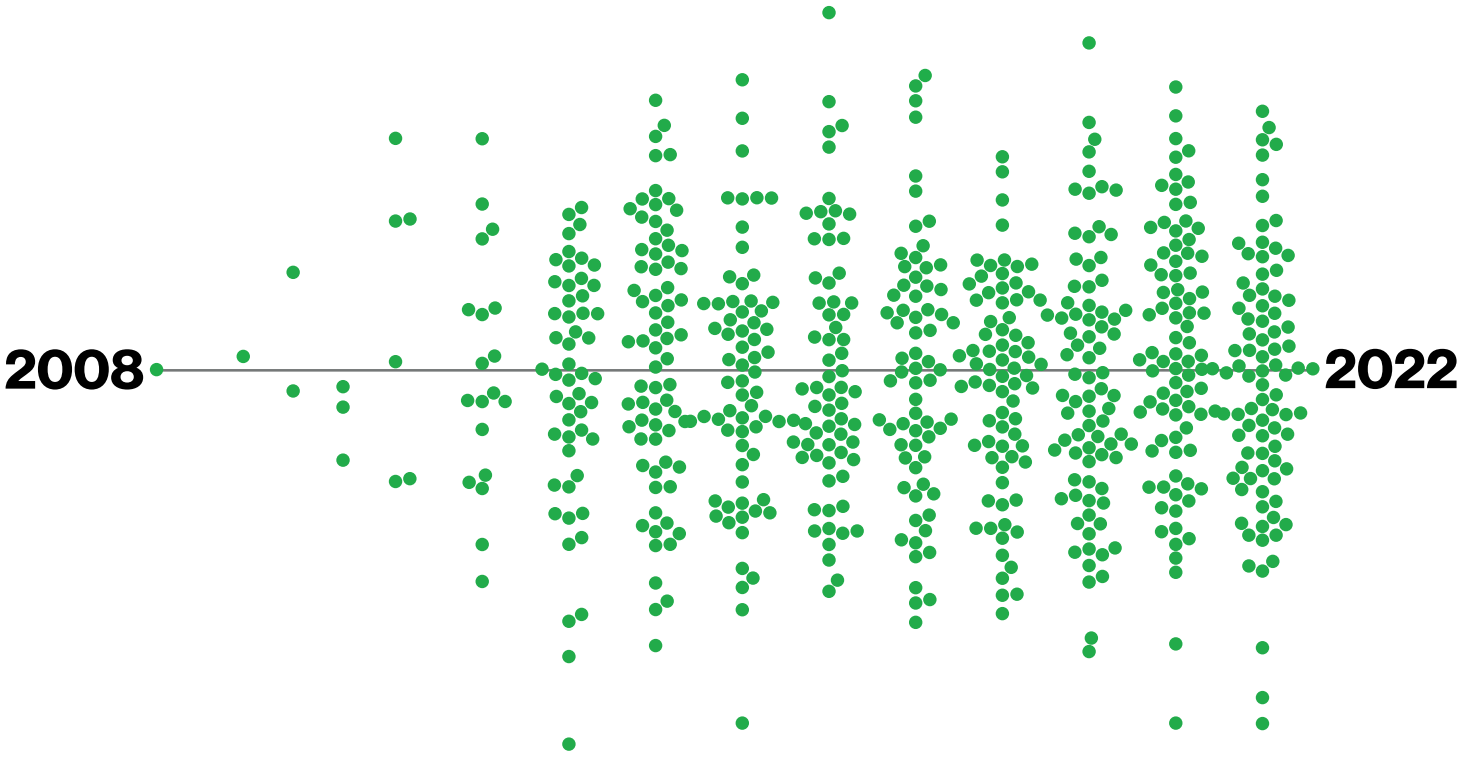
DBIR

2022 Data Breach Investigations Report

Executive Summary



About the cover

Our long-time readers may recall that the cover for our inaugural report back in 2008 depicted an empty chair in a server room. It was intended to convey the fact that many organizations are not properly minding their assets and data. The 2022 cover is a throwback to that report, both for purposes of nostalgia and to convey that many organizations continue to struggle with keeping an eye on their people and their systems. The overlay of the timeline with the dot plot illustrates the number of global contributors that have joined us over the 15-year history of the report (broken out by year).

Table of contents

Welcome to the 15th annual Verizon Data Breach Investigations Report

As introduced in the 2018 report, the DBIR provides "a place for security practitioners to look for data-driven, real-world views on what commonly befalls companies with regard to cybercrime." For this, our 15th anniversary installment, we continue in that same tradition by providing insight into what threats your organization is likely to face today, along with the occasional look back at previous reports and how the threat landscape has changed over the intervening years.

Speaking of change, the past year has been extraordinary in a number of ways, but it was certainly memorable with regard to the murky world of cybercrime. From very well-publicized critical infrastructure attacks to massive supply chain breaches, the financially motivated criminals and nefarious nation-state actors have rarely, if ever, come out swinging the way they did over the past 12 months. As in past years, we will examine what our data has to tell us about these and other common action types used against enterprise. This year we looked at 23,896 incidents, 5,212 of which were confirmed breaches. This data represents actual real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC) or provided to us by our 87 global contributors, without whose generous help this document could not be produced. We hope that you can use this report and the information it contains to increase your awareness of the most common tactics used against organizations at large and against your specific industry, and what you can do to protect your company and its assets. While we routinely compare and contrast trends in the report, this year, in honor of the 15th publication, we attempt as often as possible to illustrate how tactics have evolved over the years, as in Figure 1 and Figure 2 below. Read on for report highlights, pass this summary to colleagues and download the full report for a detailed view of the threats you face today. Without further ado, let's jump into the details.

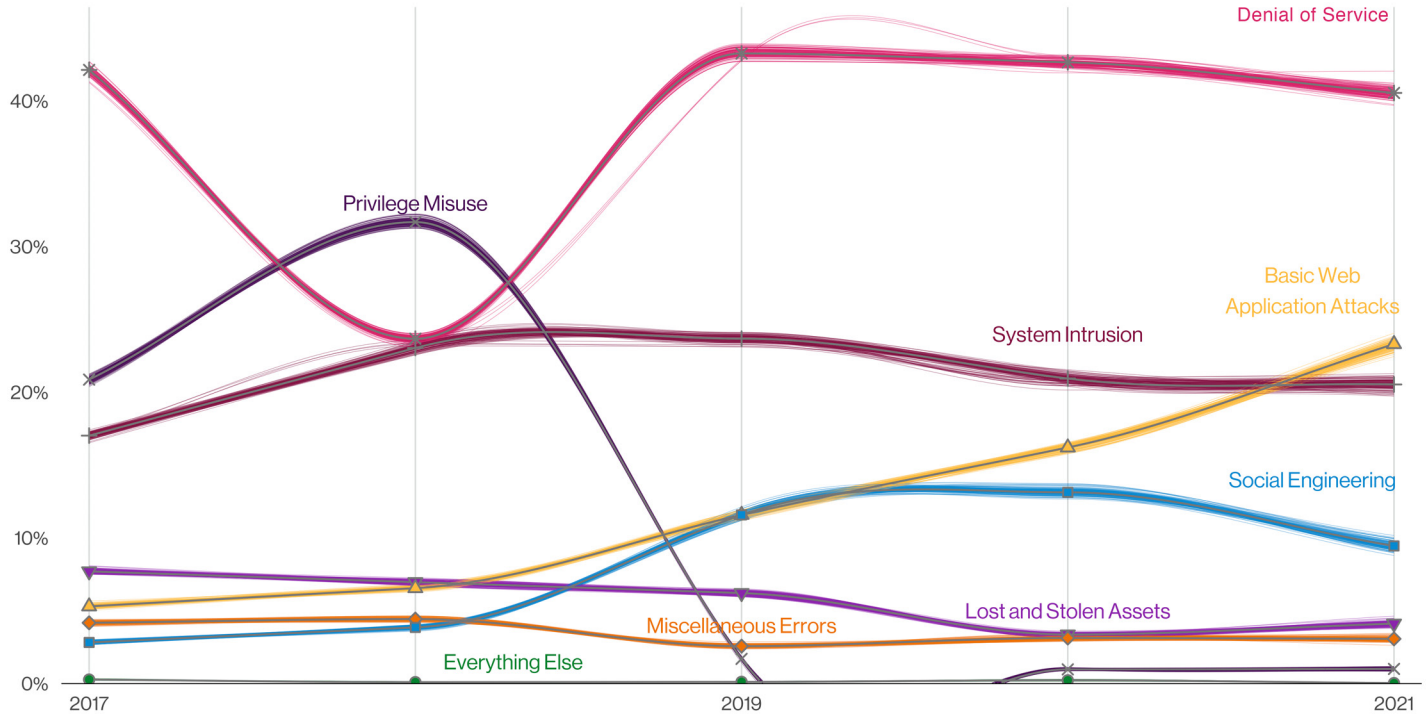


Figure 1. Patterns over time in incidents

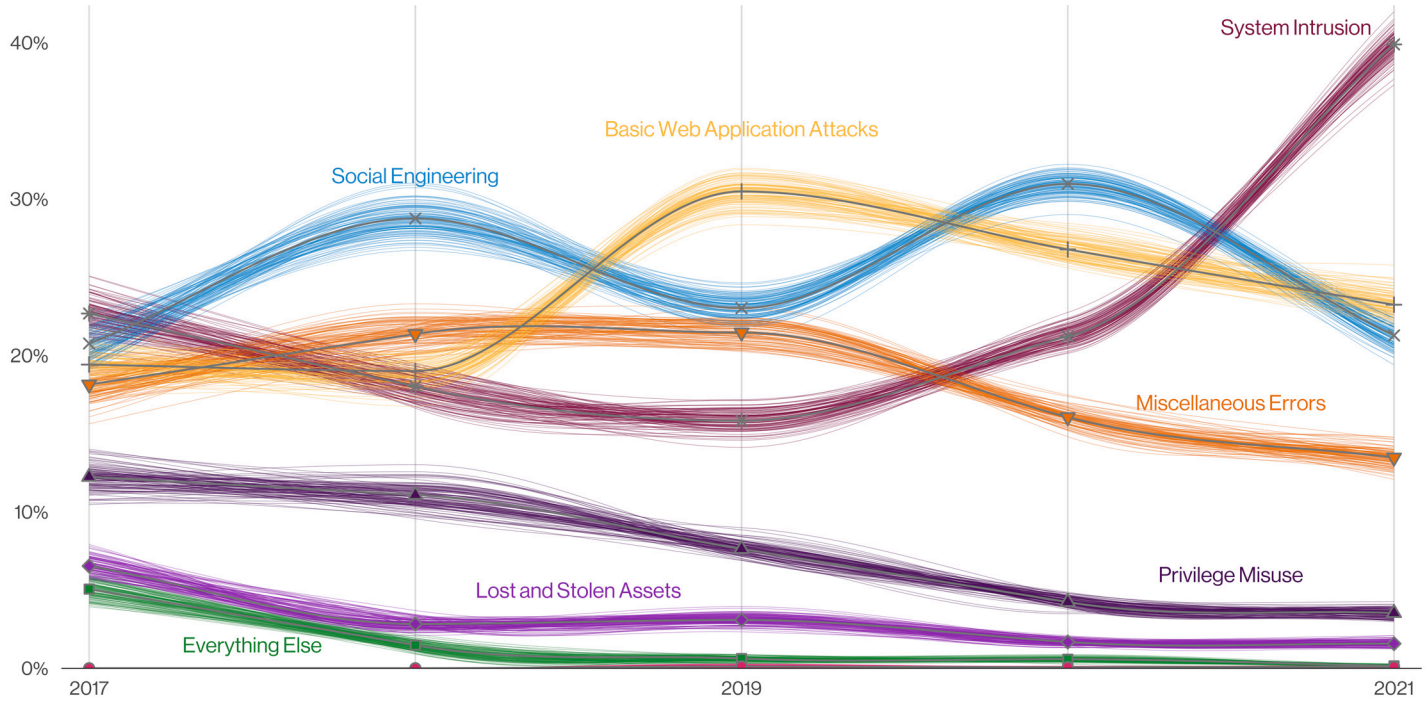


Figure 2. Patterns over time in breaches

Key takeaways

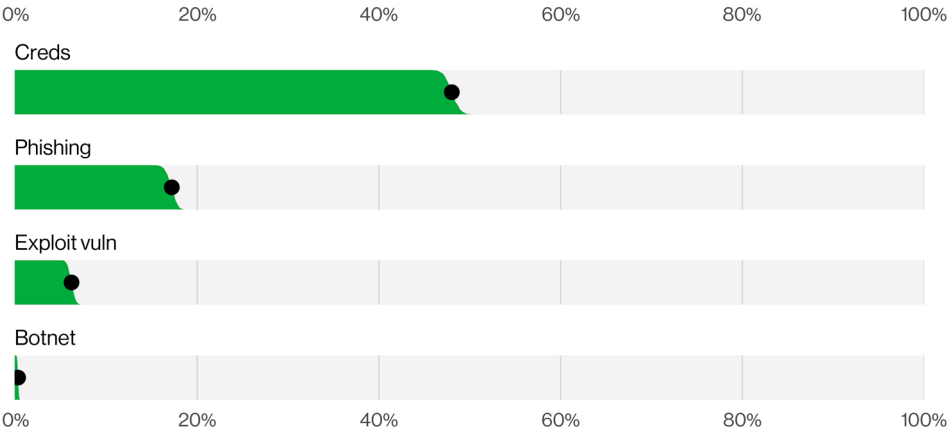


Figure 3. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and botnets. All four are pervasive in all areas of the DBIR, and no organization is safe without a plan to handle each of them.

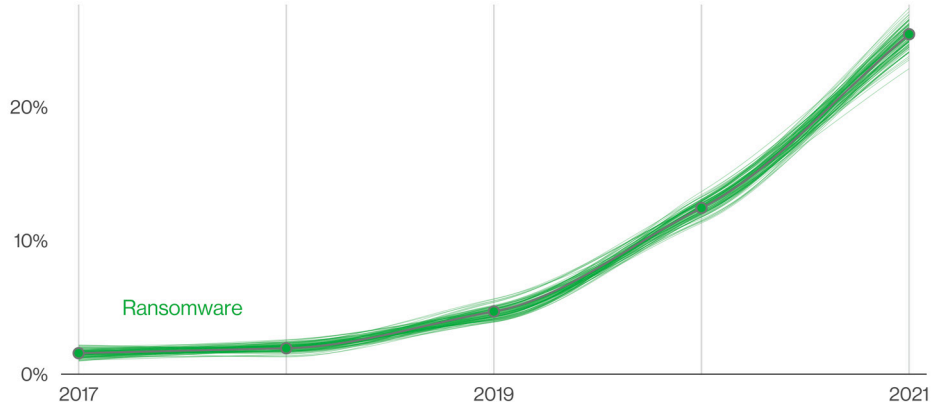


Figure 4. Ransomware over time in breaches

This year, ransomware has continued its upward trend with an almost 13% increase (for a total of 25% of breaches)—a rise as big as the past five years combined. It's important to remember that, while ubiquitous and devastating, ransomware by itself is, at its core, a model of monetizing an organization's access. Blocking the four key paths mentioned above helps to block the most common routes ransomware uses to invade your network.

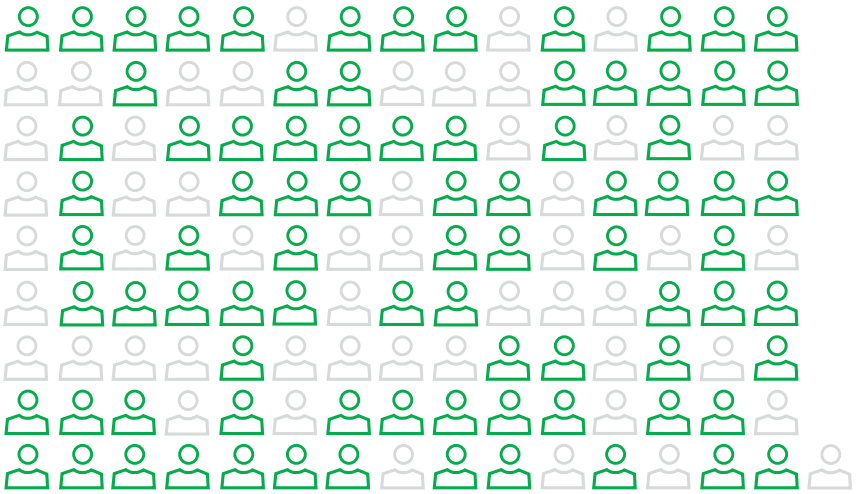


Figure 5. Partner vector in Systems Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

2021 illustrated how one key supply chain breach can lead to wide-ranging consequences. Supply chain was involved in 61% of incidents this year. Compromising the right partner is a force multiplier for threat actors. Unlike a financially motivated actor, nation-state threat actors may skip the breach altogether and opt to simply leverage the access.

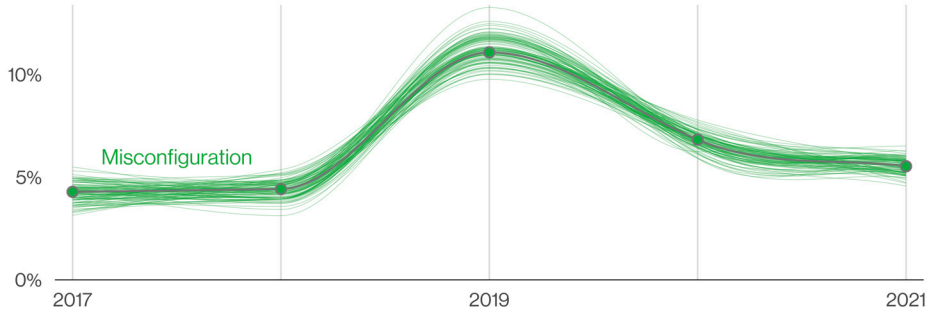


Figure 6. Misconfiguration over time in breaches

Error continues to be a dominant trend and is responsible for 14% of breaches. This finding is heavily influenced by misconfigured cloud storage. While this is the second year in a row that we have seen a slight leveling out for this pattern, the fallibility of employees should not be discounted.

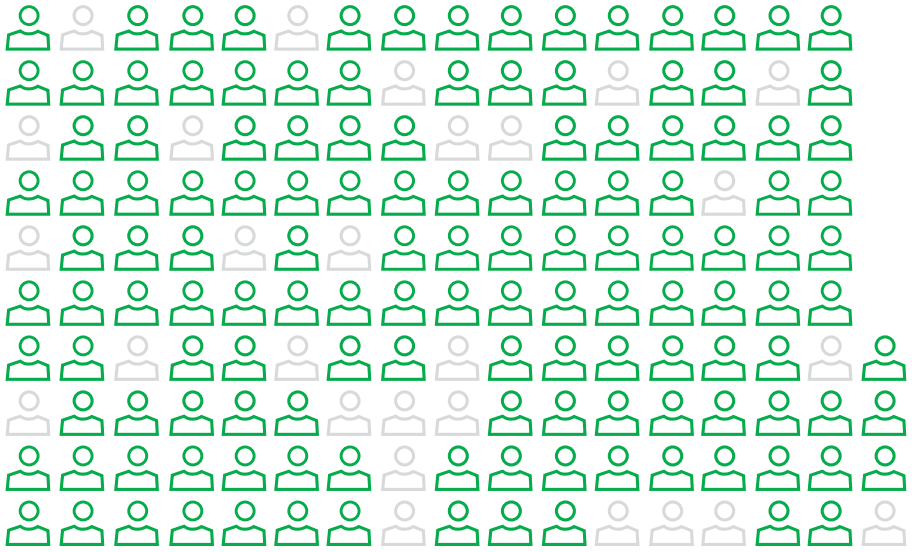


Figure 7. The human element in breaches (n=4,110).
Each glyph represents 25 breaches.

The human element continues to drive breaches. This year, 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse or simply an Error, people continue to play a very large role in incidents and breaches alike.

Industry highlights

Cybercrime is a serious risk regardless of your industry vertical or organization size, although the type and frequency of the attacks may differ to some degree depending on the size, function and location of your business. In order to deploy defenses efficiently and effectively, it is necessary to view not only the bigger picture with regard to the threat landscape, but also to be very aware of what is most likely to affect you in particular. This year, we again offer 11 industry snapshots, and for the first time, we have included a simple and easy-to-understand section geared toward very small businesses (10 or fewer employees). Finally, we also revisit the various regions of the globe for a closer look at the problems each area faces. As always, we classify organizations using the North American Industry Classification System (NAICS) codes.

Accommodation and Food Services (NAICS 72)

Accommodation and Food Services, while having seen a decrease of the System Intrusion pattern since 2016, is still victimized by Malware sent via email and the Use of stolen credentials used against Web applications.

Frequency	156 incidents, 69 with confirmed data disclosure
Top Patterns	System Intrusion, Denial of Service and Basic Web Application Attacks represent 84% of all incidents.
Threat Actors	External (90%), Internal (10%) (breaches) External (95%), Internal (5%) (all incidents)
Actor Motives	Financial (91%), Espionage (9%) (breaches) Financial (64%), Espionage (36%) (all incidents)
Data Compromised	Credentials (45%), Personal (45%), Payment (41%), Other (18%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	This industry continues to be targeted by financially motivated criminals going after payment and personal data.

Arts, Entertainment and Recreation (NAICS 71)

The System Intrusion and Basic Web Application Attacks patterns exchanged positions, but the Miscellaneous Errors pattern held on to third place on the podium. For incidents, Denial of Service attacks remain a substantial problem in the sector, particularly for the gambling industry.

Frequency	215 incidents, 96 with confirmed data disclosure
Top Patterns	Basic Web Application Attacks, System Intrusion and Miscellaneous Errors represent 80% of breaches.
Threat Actors	External (74%), Internal (26%) (breaches)
Actor Motives	Financial (97%), Grudge (3%) (breaches)
Data Compromised	Personal (66%), Credentials (49%), Other (23%), Medical (15%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	The Patterns are the same, but the order is not. Medical data continues to be compromised in this industry.

Education Services (NAICS 61)

Educational Services follows an eerily similar trend to the majority of the other industries: It is experiencing a dramatic increase in Ransomware attacks (more than 30% of breaches). In addition, this industry needs to protect itself against stolen credentials and Phishing attacks potentially exposing the personal information of its employees and students.

Frequency	1,241 incidents, 282 with confirmed data disclosure
Top Patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 80% of breaches.
Threat Actors	External (75%), Internal (25%) (breaches)
Actor Motives	Financial (95%), Espionage (5%) (breaches)
Data Compromised	Personal (63%), Credentials (41%), Other (23%), Internal (10%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	This industry continues to be impacted by attacks targeting its external infrastructure and is largely targeted by external actors with financial motives. However, this industry also faces errors as one of the top causes of breaches.

Financial and Insurance (NAICS 52)

The Financial sector continues to be victimized by financially motivated organized crime, often via the Actions of Social (Phishing), Hacking (Use of stolen credentials) and Malware (Ransomware). Finally, Miscellaneous Errors, often in the form of Misdelivery, is still a very common pattern, as it has been for the past three years in a row.

Frequency	2,527 incidents, 690 with confirmed data disclosure
Top Patterns	Basic Web Application Attacks, System Intrusion and Miscellaneous Errors represent 79% of breaches.
Threat Actors	External (73%), Internal (27%) (breaches)
Actor Motives	Financial (95%), Espionage (4%), Grudge (1%) (breaches)
Data Compromised	Personal (71%), Credentials (40%), Other (27%), Bank (22%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Data Protection (CSC 3)
What is the same?	Basic Web App Attacks and Errors continue to play a large part in breaches for this vertical as they did last year.

Healthcare (NAICS 62)

The Basic Web Application Attacks pattern has overtaken the Miscellaneous Errors pattern with regard to causing breaches in this sector. However, Errors are still a significant problem.

Frequency	849 incidents, 571 with confirmed data disclosure
Top Patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 76% of breaches.
Threat Actors	External (61%), Internal (39%) (breaches)
Actor Motives	Financial (95%), Espionage (4%), Convenience (1%), Grudge (1%) (breaches)
Data Compromised	Personal (58%), Medical (46%), Credentials (29%), Other (29%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	The top three patterns are the same, but the order is not. The threat actors were exactly the same as last year (down to the percentage point).

Information (NAICS 51)

System Intrusion moves ahead of Errors and Basic Web Application Attacks to claim the top spot this year in breaches. Meanwhile, DDoS maintains its top position in incidents. Malware has seen a noticeable rise over the past two years, while Errors appear to be on the down swing since their rise five years ago.

Frequency	2,561 incidents, 378 with confirmed data disclosure
Top Patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 81% of breaches.
Threat Actors	External (76%), Internal (24%) (breaches)
Actor Motives	Financial (78%), Espionage (20%), Ideology (1%), Grudge (1%) (breaches)
Data Compromised	Personal (66%), Other (35%), Credentials (27%), Internal (17%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	Basic Web App Attacks and Errors continue to play a large part in breaches for this vertical as they did last year.

Manufacturing (NAICS 31-33)

Manufacturing continues to be a lucrative target for Espionage, but it is also increasingly being targeted by other criminals via the use of Denial of Service attacks, credential attacks and Ransomware.

Frequency	2,337 incidents, 338 with confirmed data disclosure
Top Patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 88% of breaches.
Threat Actors	External (88%), Internal (12%), Partner (1%) (breaches)
Actor Motives	Financial (88%), Espionage (11%), Grudge (1%), Secondary (1%) (breaches)
Data Compromised	Personal (58%), Credentials (40%), Other (36%), Internal (14%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	System Intrusion and Basic Web Application Attacks continue to be among the main patterns this industry faces.

Mining, Quarrying, and Oil & Gas Extraction + Utilities (NAICS 21 + 22)

The Mining and Utilities Industries face similar types of attacks as the other industries we examined, such as attacks targeting credentials and leveraging data with Ransomware. However, they also have a high rate of Social Engineering attacks such as Phishing.

Frequency	403 incidents, 179 with confirmed data disclosure
Top Patterns	Social Engineering, System Intrusion and Basic Web Application Attacks represent 95% of breaches.
Threat Actors	External (96%), Internal (4%) (breaches)
Actor Motives	Financial (78%), Espionage (22%) (breaches)
Data Compromised	Credentials (73%), Personal (22%), Internal (9%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Account Management (CSC 5)
What is the same?	Continues to be targeted by financially motivated actors, but also suffers from espionage related attacks.

Professional, Scientific and Technical Services (NAICS 54)

Denial of Service attacks are a serious problem in this industry, and while they rarely result in a data breach, they can still have a significant impact. The System Intrusion attack pattern is in the first position again this year, while Social attacks are less prominent but still in the top three.

Frequency	3,566 incidents, 681 with confirmed data disclosure
Top Patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 89% of breaches.
Threat Actors	External (84%), Internal (17%), Multiple (1%) (breaches)
Actor Motives	Financial (90%), Espionage (10%) (breaches)
Data Compromised	Credentials (56%), Personal (48%), Other (26%), Internal (14%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	The top three attack patterns remain System Intrusion, Basic Web App Attacks and Social Engineering, but they have changed order compared to last year's report.

Public Administration (NAICS 92)

The System Intrusion pattern has risen to the top in this sector. Employees continue to be a cause of breaches in this vertical, although internal actors are seven times more likely to make a mistake than to commit a malicious act that causes a breach.

Frequency	2,792 incidents, 537 with confirmed data disclosure
Top Patterns	System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 81% of breaches.
Threat Actors	External (78%), Internal (22%) (breaches)
Actor Motives	Financial (80%), Espionage (18%), Ideology (1%), Grudge (1%) (breaches)
Data Compromised	Personal (46%), Credentials (34%), Other (28%), Internal (28%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Account Management (CSC 5)
What is the same?	Miscellaneous Errors remains in the top three patterns and holds the same position as last year.

Retail (NAICS 44-45)

The Retail industry is experiencing the same types of attacks it suffered last year: Use of stolen credentials, Phishing and Ransomware.

Frequency	629 incidents, 241 with confirmed data disclosure
Top Patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 84% of breaches.
Threat Actors	External (87%), Internal (13%) (breaches)
Actor Motives	Financial (98%), Espionage (2%) (breaches)
Data Compromised	Credentials (45%), Personal (27%), Other (25%), Payment (24%) (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	Organizations in this industry continue to be impacted by a variety of threat actors that leverage a range of tactics, such as deploying Malware to capture credit cards being processed by webforms and more common tactics like Phishing.

Very small businesses

When cybercrime makes the news, it is typically because a large organization has fallen victim to an attack. However, contrary to what many may think, very small organizations are just as enticing to criminals as large ones, and, in certain ways, maybe even more so.

Threat actors have the "we'll take anything we can get" philosophy when it comes to cybercrime. These incidents can and have put small companies out of business. Therefore, it is crucial that even very small businesses (10 or fewer employees) should take precautions to avoid becoming a target.

The number-one Action type in our dataset for very small businesses is Ransomware attacks. Ransomware is a type of malicious software that encrypts your data so that you cannot view or utilize it, and once the ransomware is triggered, the threat actor demands a (frequently large) payment to unencrypt it. The second most common is the Use of stolen credentials. Attackers can get your credentials (username and password) via many different methods: Brute force attacks (where attackers use automation to try numerous combinations of letters, symbols and numbers to guess your credentials), various types of Malware (thus the value of having an up-to-date antivirus), along with reused passwords from another site. Social attacks such as Phishing and/or Pretexting are also quite common. These attacks can be quite convincing (such as an invoice that looks like it comes from a known supplier but has a different payment account). While most come in via email, criminals have also employed the telephone to convince their target of the legitimacy of their request.

Check out the Very Small Business section in the full report for a detailed list of practical security recommendations and suggestions on who to contact if you believe your organization has been a victim of cybercrime.

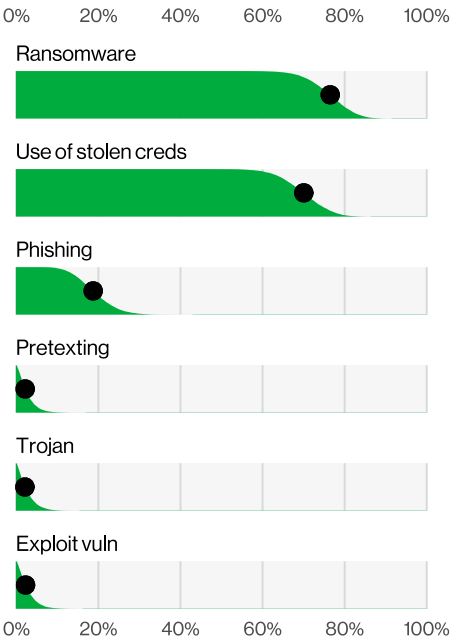
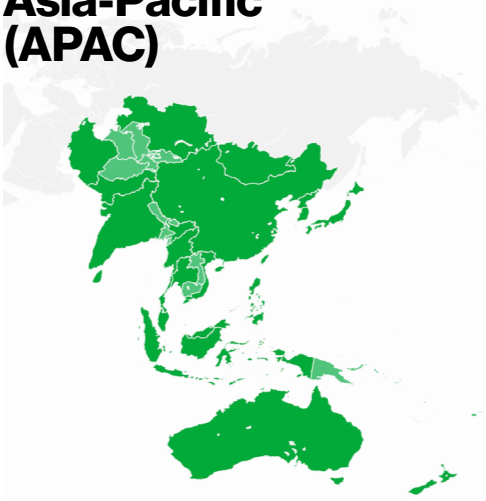


Figure 8. Action varieties in 1 to 10 employee organization breaches (n=61)

Regional findings

This edition of the DBIR marks the third year that we have analyzed incidents and presented them from a macro-region perspective. It is our hope that our readers find this more global view of cybercrime helpful and informative. As we have mentioned in the past, we have greater or lesser visibility into a given region based on numerous factors, such as contributor presence, regional disclosure regulations, our own caseload and so on.

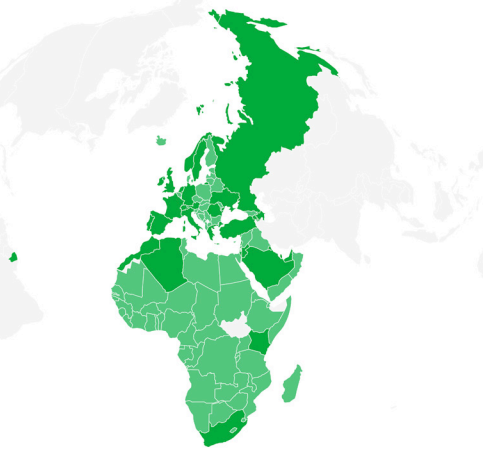
Asia-Pacific (APAC)



APAC experiences a high number of Social and Hacking related attacks but has a much lower number of Ransomware cases than other areas.

Frequency	4,114 incidents, 283 with confirmed data disclosure
Top Patterns	Social Engineering, Basic Web Application Attacks and System Intrusion represent 98% of breaches.
Threat Actors	External (98%), Internal (2%) (breaches)
Actor Motives	Financial (54%), Espionage (46%), Secondary (1%) (breaches)
Data Compromised	Credentials (72%), Internal (26%), Secrets (18%), Other (11%) (breaches)
What is the same?	Basic Web Application Attacks and Social Engineering attacks continue to be persistent threats for this region.

Europe, Middle East and Africa (EMEA)



The rise of the Social Engineering pattern in this region illustrates the need for controls to detect this type of attack quickly. Credential theft remains a large problem as well, as illustrated in the continued persistence of the Basic Web Application Attacks pattern in EMEA.

Frequency	1,093 incidents, 307 with confirmed data disclosure
Top Patterns	Social Engineering, System Intrusion and Basic Web Application Attacks represent 97% of breaches.
Threat Actors	External (97%), Internal (3%), (breaches)
Actor Motives	Financial (79%), Espionage (21%) (breaches)
Data Compromised	Credentials (67%), Internal (67%), Secrets (20%), Other (18%) (breaches)
What is the same?	The patterns are the same top three, but they have rearranged themselves in order. External actors continue to perpetrate the vast majority of breaches in this region.

Northern America (NA)

The System Intrusion pattern has become the dominant pattern in this region. Social Engineering gave way as System Intrusion increased, but there remains a large problem with Social actions such as Phishing in Northern America. Basic Web Application Attacks continue to beset organizations here as well.

Frequency	4,504 incidents, 1,638 with confirmed data disclosure
Top Patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 90% of breaches.
Threat Actors	External (90%), Internal (10%), Multiple (1%) (breaches)
Actor Motives	Financial (96%), Espionage (3%), Grudge (1%) (breaches)
Data Compromised	Credentials (66%), Internal (21%), Personal (20%), Other (20%) (breaches)
What is the same?	The top three patterns remain the same, only their order has changed. External actors continue to hold sway in breaches in this region.

Go with the flow.

The DBIR team continues to expand the Vocabulary for Event Recording and Incident Sharing (VERIS) framework to classify and analyze incidents and breaches. We have collaboratively developed mappings with MITRE ATT&CK and the Center for Internet Security Critical Security Controls (CIS CSC) to assist organizations with developing and maintaining a data-driven cybersecurity program. In addition, we assist with the creation of Attack Flow in collaboration with other members of the information security community to help capture the sequence of events associated with an attack. We used the mappings and additional frameworks to boost our analysis and have made them available for use by the larger security community too.

Best practices

Once again, we've aligned our findings with the Center for Internet Security's Critical Security Controls to provide you with a way to translate DBIR data into your security efforts. Here are the top controls that our data suggests will be worthwhile for most organizations.

Control 3 – Data Protection

This Control pertains to the processes and technical controls to identify, classify and securely handle organizational data in all its form. This Control helps prevent organizations from accidently exposing their data through email or misconfigurations.

Control 4 – Secure Configuration of Enterprise Assets and Software

This Control is not only a mouthful, but it also contains safeguards focused on engineering solutions that are secure from the outset, as opposed to tacking them on later. This Control offers substantial benefits when it comes to reducing Error-based breaches such as Misconfiguration and Loss of assets by enforcing remote wiping abilities on portable devices.

Control 5 – Account Management

This Control is very much targeted toward helping organizations manage the access to accounts and is useful against Brute force and Credential stuffing attacks.

Control 6 – Access Control Management

This Control manages the rights and privileges of users and enforces multifactor authentication on key components of the environment, an important defense against the Use of stolen credentials.

Control 14 – Security Awareness and Skills Training

This Control is a classic and one that hopefully does not require a great deal of explanation. Considering the prevalence of Errors and Social engineering we see in our data, it is clear that security awareness and technical training are a great place to put some dollars in order to help support your team against a world full of cognitive hazards.

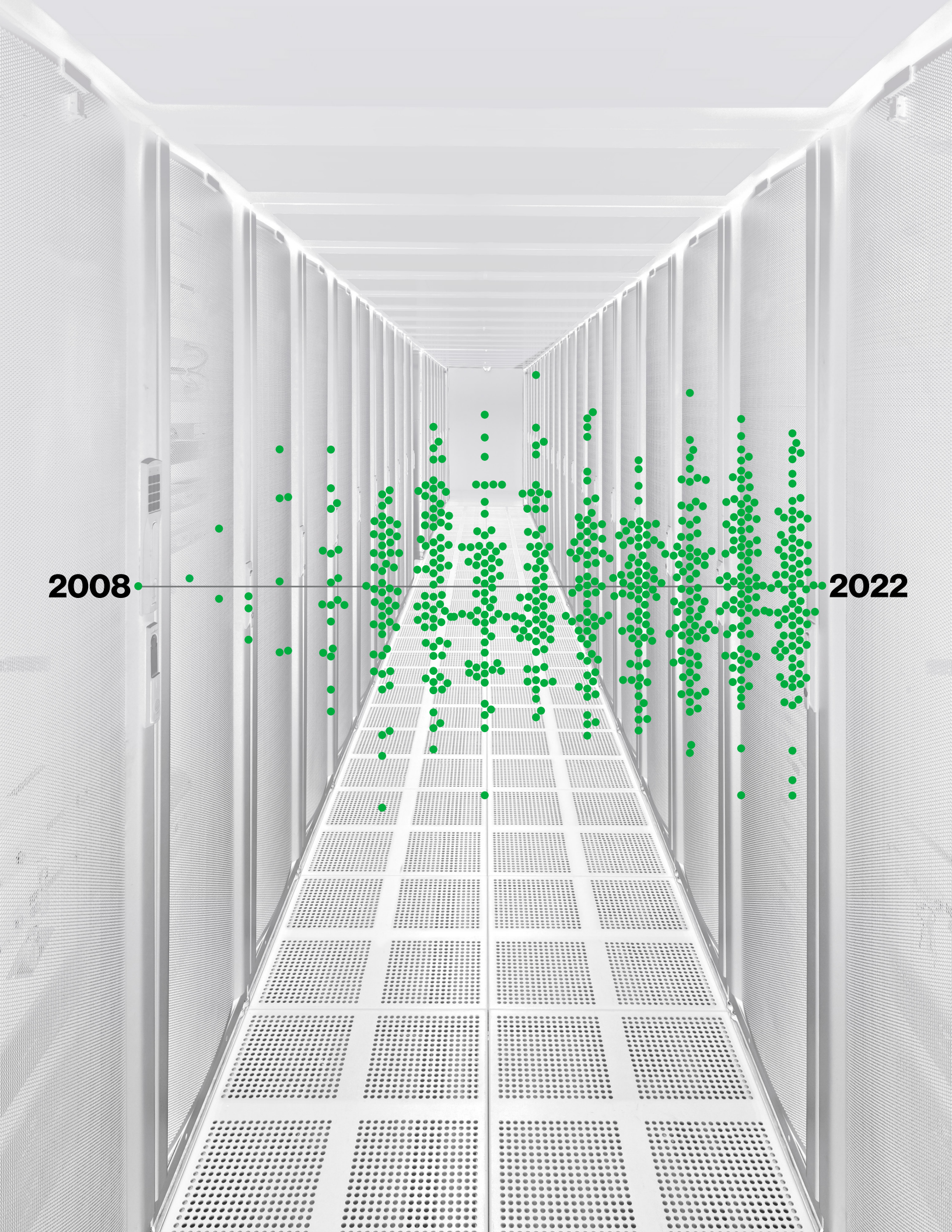
Stay informed and threat ready.

Facing today's threats requires intelligence from a source you can trust. The full DBIR contains details on the actors, actions and patterns that can help you prepare your defenses and educate your organization. Get the intelligence you need to protect your organization:

Read the full 2021 DBIR at enterprise.verizon.com/resources/reports/dbir

Want to make the world a better place?

The DBIR relies on contributions from dozens of organizations, and we'd love to have you. Become a contributor to next year's report, or provide us feedback for improving the DBIR at dbir@verizon.com, tweet us @VZDBIR and check out the VERIS GitHub page: https://github.com/vz-risk/veris.


2008
2022