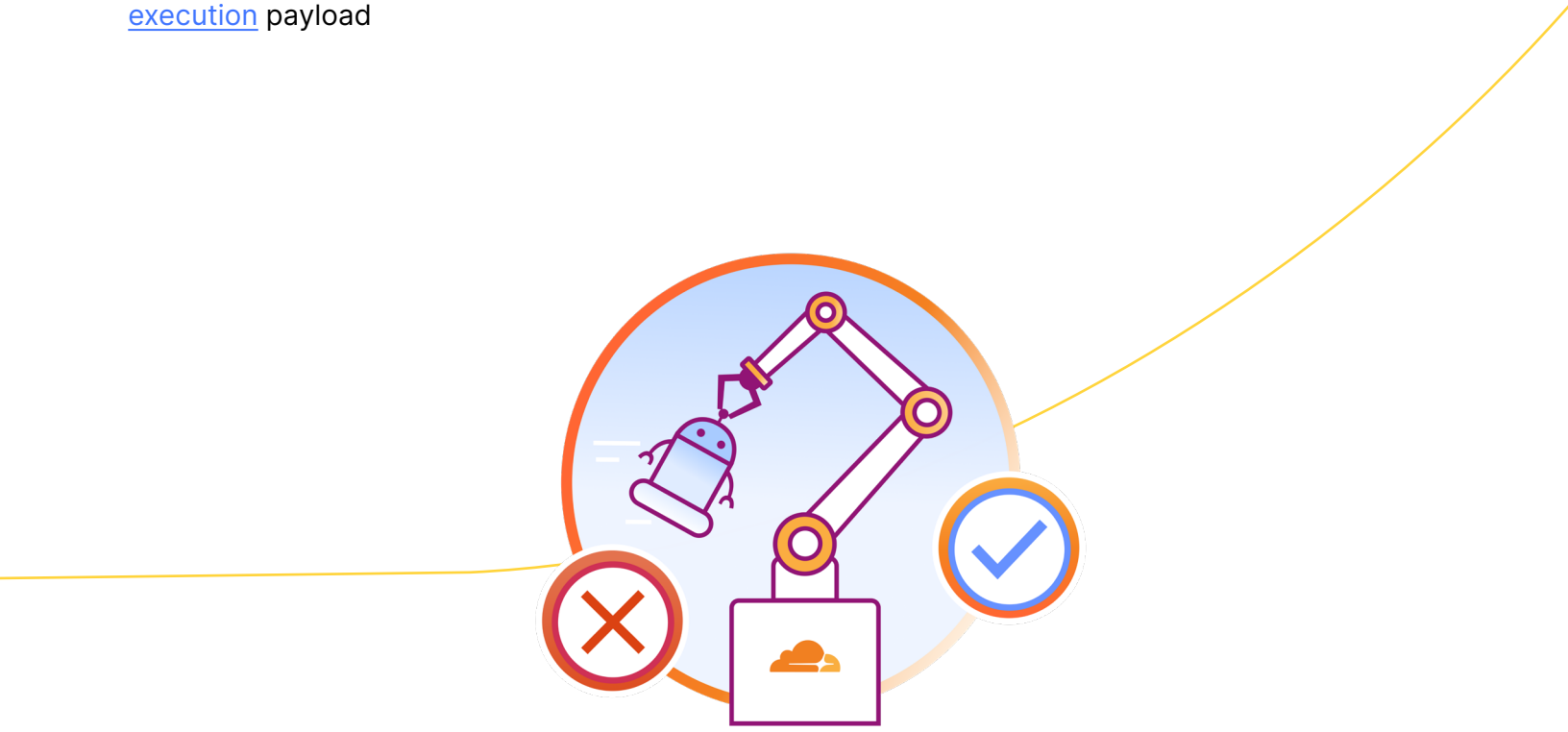
Example models for risks to apps

To protect apps, for example, Cloudflare's platform detects and mitigates malicious payloads and bots using risk models backed by machine learning (ML) including:

- Our **WAF attack score**, which scores whether a request contains a zero-day exploit, or common OWASP Top 10 risks such as a SQL injection, cross-site scripting, or remote code execution payload
- Our **bot score**, which scores the likelihood that a request came from a bot
- Our **malicious script classifier**, which looks at the dangers of browser scripts for your website visitors

Other ML models help security teams discover new API endpoints and schemas without requiring any prerequisite customer input.

Visibility across your application infrastructure helps proactively surface risks in dashboards like exposed RDP servers, unproxied DNS records, domains without TLD encryption, and more.



Step 2: Exchange risk indicators

Do more with existing tools, with less effort

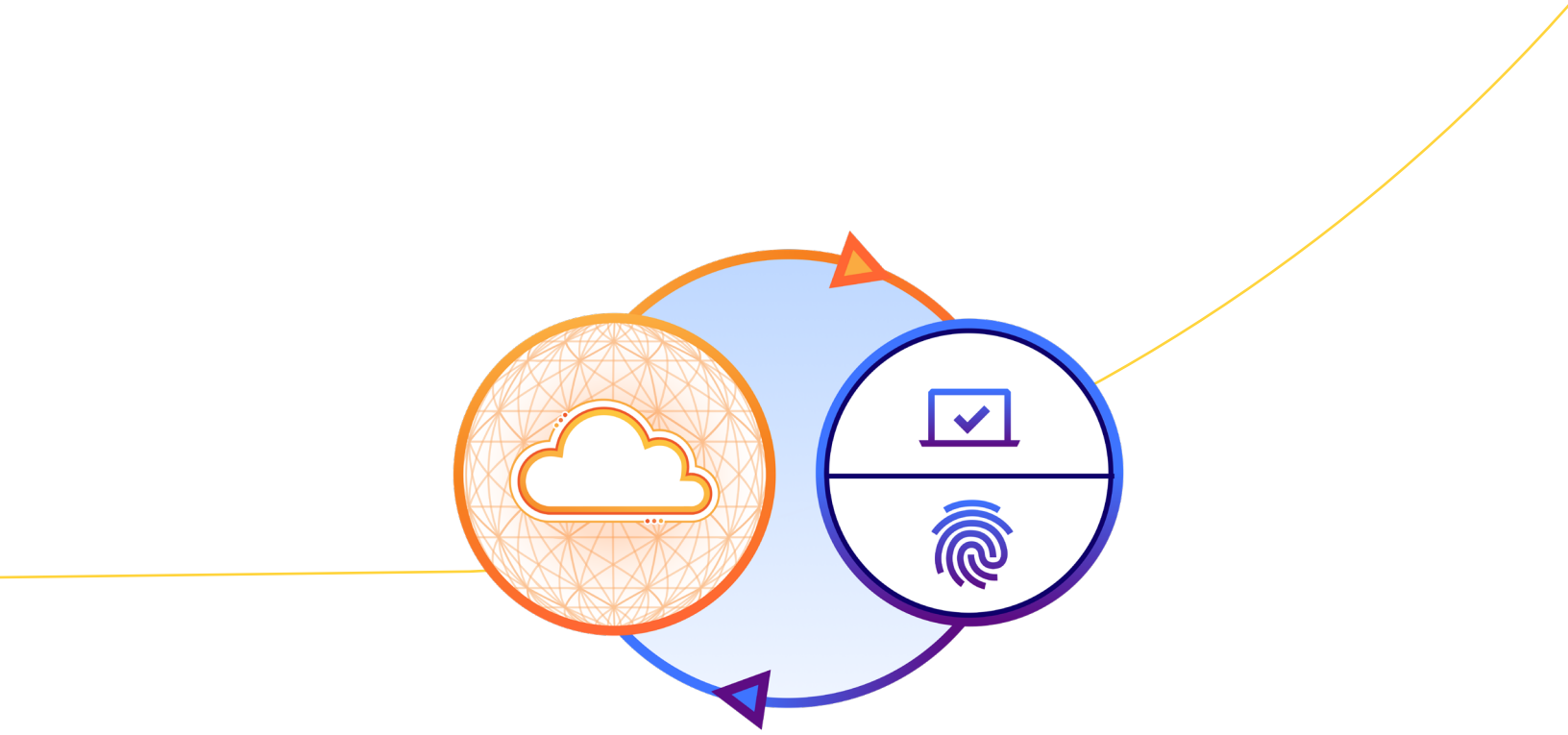
Imagine that your security team successfully identified (and stopped) a phishing attempt against contractor "Bob Fisher." Seeing a user targeted by a phishing campaign may be enough to flag that user as risky — which is consistent with the first step we just outlined. Increasing that user's risk score can translate to more restricted access to systems.

But, was this an isolated incident? Are the same adversaries continuing to target Bob or other employees in different ways? Has his device been compromised?

CISOs need the big picture — not just one set of logs — to continuously maintain and improve their organization's cybersecurity posture.

For effective and efficient threat response, CISOs require automated two-way exchange of risk indicators with their broader ecosystem of tools including:

- **Identity providers (IdP)** store and manage your users' digital identitiess
- **Endpoint protection (EPP)** protect the devices that connect to your network
- **Security information and event management (SIEM)** collect, analyze, and manage your log and event data to look for signs of a security incident
- **Extended detection and response (XDR)** streamline the ingestion of security data analysis and help you enforce further prevention and remediation

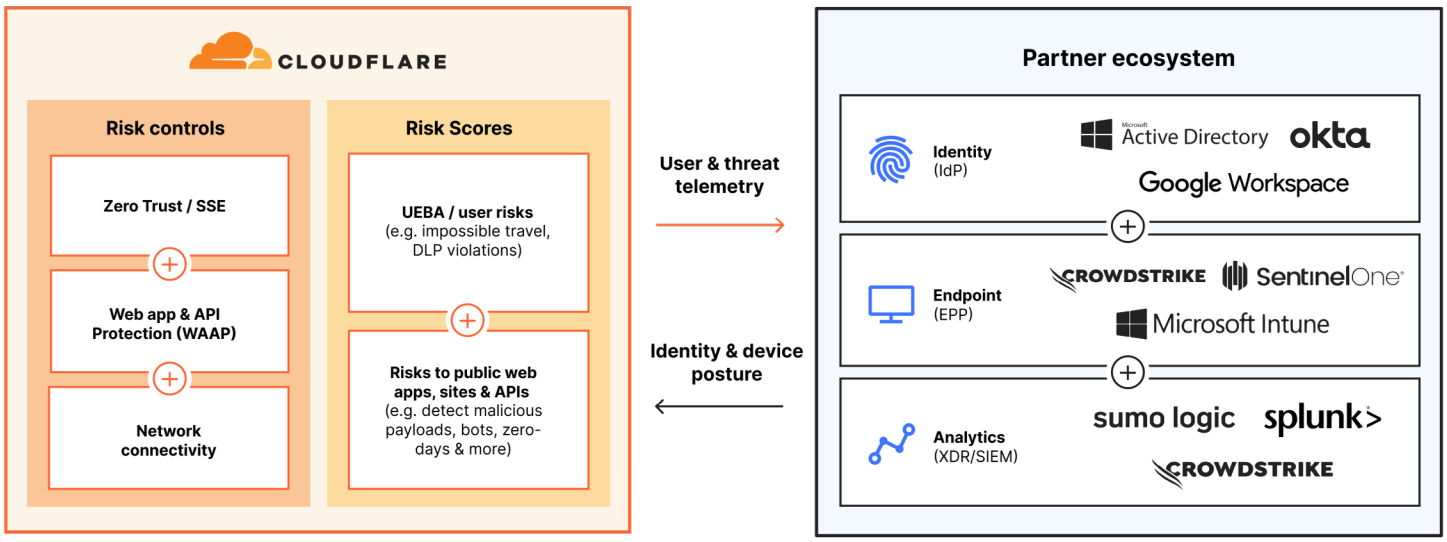


So, in the incident involving "Bob," unified risk posture management reduces the burden on your SecOps teams by automatically exchanging information with your existing security tools:

1. Telemetry from Cloudflare, including logs on blocked activity and even individual user risk scores, is shared across your security ecosystem, including with SIEM and XDR tools that can continue with deeper automated scans in parallel.
2. Those security tools report back dynamic risk intelligence to Cloudflare — for example, IdP and EPP partners can share their user and device risk scores back for Cloudflare to build in as posture checks to restrict access.

One-time integrations of Cloudflare with these EPP, IdP, XDR, and SIEM tools provide CISOs with more visibility and automate security orchestration across multiple domains — so your SecOps teams can **do more with your existing tools.**

Cloudflare's first party risk evaluation and risk exchange with best-in-class partners



Step 3: Enforce

Automate risk controls across the growing attack surface

With the first two steps, CISOs can build a dynamic and holistic view of risk across their environments.

But the final step is the most important: enforcing controls and protections based on what you've learned in steps 1 and 2. A unified platform that brings together all three steps helps apply policies consistently across all locations and environments, so security evolves to your needs.

The following three use cases illustrate how enforcement makes the benefits of unified risk posture management a reality with Cloudflare.

Use case #1: Adopt Zero Trust with device posture checks

Cloudflare works with your EPP and SIEM tools to enforce Zero Trust controls that adapt to risks across your workforce.

For example, consider a scenario where threat actors are targeting a user across various channels including web and email. Cloudflare will:

- **Deliver the first line of defense** by blocking browsing to risky websites and phishing emails
- **Ingest device posture from your EPP tool,** which has scanned and determined that user's device is infected
- **Restrict that user's access** to applications based on your EPP's device posture
- **Share log data** with your SIEM / XDR for further analysis, which can lead to further remediation steps like quarantining the device

Use case #2: Protect apps, APIs, and sites — even from zero-day threats

It is difficult for security teams to keep up with the non-stop attacks using zero-day vulnerabilities, bots, malicious third-party client-side scripts, injections, and other exploits.

To defend apps, APIs, and sites, Cloudflare helps:

- **Automatically block** malicious payloads, bots, and even zero-days using ML-backed risk models that identify attack variations and dangerous or anomalous traffic.
- **Centralize visibility** with dashboards and analytics to review potential misconfigurations, data leakage risks, and vulnerabilities that impact your infrastructure.

With Cloudflare, the same security that organizations can place in front of public-facing apps (like WAF, DDoS mitigation, and bot management) can also be used to protect internal infrastructure like self-hosted Jira and Confluence servers.

Use case #3: Protect sensitive data

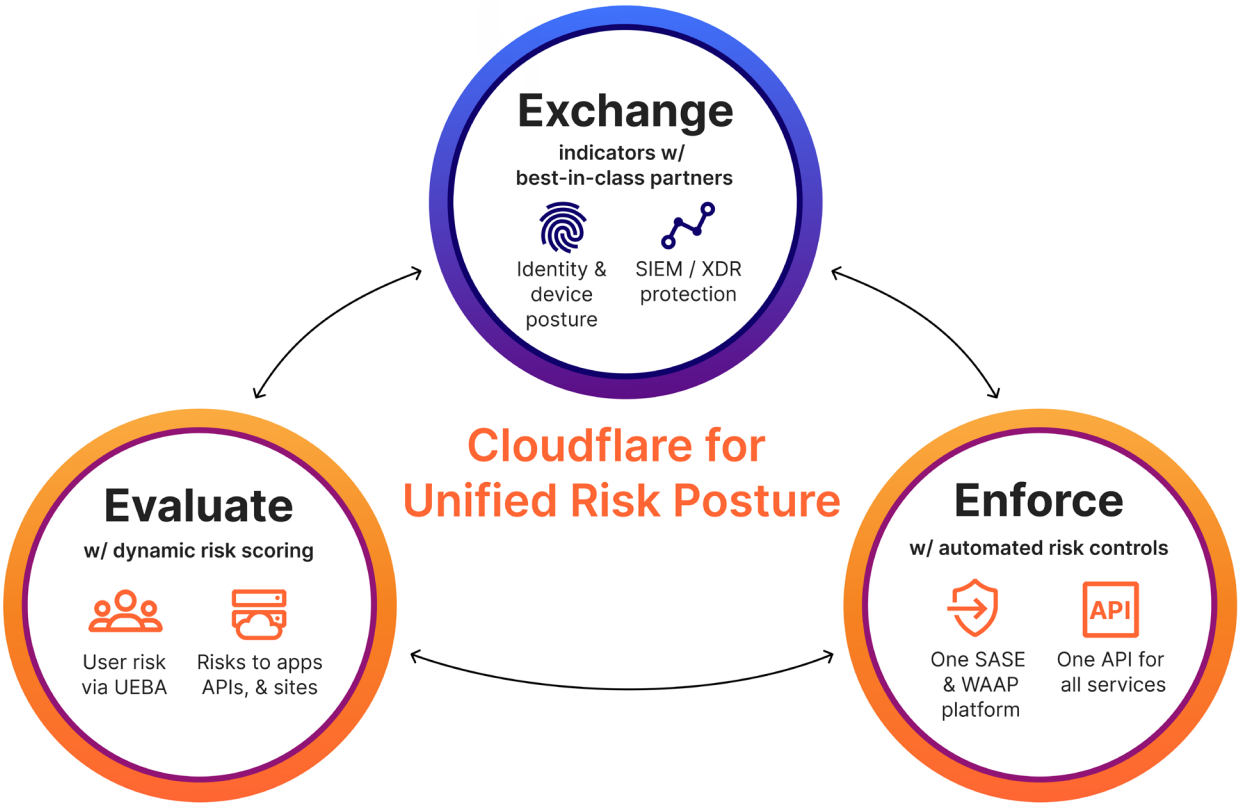
With the sheer volume of big data, IoT devices, and now the popularity of AI and LLMs, it is harder than ever to maintain visibility and security controls over how data is shared across cloud environments.

Cloudflare makes it simple to identify high-risk users handling sensitive data — and restrict access accordingly.

For instance, if a developer attempts to upload proprietary source code to a public GitHub repository, Cloudflare will:

- **Enforce data controls** to block that upload and prevent the code from leaving your corporate tenants
- **Increase the user's risk score** (via UEBA) based on this suspicious activity, allowing security staff to investigate further
- **Restrict access** until the investigation is complete, either by isolating or blocking access entirely to business apps

Why Cloudflare for Unified Risk Posture



Simplicity | One platform for unified risk posture

Cloudflare reduces operational overhead by consolidating security and simplifying how you manage risk across people, applications, and networks.

By converging SSE and WAAP risk scoring and controls on one platform and global network, Cloudflare helps you eliminate multiple, overlapping tools that introduce redundancy, blind-spots, and hidden costs.

- Reduce time and effort spent on policy building and enforcement
- Extend protections at your own pace with limitless interoperability between services
- Orchestrate all services with our single API, which enables customization and automation
- Minimize and protect your attack surface with Zero Trust best practices

"Cloudflare is helping us mitigate risk more effectively with less effort and simplifies how we deliver Zero Trust across my organization."

indeed

Why Cloudflare for Unified Risk Posture

Flexibility | One-time integrations with best-in-class partners

Cloudflare works with the tools you already use to exchange risk data. Unlike with other vendors, establish integrations only once and leverage those capabilities across Cloudflare's entire platform, so you can focus on risk management, not set up.

Endpoint protection providers (EPPs): When a user logs in to an application protected by Cloudflare, we can verify whether the device is protected by an EPP, who can check if the device has been infected with malware or has any other active security threats present. In some cases, Cloudflare ingests risk scores from EPP partners to further verify if a device is deemed too risky to access internal apps or network capabilities. This instantaneous exchange of information shuts down threats automatically.

Identity providers (IdPs): Meanwhile, identity providers verify that employees accessing the network are who they say they are. Cloudflare works with leading IdPs to thwart fraudulent access attempts, including incidents of impossible travel.

SIEM / XDR providers: Our collaboration also extends to SIEM and XDR partners, who ingest comprehensive data from Cloudflare into a centralized dashboard. This empowers security analysts to swiftly detect and respond to security threats. Some XDRs, including those backed by AI / ML, prompt analysts with high-fidelity alerts, enabling decisive responses to neutralize threats before they escalate.

Scale | One global network for enforcement and threat intelligence

Every security service is available for customers to run across each of our 320+ network locations (as of Q1 2024). Single-pass inspection and policy enforcement are always fast, consistent and resilient.

Plus, our AI/ML-powered models to identity risks are powered by unique data from our global network including:

- Visibility as a reverse proxy used by nearly 20% of all web
- ~3 trillion DNS queries per day
- Crawls of more than 8 billion web pages every 2 weeks
- 209 billion cyber threats blocked each day on average

"Having a single Cloudflare solution in place to help us manage complexity across our global operations has made our lives so much easier. Cloudflare has supported us every step of the way."

Delivery Hero

Learn more

Cloudflare for Unified Risk Posture is a new suite of cybersecurity risk management capabilities that help enterprises with automated and dynamic risk posture enforcement across their expanding attack surface.

Learn more about Cloudflare's unified approach

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-5826.2024MAY15