WAF Benchmark Report

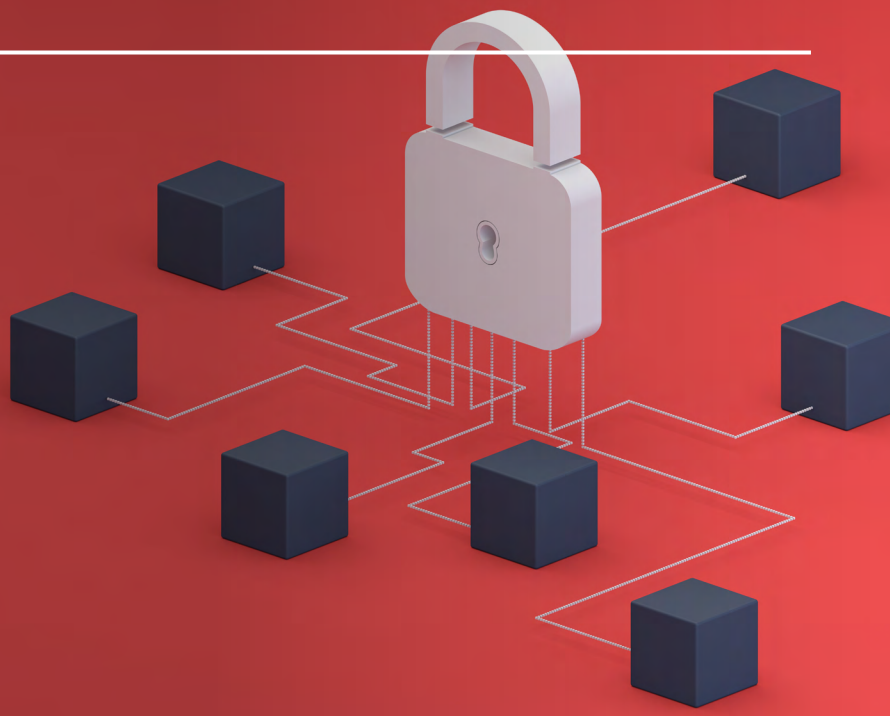
A review of last year's threats and a look at this year's solutions.

verizon

Table of contents

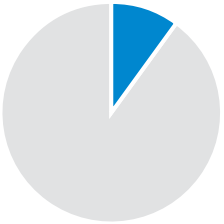
Making security job 1

Last year was a transitional year for application security. Rapid digitization in 2020 exposed new application surfaces to old vulnerabilities. And new vulnerabilities and attack types such as bots targeting APIs and Layer 7 volumetric DDoS attacks, plagued application stacks. These issues were compounded by a shortage of security talent, remote working arrangements and the Great Resignation, leaving IT, security and development departments scrambling to ensure adequate network and app protection.



To assess the impact these challenges had on businesses, Verizon commissioned a survey to understand how organizations are adapting their application security practices. The findings confirm what we suspected:

1. Application security teams are small compared to the rest of the organization
2. Security teams' responsibilities have increased
3. Organizations want to improve their speed in responding to security events
4. The industry needs better intelligence and visibility into attacks
5. Security teams need to identify and remove vulnerabilities to better triage bugs



ONLY

10%

of those surveyed reported that application security is their dedicated focus, suggesting that it is just one (small) part of their responsibilities.

90%

Of those surveyed said application security responsibilities had increased year over year, which isn't surprising, given the increase in certain types of high-profile attacks in the past 24 months, such as ransomware and the SolarWinds breach.

Given these increased security demands, making application security a shared responsibility should be a business priority. Here's where the survey group will be focusing its efforts in 2022.

Improving application security in 2022

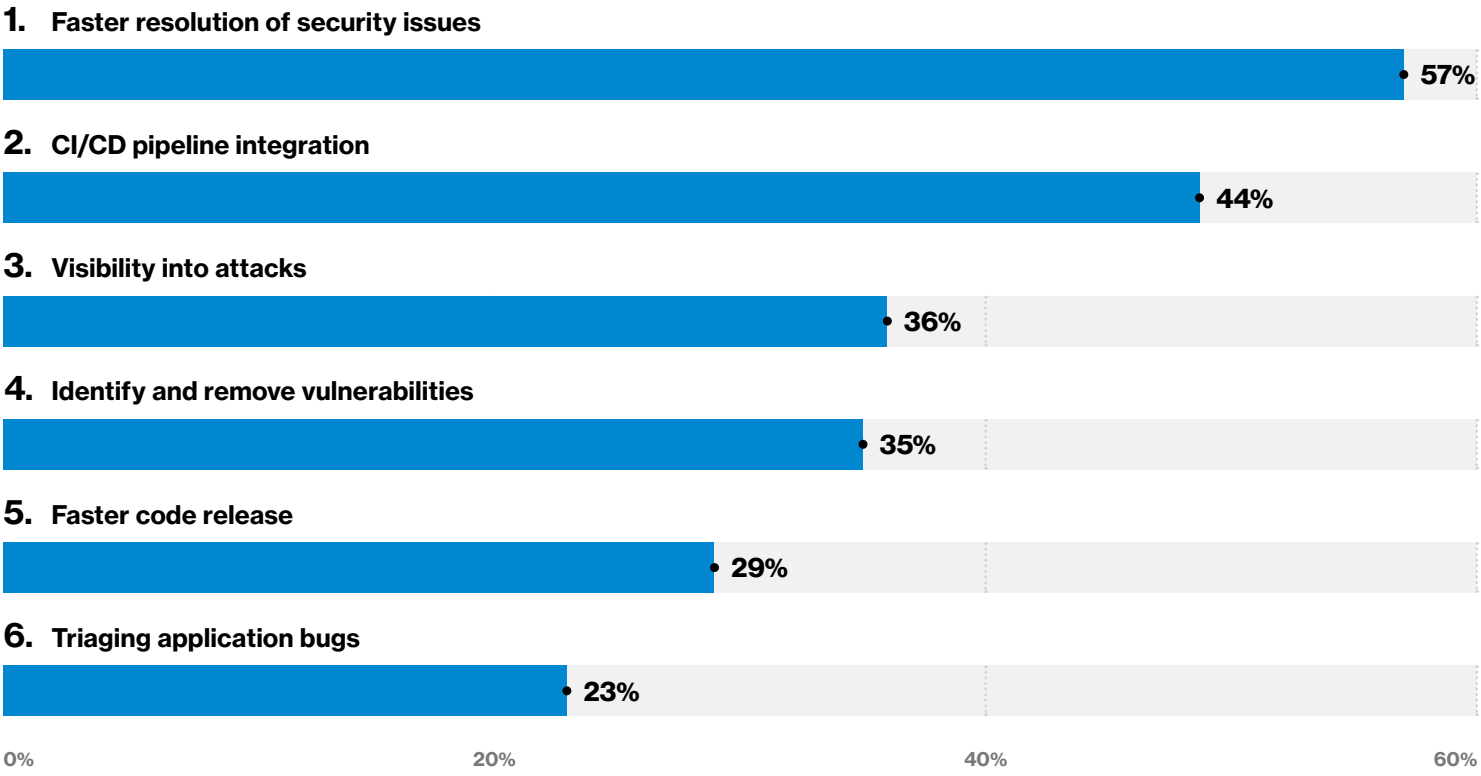
A common challenge with reducing the application attack surface is that your web applications are in constant motion – evolving and adding new features.

Implementing security fixes clogs application pipelines, forcing tradeoffs between business, engineering and security interests. Removing old vulnerabilities, especially from legacy applications, pulls developer and project management teams away from current business focus/ investment areas. In both of these scenarios, bad actors count on management lapses and inaction to find and exploit vulnerabilities.

The survey asked respondents about their organization's priorities for the next twelve months around application security (AppSec), analytics, security operations, software development and IT operations (DevOps).

Question

What are the top application security-related analytics and intelligence challenges you/your business will focus on solving in the next 12 months?



1. Faster resolution of security issues.

The survey showed that 57% of respondents want to focus on faster resolution of security issues in their operations. The quicker security issues are addressed, the less potential for damaging breaches. A company can save more than $1 million **by containing a breach in less than 30 days**.[1] An **average breach costs $4.42 million**, so organizations should resolve security issues quickly.[2] A business that employs security automation can reduce its average time to **detect and contain a breach by up to 77 days**.[3] Although not all operational security issues are related to a breach, having overall faster resolution times help reduce damage when a breach occurs.

A key strategy for improving the speed of security is reducing reaction time. Having a system and process that enables correlating events from various sources can help detect security issues faster and provide sufficient information to determine the root cause. The first step is to have the web application firewall (WAF), web application and servers send logs and events to a security information and event management (SIEM). The SIEM analyzes the data and determines patterns. It can create an alert or support ticket when it detects an anomaly.

In some cases, SIEMs can launch automated responses. If it generates a ticket, some ticketing systems can group tickets, allowing associating user-reported tickets to provide more insight into the issue. This type of integration can enable faster detections and empowers personnel to respond to issues promptly. Furthermore, fixes can be used to update the application, server and WAF to improve their security postures and detection process.

$1M+

Can be saved by a company who contains a security breech in less than 30 days.

$4.42M

Average cost of a security breech.

77 Days

The average reduction in time to detect and contain a breach once security automation is employed.

2. CI/CD pipeline integration and faster code release.

Development teams play a critical role in the security of internet-facing applications. While bad actors are the most significant threat these teams encounter, they also face internal challenges implementing security fixes while balancing business, engineering and security interests.

Given the focus on digital transformation, it's no surprise that continuous integration and delivery (CI/CD) and faster code releases were the top two focus areas for DevOps. This shift left reinforces the approach of making security an ongoing part of development – not a single task attached to the release process. The CI/CD pipeline can perform static code analysis when it's checked in and before it's approved in a pull request. The pipeline can run dynamic scans and automated penetration testing on the web application during the integration and testing stages. Findings can be assessed, and fixes checked in and tested prior to the software's release. By the time the application is released to the production system, the CI/CD pipeline will have tested it numerous times.

3. Visibility into attacks.

Respondents stated that visibility and better alerts are priorities for their security analytics. A SIEM helps with the faster resolution of security issues by providing visibility of attacks and patterns that could indicate emerging threats. A SIEM that integrates with a traditional on-premise WAF or a cloud WAF can use the event data to find anomalies and new patterns. Suppose a threat actor is performing reconnaissance on the web application, a SIEM can alert on the increase of the 4XX and 5XX, or that the web traffic is deviating from typical web patterns. Yet, some requests do not reach the web application when the application uses a CDN. Therefore, if you're using a CDN, ensure you capture CDN logs into your SIEM to resolve all requests and potential errors. These can be enriched with data from your other systems to create intelligent alerting and help operations and security teams analyze and investigate anomalies.

When a CDN WAF is also activated, the SIEM can use the CDN events in addition to WAF blocks to provide a complete, end-to-end picture of normal traffic patterns, anomalies and security threats. Here's an example of a CDN WAF in action. **Plus500**, a leading trading platform, used a CDN WAF to build a robust threat intelligence pipeline to inform them of emerging security threats and to allow them to deploy code faster and more securely.

Plus500 uses the intelligence they get from the CDN and WAF to help its development teams identify vulnerabilities before deployment. With an audit WAF profile, new software can be tested against real production traffic and attacks. Developers can see how the WAF rules interact with application changes. Read the **case study** for additional details.

4. Removing vulnerabilities.

As security shifts left, it becomes a shared responsibility. This distributed accountability may be one of the reasons removing vulnerabilities from application code was cited as a priority by nearly 40% of respondents. The 2020 Verizon Data Breach Investigations Report confirmed that web applications are commonly breached via older (four or more years old) vulnerabilities. Bad actors continually exploit these older vulnerabilities because they're often the stacks IT security teams ignore. They're also easy to research, find exploits for, and wwrelatively inexpensive to mount.

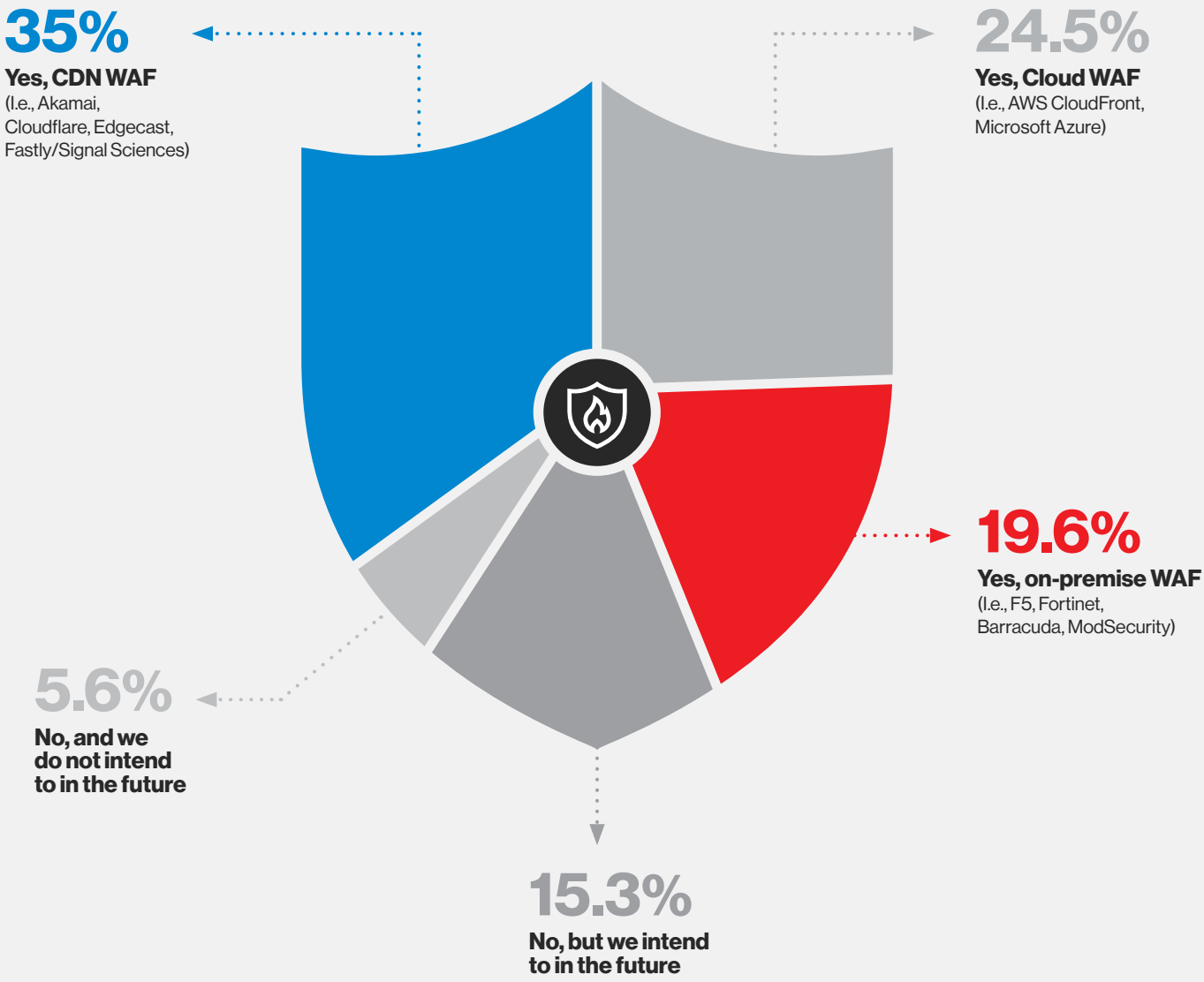
Read this recent **blog** to learn the **five security questions** that you should be asking and answering to improve awareness of your applications security needs and reduce the risk of a web application security event impacting your business.

Improving WAF management

According to our survey, an overwhelming majority of organizations use a web application firewall (WAF) to protect their web applications. The majority of respondents are leveraging a CDN-based or Cloud WAF, with less than 20% using a premise-based WAF. This result is consistent with our 2020 survey, where the majority of respondents indicated plans to replace their premise-based WAF with a cloud or CDN-based WAF.

Question

Is your organization using a WAF?

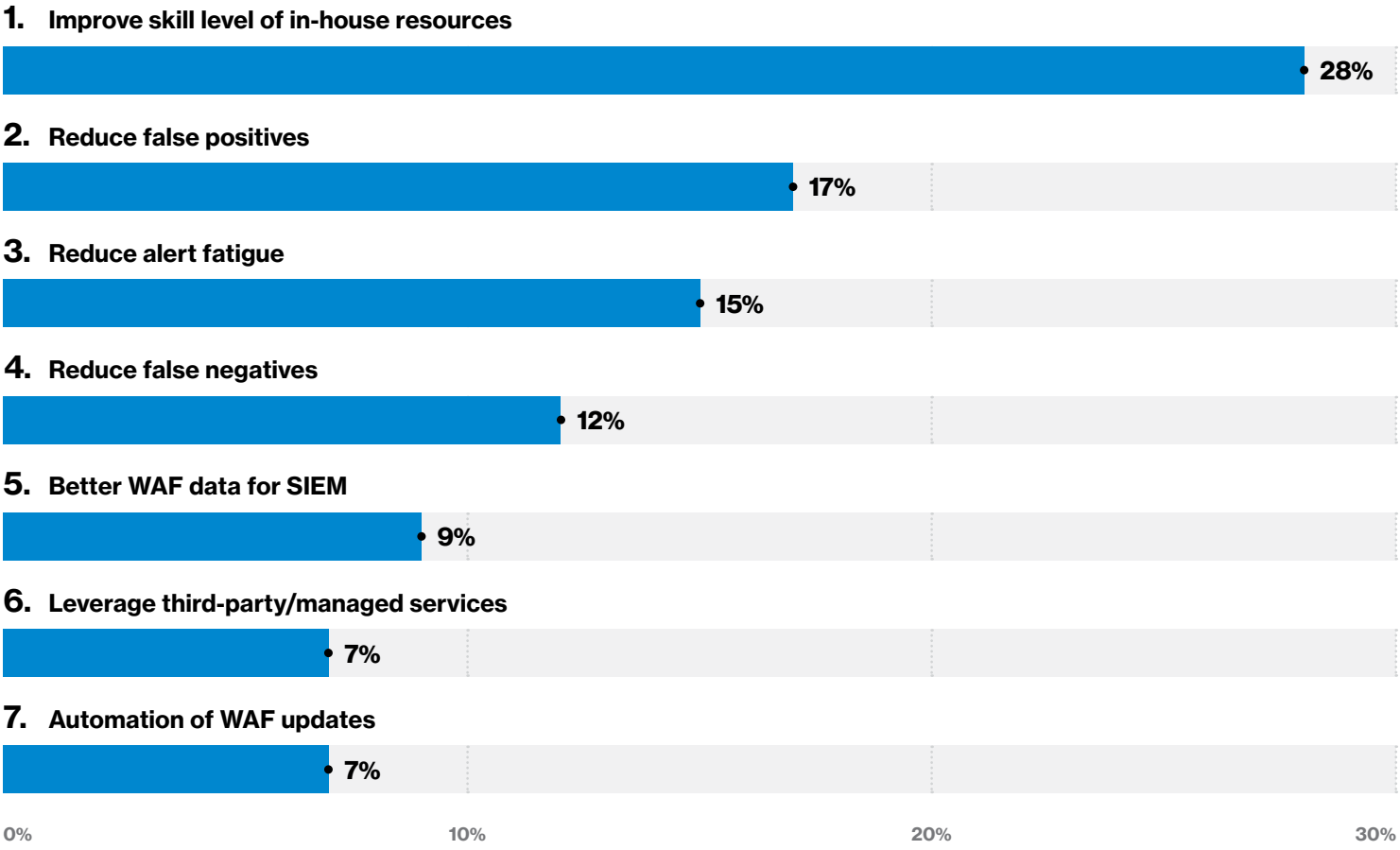


The large majority of respondents indicated satisfaction with their WAFs. Cloud and CDN WAFs offer several advantages compared to their on-premise counterparts. Verizon Web Security is application and API protection built on our global content delivery network. It has the horsepower to inspect and filter every request to your web application without slowing down your systems. Additional security capabilities such as DDoS protection, fraud and bot management can also be integrated into the CDN edge, keeping malicious traffic far from your critical web infrastructure. The large volume of internet traffic passing through the CDN informs threat engineers about new dangers in real time, providing customers on the system with regular, automated rule updates with each discovery.

When asked to rank their top concerns with WAF management, it's not surprising that most respondents pointed to a lack of internal skills to manage their systems. They also wanted to prevent false positives, which correlates with WAF expertise that's needed to tune the WAF rules and signatures.

Question

How would you like to see your WAF management improve?



According to the survey, 10% of respondents indicated that WAF management/application security is their dedicated focus. And 47% of these multithreaded staff mentioned their application security responsibilities had increased year over year. The extra responsibilities may leave these team members with little time for professional development, compounding the challenge of maintaining the WAF, which leads to increased false positives, alert fatigue and many of the other challenges indicated in the chart above.

Solving the security skills gap will be a top priority throughout 2022. But employee shortages may lead organizations to conclude that enabling in-house teams with better WAF management and application security skills is the best option.

Conclusion

Verizon Web Security solution is application and API protection built on our global content delivery network. It has the horsepower to inspect and filter every request to your web application without slowing down your systems. It's been engineered to:

- Remove malicious threats
- See and respond to attacks
- Improve security operations
- Protect your users and your data
- Deliver a better user experience

Improve visibility

Verizon Web Security gives you an end-to-end view of every user – good and bad – coming into your web application all the way to your server. You can view this information in out-of-the box dashboards, and also as raw logs. We enrich this data for a complete picture of your users and attackers – from location to device to header and cookies. Use this information to monitor, alert, analyze and improve your security and performance.

Create actionable intelligence

By integrating a SIEM with Verizon, security events provide intelligence data that can correlate with application events. Verizon WAF and CDN provide real-time log delivery into SIEMs. Security teams can build custom dashboards, enable analytics and configure alerting using all the data sources.

Reduce false positives

By leveraging the Dual WAF mode, security teams can tune WAF rules to reduce unnecessary alerts and discover new rules to avoid missing critical security events. Read our blog on tuning WAF rules to **learn more**.

Release secure code faster

With a parallel WAF engine running production traffic in audit mode, Verizon Web Security enables you to test changes to your application code and WAF rules before being implemented into production. Empower your developers with predictive threat intelligence throughout the CI/CD pipeline and release secure code faster.

Automate and scale the WAF

Verizon provides best practices in managing the WAF without overcomplicating them and making them easier to scale. Security teams can automate WAF management and deployment by leveraging CI/CD pipelines and the WAF APIs to embrace the infrastructure as a code principle. The CI/CD pipeline automatically deploys the WAF rules to the Dual WAF and the production WAF according to the stage of the software release. This automated process ensures faster deployments with a reduced risk of errors.

Get expert support

Our industry-leading Managed Cloud Security (MCS) service consists of two groups of expert security professionals: the Cloud Security Advisory, which ensures your WAF is tuned and updated to protect against the latest threats, and the Computer Security Incident Response Team, a dedicated group of security professionals who monitor your website and apps 24/7 for anomalies and potential misuse. These groups, along with our advanced security technologies and services help protect your business against an evolving threat landscape.

Methodology

The survey was conducted between October 4-15, 2021, and included 168 respondents, of which 81% were from companies with less than 1,000 employees.

Resources

1 IBM, 2020. "Cost of a data breach report," IBM.com.

2 IBM, 2021. "How much does a data breach cost?" IBM.com.

3 IBM, August 2021, "Cost of a data breach. A view from the cloud," IBM.com.

Harden your security
Don't wait another day to protect your infrastructure, applications, content and reputation. Speak with one of our security experts now.

verizon.com/business/products/security/web-security

verizon

Verizon Communications Inc. (NYSE, Nasdaq: VZ) was formed on June 30, 2000 and is one of the world's leading providers of technology and communications services. Headquartered in New York City and with a presence around the world, Verizon generated revenues of $133.6 billion in 2021. The company offers data, video and voice services and solutions on its award-winning networks and platforms, delivering on customers' demand for mobility, reliable network connectivity, security and control.

Learn more about how Verizon is powering experiences of the future at verizon.com/business/products/security/web-security