Insurance

Reducing Cyber Insurance Risk with Zero Trust Data Surveillance

When Data is the Prize

In 2021, the combination of unprecedented ransomware attacks and restricted cyber insurance capacity created a crisis in the cyber insurance industry. As losses grew, carriers raised premiums, reduced coverages, and began asking clients to fund more of their own risk through self-insured retention increases. According to a World Economic Forum report, "cyber insurance pricing in the United States rose by 96% in the third quarter of 2021, marking the most significant increase since 2015 and a 204% year-over-year increase."[1] It appears that the volatility will continue.

For carriers and their policyholders, only one thing is certain. Cyber attacks aren't going away. Cybercrime bad actors and nation-state threats want only one thing—data. When data is the prize, protecting it means securing more than just the infrastructure that stores and carries it. In this brief, we'll look at the factors influencing cyber insurance practices and how a new approach to securing data can reduce risk for both carriers and their clients.

__Flying Cloud__ is the first company to secure the data itself. Flying Cloud CrowsNest is the only patented solution that integrates data surveillance techniques with a Zero Trust architecture to secure data of consequence.

Data is at Risk Everywhere

Large, medium, or small—no business escapes cyber attack. Enterprises have large amounts of juicy data, but they have significant staff and technology resources for fighting cyber crime. Small businesses also have valuable data assets but fewer resources and trained staff, which makes them easy targets. Attackers don't care. Regardless of business size, data is data and cyber criminals will take everything they can get.

In 2021, cyber criminals binged. According to Check Point Research, cyberattacks increased 50% in overall attacks per week on corporations, compared to 2020, with each organization facing an average of 925 attacks per week. With all of those attacks, breaches are inevitable. In spite of new law enforcement approaches to intercepting ransom payments and criminal funds, there was an 82% increase in ransomware-related data leaks in 2021 compared to 2020.[3] Victim data is a hot commodity.

[1] The Global Risks Report 2022, World Economic Forum
[2] Check Point Research: Cyber Attacks Increased 50% Year Over Year
[3] CrowdStrike 2022 Global Threat Report

Eighty percent of data compromises are caused by external actors.[4] These are typically global adversaries focused on targeted intrusion, e-crime, and hacktivist activities. Highly sophisticated, these attackers unleashed the Sunburst attack, big game hunting (BGH) ransomware attacks, and Log4Shell attacks in 2021—in addition to exploiting architecture and software vulnerabilities.

The top industries that were breached (confirmed disclosure of data to an unauthorized party) were Financial, Professional Services, Healthcare, Public Administration, Information, and Manufacturing. The top-ranking industries that encountered incidents (events that compromise the integrity, confidentiality or availability of an information asset) were Professional Services, Public Administration, Information, Finance, Manufacturing, and Education. All of these industries offer data-rich targets for attackers.

The Favorite Tactic: Ransomware

According to the Verizon DBIR, ransomware was by far the leading attack tactic. Ransomware increased 13% in 2021—an increase as large as the previous five years combined.[5] Ransomware attacks routinely make news and in 2021, they also sparked the meteoric rise in cyber insurance premiums.

However, ransomware is usually the last stage of a malware breach. Attackers typically gain access to a network and take up residence through phishing, credential theft, or other methods. Once in, they drop detection-evading malware in advance of the ransom demand. Most actors exfiltrate data for a period of time, extracting as much value as possible. Not only can they generate revenue from the data stolen, they also can expose highly sensitive data and leverage that power in their ransom demands. Once the data being exfiltrated is no longer of value, they just "burn the place down"—demand a ransom and collect. Other ransomware attackers don't bother looking for data of specific value. They only aim to interrupt organizations' critical functions by encrypting their data to expedite ransom payment.

In 2021, a record 71% of organizations experienced successful ransomware attacks, and of these, 63% paid the requested ransom.[6] But the collateral cost to an organization is seven times more than the ransom they pay, according to Check Point Research. Further, there is no guarantee that the organization will recover all—or any—of its encrypted data. While 99% of companies recovered some of their data, on average they could only recover 61% of encrypted data. Only 4% of companies paying a ransom received all their data back.[7] Ransom payments have terrible ROI.

Other Tactics on the Rise

While ransomware made the biggest news, it wasn't the only tactic used. The second half of 2021 also saw supply chain attacks jump by 51%.[8] Cybercriminals often use intrusion attacks into smaller, more vulnerable companies in a supply chain to gain access to larger, better-defended companies. They might use ransomware or command-and-control (C2) tactics to steal data. Many of these attacks targeted open source software tools, security software, and software updates.

Stolen credentials are used extensively to access networks, especially in cloud environments. Stolen credentials accounted for nearly 50% of attacks and were present in third-party breaches, phishing attacks, basic web application attacks (BWAA), and system intrusions.[9]

[4] 2022 Data Breach Investigations Report, Verizon
[5] 2022 Data Breach Investigations Report, Verizon
[6] Cyberthreat Defense Report, CyberEdge Group, April 4, 2022
[7] State of Ransomware 2022, Sophos
[8] Insight Space: Supply Chain Risk, NCC Group, April 2022s
[9] 2022 Data Breach Investigations Report, Verizon

Attackers continuously evolve their tactics, techniques and procedures (TTPs). In 2021, some adversaries avoided publicly available exfiltration tools and developed their own. Data theft and extortion rates without the use of ransomware rose. It's always about the data—organizations need to be able to see their data, where it goes, and how it's used—as well as identify traffic that isn't theirs in order to stop exfiltration before a major ransomware attack.

Costs Keep Rising

Every breached company faces high associated costs, many of which are felt for years after an incident. In 2021, the average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years. The global average total cost of a data breach increased to $4.24M.[10]

Customer personally identifiable information (PII) was the most common type of record lost, included in 44% of breaches. It was also the most expensive record type, at $180 per lost or stolen record.[11] It's no wonder that cyber risk now ranks among companies' top five concerns.

The Insurer's Perspective

The Impact on Cyber Insurers

For cyber insurers, none of these facts are good news. Although demand for cyber insurance has been increasing, cyber attacks and their aftermath have too. For the cyber insurance industry, loss ratios began to deteriorate in 2018 and 2019. In 2020, they jumped to a record high of 73%, indicating an industry-wide underwriting loss. In 2021, the ratio improved to 65%, but was still high compared to the 42% average loss ratio for 2015-2019.[12]

Insurers stepped back and reevaluated their risk tolerance. As a result, insurance premiums rose sharply in 2020 and then skyrocketed in 2021. Premiums for standalone coverage increased by 92% to over $3.1 billion for 2021.[13] At the same time, capacity decreased. For example, medium-sized companies that had $10 million in coverage are now likely to find only $5 million or less available. A firm that is considered to be high risk might not be able to get coverage at all. Some firms are dropping coverage for certain kinds of cyber incidents. AXA, a French firm, stopped covering ransomware payments in France, starting in May 2022. Insurers began applying co-insurance provisions, similar to a deductible, requiring policyholders to carry more risk

Underwriting Needs Closer Scrutiny...But

Clearly, underwriters need better data for making risk decisions. However, unlike counterparts in property and casualty or health insurance, cyber insurance underwriters don't have decades of "cyber actuarial" data underlying their decisioning processes. Making these decisions is just plain difficult for many reasons.

Normal business factors do not reflect security posture: The type and size of a business, value of its data, annual revenues, and a history of previous cyber breaches or incidents are important factors to consider. However, it's critical to understand the maturity level of clients' security postures and track record over time.

[10] Cost of a Data Breach Report 2021, IBM
[11] Cost of a Data Breach Report 2021, IBM
[12] US Cyber Insurance Sees Rapid Premium Growth, Declining Loss Ratios, Fitch Ratings, April 2022
[13] US Cyber Insurance Payouts Increase Amid Rising Claims, Premium Hikes, Fitch Ratings, May 6, 2022

Adversaries' toolboxes are formidable: Even when clients are questioned about their ransomware prevention and mitigation measures, ransomware is only one type of threat or tactic to worry about. To put this in perspective, the MITRE ATT&CK Framework identifies 14 enterprise tactics (the adversary's goal) and 191 techniques (how the adversary goes about achieving their goal) used in attacks on enterprises. There are 43 categories of mitigation techniques—each including dozens of possibilities for stopping or reducing the impact of a given technique. How does the client's security posture address all of these known threats—let alone unknown and zero-day threats?

Threats morph continually: The "threat du jour" changes constantly. Malware is notorious for innovation. Every day, AV-TEST registers more than 450,000 new malwares and potentially unwanted applications. AV-TEST registered 153 million new malware samples from March 2021 to February 2022 alone—a 5% increase on the previous year. To make matters worse, much malware is polymorphic, meaning it has the ability to constantly change its code to evade detection.

Attackers also go back and re-purpose previously successful techniques to spark fresh attacks. Denial-of-service (DDoS) attacks brought CNN, Dell, E-Trade, eBay, and Yahoo! to their knees in 2000. A DDoS attack on Dyn in 2016 disrupted Airbnb, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit, and GitHub. Even with 16 years of cyber intelligence in between, the second wave was as crippling as the first.

Assessments are limited: Even if an insurer sends teams to conduct pen testing and other assessments, results vary tremendously. Testing strategies vary. Each testing team is different. Results depend on individual skills of testers. Testing is usually conducted in a controlled environment, doesn't cover all elements of each system, and rarely uses the latest TTPs that real attackers use. How can an insurer determine how much testing and which kinds, are enough? What are the odds that an attack would succeed?

Complexity reigns: Enterprises rely on dozens of security products. It's difficult to know if—or how well—current configurations, policies, and control settings are delivering the desired protection. Additionally, new development and infrastructure is constantly introduced, making it impossible to measure security posture consistently over time. Even with best practices in place, constant change opens the door to new risks.

There are no universal standards: Because of the above factors, there are no standards for accurately and universally assessing risk associated with the vast number of security controls in place. It's almost impossible to accurately estimate potential losses based on a given threat scenario or to apply consistent judgment across a risk pool.

Point-in-time evaluations are not enough: In environments with constantly moving targets, an annual review only provides a snapshot of the truth limited to specific aspects of the overall infrastructure, policies, and practices.

So now what?

Insurers realize that they need more. Many have adopted detailed questions and discovery processes to better understand their policyholders' existing security measures. There are varying lists of items on their question lists, but these are examples of what underwriters consider:

- Multi-factor authentication across the applicant's systems, including email, remote access, vendor access, etc.
- A tested incident response plan
- Presence of an endpoint detection solution
- Security awareness training, including phishing training
- Removing end-of-life software
- Closed remote access ports, including remote desktop protocol (RDP)
- Specific controls for ransomware
- Dependent business interruption recovery procedures
- Existing IoT/OT networks and security controls

There is also an emerging category of security ratings providers who score security postures to help organizations—and their potential cyber insurers—better understand the cyber risks they face. Some focus exclusively on third-party risk, others on security best practices, and still others on metrics related to compliance. Each uses different techniques and processes to arrive at their scores. This is clearly a move in the right direction, but it's not enough.

The prize in cyber attacks is the data itself. Even with the best security practices and compliance measures in place, organizations are still being attacked and breached. The focus on networks, devices, and users can only take you so far. When data is the prize, the data itself must be defended. Insurers need to see that an organization clearly knows the data it has, what normal usage looks like, and how it's being defended in an attack. They need real-time perspective and context for their data over time.

Solution

Eyes on the Prize

Organizations can no longer live with these unknowns, and many are beginning to implement Zero Trust strategies. Zero Trust is a framework that redefines the concept of trust. Instead of assuming that users, devices, and data are trustworthy, a Zero Trust model is based on a perspective of "never trust, always verify." Users, devices, and connections, whether inside or outside of the network, are continuously authenticated, authorized, and validated for security posture. Companies with mature Zero Trust policies saved $1.76 million per breach compared to companies without Zero Trust.[14]

Although there are Zero Trust segmentation and security policy solutions available for networks, devices, users, and applications, there have been no solutions for applying Zero Trust policies to data itself. Until now.

[14] Cost of a Data Breach Report 2021, IBM

Flying Cloud CrowsNest Data Surveillance for Zero Trust Data Security

Flying Cloud CrowsNest is the only patented solution that integrates data surveillance with a Zero Trust architecture. CrowsNest protects any data of consequence, not just regulated data. Whether customer PII, financial, IP, legal, IoT, or compliance information—CrowsNest fingerprints data, monitors and analyzes usage, and defends data against threats in real time.

Know the Data

CrowsNest begins by fingerprinting the organization's business-critical data from the repositories where it resides. Working at the binary level, CrowsNest identifies where the data originates, as well as its purpose, level of sensitivity, movement and relationship to other data and users. CrowsNest then catalogs data content and structures without modifying files in any way.

Monitor the Data

When data is accessed, CrowsNest conducts data surveillance—following and monitoring the data everywhere it goes. For example, User A is authorized to access sensitive data about a company's proprietary formulas. User A needs the data for legitimate business purposes. But once accessed, data quickly proliferates across the organization. Suddenly, User B has some of the formula data, but why did User A share it? How did it then get into the hands of Vendor C? Suddenly, sensitive data is in the hands of people who never had authorization to access it in the first place.

CrowsNest recognizes fingerprinted data at the bit level and monitors it. It can scan for unauthorized data movement between enterprise applications and tools, as well as scan for unauthorized data movement between on-premises and cloud systems. Patented machine learning and automation quickly establish a baseline of normal data patterns. By continually analyzing incoming data, data in motion, and data leaving the environment, CrowsNest continuously updates the rolling baseline.

CrowsNest also understands how data feeds into every area of the business model, such as loyalty programs, analytics, customer communications, financial and payment systems. It knows when new data is added to original data, when original data is modified, and when it's deleted. It knows who uses the data, where the data is located, when it's used, and how it's used.

Defend the Data

Once data is known and a rolling baseline is established, CrowsNest identifies anomalies, breaches, and exfiltration in real time and alerts the security team. Patented machine learning techniques isolate threats including ransomware, botnets, malware, Bitcoin, back doors, and C2 software. CrowsNest also can see applications and monitor their behavior to identify and alert to attacks launched through internal users.

Contextual analysis connects the dots across attackers' tactics. Full-session capture of events enables CrowsNest to reconstruct events, extract payloads, and provide play-by-play analysis of the activity. Teams will immediately know exactly what happened, where, and by whom—gaining a data "chain of custody" to support their response and remediation capabilities.

Benefits

Data Accountability for Organizations and Insurers

Establish Data Accountability

Surveillance of incoming data, data in motion, and data exiting the network delivers granular visibility into all data. Data chain-of-custody reports enable security teams to easily trace data movement and usage. They can now prove that critical data remains within the organization or verify that there are no overlaps or exfiltration.

Data accountability also enables a company to identify data on the network that isn't theirs. The appearance of non-fingerprinted data or anomalous movements are early indicators of attackers in the environment. For example, if C2 data movement is detected, it can be stopped weeks or months before a ransom demand or breach.

Apply Data-Level Policy

For the first time, organizations can create, apply, and enforce policy on data at the bit level. Data itself is monitored and protected wherever it goes. Unlike DLP solutions, CrowsNest protects any data—not just regulated data in specific formats. And unlike DLP, CrowsNest protects at the binary level. Regex can be imported to CrowsNest, giving data-level visibility to data currently monitored by DLP systems.

Easily Ensure Compliance Everywhere

CrowsNest is ideal for global organizations that must comply with the data standards of every country in which they have a presence. Data-level policies are easily tailored to any compliance regulations. Chain of custody reports provide immediate, granular visibility to verify data residency and retention.

Any Business Model, Any Infrastructure

CrowsNest fits with any business model to secure the data that matters most in the way that works best for the business. It integrates easily into existing security infrastructure—NACs, firewalls, SIEMs, DLP solutions, IoT solutions, and cloud security—without impact on users or systems. It can be implemented per dataset, per site, or enterprise-wide.

In organizations with multiple product brands or organizational units, CrowsNest can automatically surveil and defend data at any level and at any scale. One Flying Cloud customer has fingerprinted hundreds of petabytes of data, relying on CrowsNest to automatically scale and follow the data as it proliferates across the business.

Simplify Operations

Once a company knows what it's protecting and where it's going, it can make better decisions about how to protect it. For example, better control over data enables organizations to reduce or eliminate high costs associated with data encryption or false positives associated with DLP. At the same time, CrowsNest enables far better protection against insider unauthorized access.

The ability to see and send real-time, detailed anomaly data streamlines incident response and reporting. CrowsNest customers have greatly simplified compliance analysis and reporting, freeing team members for other projects.

Team with Policyholders

Flying Cloud can help insurers structure their underwriting analysis based on quantifiable information about their policyholders' data. Gain a standard way to measure data security over time periods and threat windows. At the same time, insurers can add value to their cyber insurance products by enabling clients to understand their own data environments and threats more clearly to better protect their data assets. When CrowsNest enters the picture, everyone wins but the attackers.

See Data. For the First Time.

For the first time, organizations can actually protect the object of attack—the data itself—and not just the systems and devices surrounding it. See an organization's actual data as it is accessed, moved, and used. Flying Cloud customers choose CrowsNest data surveillance to protect IP, track data, ensure data safety and integrity across large ecosystems, prevent data harvesting, and accelerate threat response. Insurers choose CrowsNest to gain quantifiable data for risk decisions and the ability to add value to their policyholders' security postures.

What next?
Go to www.flyingcloudtechnology.com/demo