Zero-Day Dilemma: Understanding to Protect

Discover the dangers of zero-day vulnerabilities and learn how to best protect your organization.

SECNAP
NETWORK SECURITY

Why are Ransomware Attacks happening more often?

A few years ago cybercriminals enjoyed a breakthrough in technology that allowed them to bypass the most common defenses that had proven to be successful against ransomware up until about 2019.

That's the high level answer; however, in order to completely understand this, it's a bit more complex. What's more, if you are involved in cyber security at any level (from an entry-level practitioner to the chief information security officer of your company or business), it's important that you understand the detailed answer -- your business' or governmental entity's financial future may depend on it.

The detailed, complex answer begins with an understanding of what the most commonly deployed cybersecurity defense against ransomware has been -- a sophisticated endpoint protection solution plus frequent and complete backups of all important data. Everyone who practices cybersecurity knew that this was the "best defense." Unfortunately, the cybercriminal community also had access to the same information; and in 2017 they were handed a technological breakthrough to empower them to skirt past these normally-deployed defenses.

Zero-Day Vulnerabilities

The Dark Net has long hosted a very active cybercrime market in which cybercriminals sell zero-day vulnerabilities to anyone who is willing to pay for them (zero-days are often referred to as "0-days").

Sometime between 2008 and 2010, a US federal agency began buying these vulnerabilities, with very good intentions. The idea was to turn many of these vulnerabilities over to the impacted vendors so that the vendors could issue patches, while retaining some of the 0-days to potentially use them in the war on terror and the war on cybercrime.

However, these actions backfired in spectacular fashion. First, bidding up the prices for zero days helped to inflate the prices in the 0-day market, which signaled to hackers that they could handsomely profit from discovering these vulnerabilities, which led to many more vulnerabilities being discovered and held for sale on the black market. This also signaled to cybercriminals that they could also participate in that market and actively seek out and bid on zero days for themselves -- which they did.

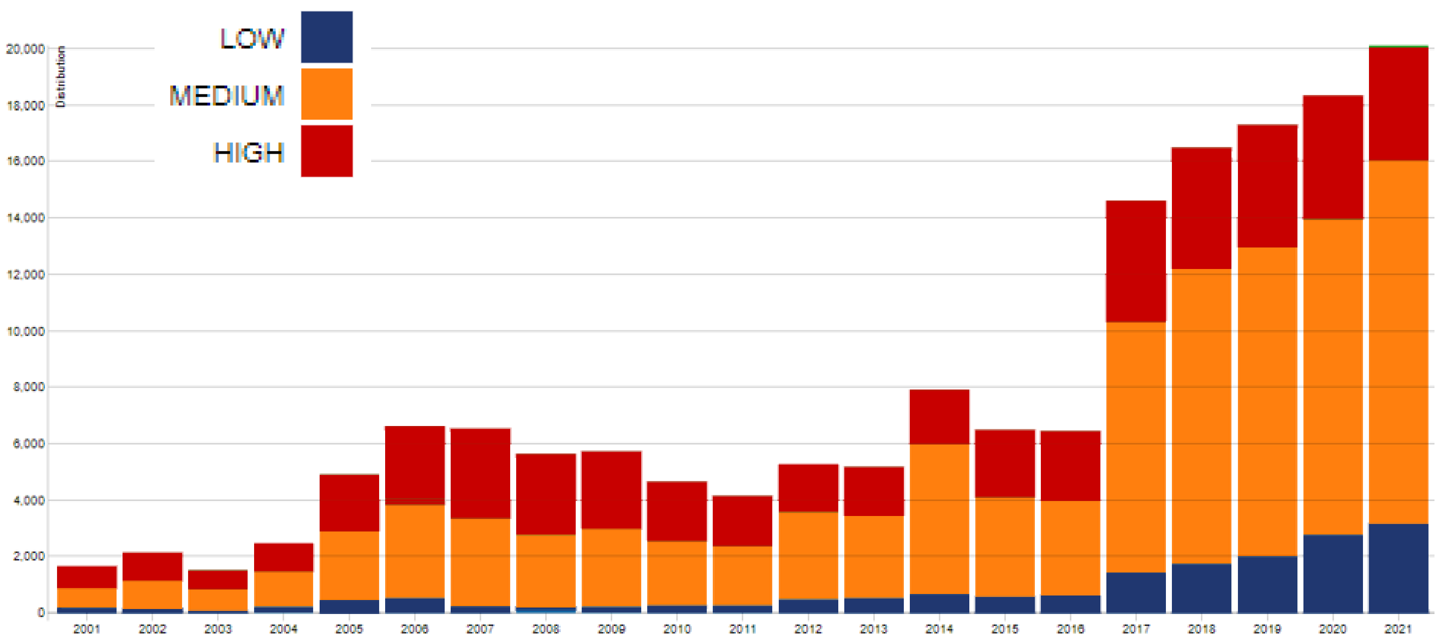
The Dark Net has long hosted a very active cybercrime market in which cybercriminals sell zero-day vulnerabilities to anyone who is willing to pay for them.

Then the worst happened. In 2017, the “Shadow Brokers” cybercrime cartel announced that they had successfully breached a treasure trove of zero-day vulnerabilities that was being held by government agencies, then proved it by publishing a select few of them on the internet. They offered to sell the entire stash to the highest bidder.[1]

However, no one was willing to bid, likely because no one wanted to risk being on the US’s list of bad actors. Theoretically, Dark Web purchases are anonymous, but no one wanted to take the chance that the government

As a result, Shadow Brokers decided to simply publish the entire set of zero-day vulnerabilities, making them freely available to anyone who wished to use them[2] and kicking off a bold new era in zero-day attacks.

Reported Security Vulnerabilities by Year



Zero-day exploits are behind some of the largest ransomware attacks in recent months. Recent exploits include the Kaseya supply chain attack,[3] the SolarWinds/Orion breach,[4] the related Sunburst attack,[5] and the HAFNIUM/Microsoft Exchange server exploit,[6] which together compromised thousands of businesses worldwide and empowered ransomware. The problem has become so severe that the White House and Congress have gotten involved.[7] Understanding zero-days is crucial to defending against ransomware and other cyberattacks.

[1] https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

[2] https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/

[3] https://thehackernews.com/2021/07/revil-used-0-day-in-kaseya-ransomware.html

[4] https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/

[5] https://www.govtech.com/security/the-sunburst-hack-was-massive-and-devastating--5-observations-from-a-cybersecurity-expert.html

[6] https://www.theverge.com/2021/3/5/22316189/microsoft-exchange-server-security-exploit-china-attack-30000-organizations

[7] https://www.nytimes.com/2021/07/07/us/politics/biden-ransomware-russia.html; https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/; https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Zero-Day "Lifecycle"

- A zero-day **vulnerability** is a software or hardware security hole for which no patch yet exists.
- A zero-day **exploit** is a method by which a cybercriminal takes advantage of the vulnerability to launch an attack.
- A zero-day **attack** leverages a zero-day exploit to exfiltrate data, plant ransomware or malware, and/or cause other damage to systems.

What makes zero-days so dangerous?

It's important to note that a zero-day vulnerability, in and of itself, presents only the potential for an attack. Unless cybercriminals can exploit the vulnerability, they cannot launch an attack. If the vulnerability is a vault, the exploit is the combination to open it, and the attack is what happens once cybercriminals get inside.

Additionally, gaining a foothold through a zero-day exploit does not, on its own, equal a serious breach. Once inside, cybercriminals must move laterally through the network. However, since zero-day exploits that enable initial compromise are so widely available, cybercriminals have developed tools and tactics to aid in lateral movement.

Tactics and techniques for lateral movement through networks have been successfully deployed in part because many organizations have been focused on endpoint protection plus frequent thorough backups as the solution for ransomware. Given that cybercriminals know they can gain a foothold through zero-day exploits, they have developed techniques to get past these commonly-deployed security defenses.

[4] https://insights.dice.com/2021/02/11/data-breach-costs-calculating-the-losses-for-security-and-it-pros/

Why zero-day patches do not solve the problem

If a zero-day vulnerability is first uncovered by the vendor or an ethical hacker, the vendor may be able to fix it before cybercriminals can craft an exploit for it and launch an attack. Unfortunately, that does not always happen. In fact, according to the latest federal Cybersecurity and Infrastructure Security Agency (CISA) alert on routinely exploited vulnerabilities, "[A] majority of the top vulnerabilities targeted in 2020 were disclosed during the past two years."[8] In other words, patches were available for these vulnerabilities, but they continued to be routinely exploited.

Frequently, vendors have no idea a zero-day vulnerability exists until a cybercriminal exploits it and launches an attack -- or a series of attacks, as in the case of the NotPetya attacks, which were fueled by an NSA zero-day exploit called EternalBlue.[9]

Unpatched Systems: Many companies do not apply patches on a timely basis. The 2017 Equifax data breach, which compromised data belonging to over 145 million Americans, happened when cybercriminals exploited a vulnerability in Adobe Struts. A patch for the vulnerability had been available for several months, but Equifax had not applied it.[10]

Cost of Patching: Many companies cannot afford to patch regularly. This is particularly the case among small and medium-sized businesses (SMBs) and small municipal government agencies.

Prioritizing Business Operations over Patching: Many companies cannot patch regularly because they have limited windows in which they can take their network down to perform significant patching. This happens frequently in healthcare settings, as well as other critical infrastructure, such as utilities.

Exploits are Deployed Faster: Many zero-day exploits are deployed rapidly, enabling cybercriminals to gain a foothold into enterprise systems, move laterally, and find and exploit additional zero-day exploits.

[8] https://us-cert.cisa.gov/ncas/alerts/aa21-209a

[9] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

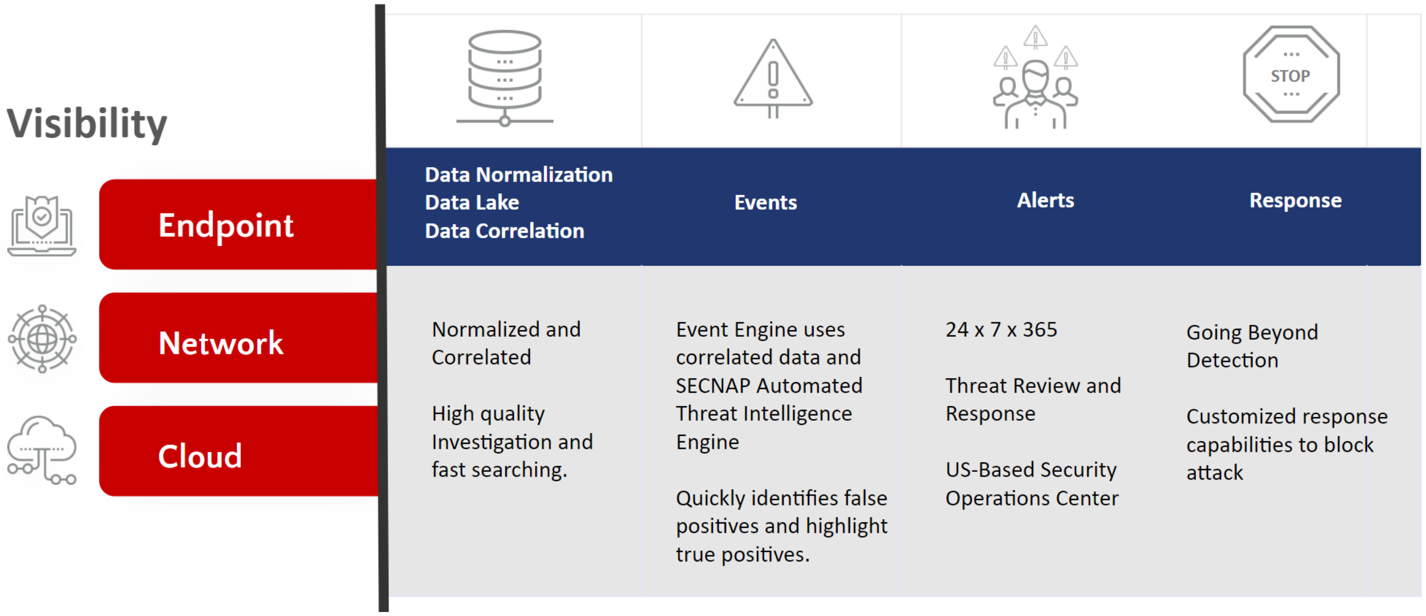
[10] https://www.theverge.com/2017/10/3/16410806/equifax-ceo-blame-breach-patch-congress-testimony

The SECNAP CloudJacket XDR Platform

SECNAP Network Security has created CloudJacket XDR™ -- an Extended Detection and Response (XDR) platform to solve this problem. We created CloudJacket XDR to solve these issues of affordability by creating from the ground up a complete XDR solution that is designed for, and affordable by SMBs and midsize enterprises. CloudJacket XDR is our own proprietary, patented and patent-pending technology, and has been successfully

CloudJacket XDR™ empowers organizations of all sizes to detect and respond to ransomware and other advanced cyber threats, enabling them to have the same comprehensive protection against cyberattacks that large enterprises and the federal government enjoy, but at a fraction of the cost.

Five years ago, we foresaw that the significant uptick in cybercriminal activity was not an anomaly, and that it would begin to increase exponentially. Accordingly, five years ago, we began building a security solution created on the concept that every item in a “complete security stack” is a necessary element for middle market companies (SMB to mid-enterprises) to effectively detect and respond to ransomware. CloudJacket XDRTM is the result of those efforts. (In our view, a “complete security stack” comprises -- Intrusion Detection; Intrusion Prevention; Security Info Event Management (SIEM); Managed Detection and Response; Internal Threat Detection; Lateral Threat Detection; Vulnerability Management and Security Assessments -- with all data and log information from all of these security components collected, normalized and correlated, analyzed through an advanced intelligence engine, and with the resulting alerts provided to a security operations center (SOC) for final analysis and decisions as to blocking and addressing threats).



Visibility

- Endpoint
- Network
- Cloud

Data Normalization Data Lake Data Correlation	Events	Alerts	Response
Normalized and Correlated High quality Investigation and fast searching.	Event Engine uses correlated data and SECNAP Automated Threat Intelligence Engine Quickly identifies false positives and highlight true positives.	24 x 7 x 365 Threat Review and Response US-Based Security Operations Center	Going Beyond Detection Customized response capabilities to block attack

How organizations can defend themselves against zero days

Many organizations deploy a combination of endpoint detection and response (EDR) systems plus backups of data as the principal defense against zero-day attacks. EDR systems collect and analyze telemetry from endpoints, such as employee devices, and trigger alerts when they detect anomalous or malicious activity. However, because cybercriminals have learned to get around these systems, they have a high failure rate. In a recent research study, a team of security experts tested 11 of the most popular EDR systems by launching attacks against them. Over half of the attacks were successful, meaning that the EDR did not even generate an alert. [11]

Defending against zero-day attacks requires a layered approach. Gartner and other cybersecurity tech consultants have named this approach "extended detection and response" ("XDR"). Extended Detection and Response (XDR) is a new class of cybersecurity solution specifically created to address the exponentially increasing threats to our country's businesses and governmental organizations from cybercriminal activity such as ransomware. Somewhat like EDR, XDR works by collecting and analyzing telemetry. However, while EDR focuses on endpoint devices, XDR takes a broader, more holistic approach.

In a recent research study, a team of security experts tested 11 of the most popular EDR systems by launching attacks against them. Over half of the attacks were successful, meaning that the EDR did not even generate an alert. [11]

An XDR platform provides unified security, automatically collecting, normalizing and correlating logs and other data from numerous network, cloud and security components. This data is digested and analyzed through an alerting-logic engine, with the results provided to Security Operations Centers (SOCs) security analysts, who monitor these alerts 24/7.

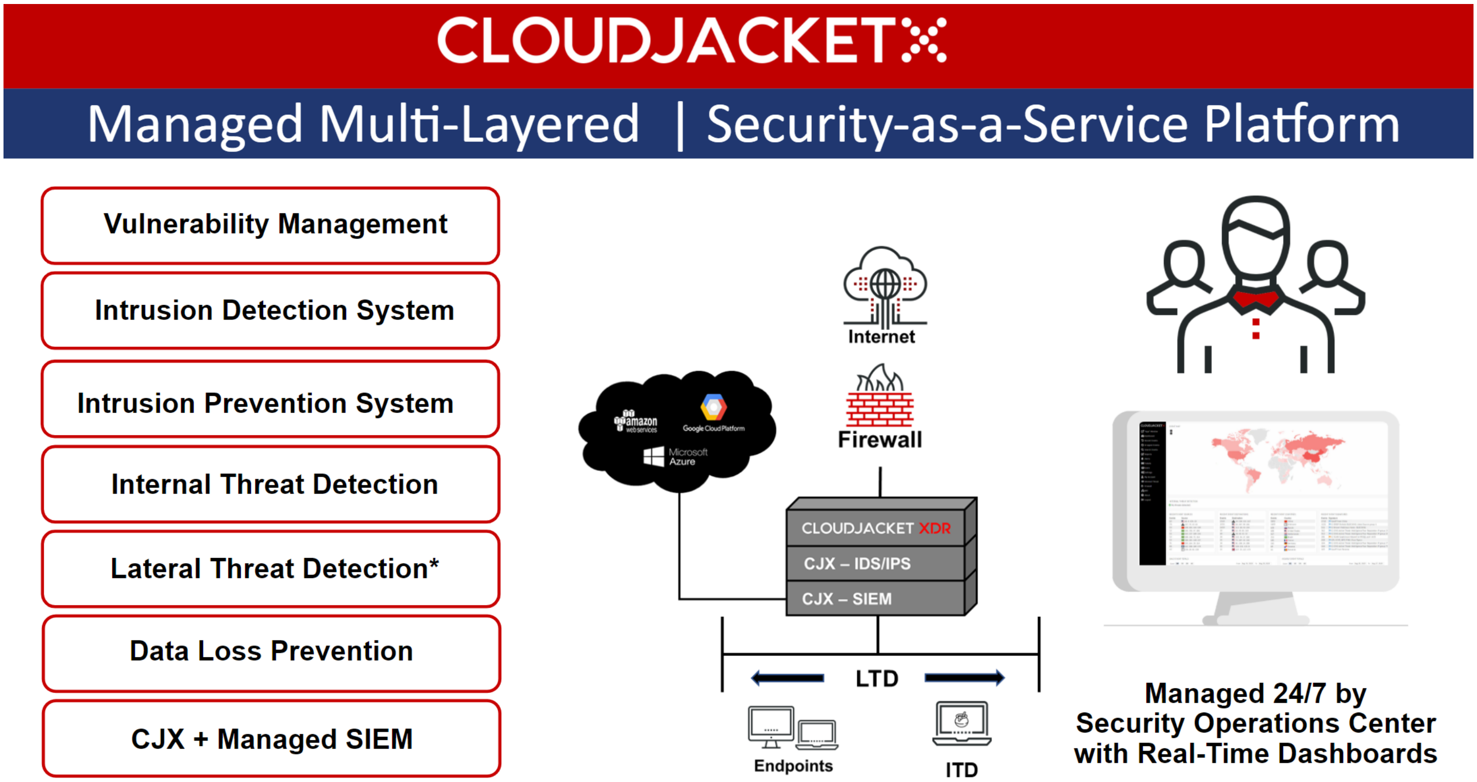
The problem described above has, of course, mainly been a problem for middle market companies. [12] Large organizations (Fortune 1000 companies and major federal government departments) are rarely hacked by cybercriminals, because they can afford to spend the millions of dollars annually that proper cyber security defenses have traditionally required. Middle-market companies and municipalities are major targets of cyber criminals because they have not been able to afford these high costs of cyber defense. That's the problem – extremely high costs of deploying and maintaining a full XDR solution, making this defense out of reach for most middle-market companies.

[11] https://www.scmagazine.com/home/research/edr-alone-wont-protect-your-organization-from-advanced-hacking-groups/

[12] For this paper, we define middle market companies as small-to-medium businesses (SMBs) and mid-size enterprises (MSEs) -- companies from the smallest that need security up to approximately $3 billion in annual revenues and 3,000 employees.

SECNAP's Solution to the Dilemma

In summary, we saw a need in the market for a unified, integrated, complete solution for middle-market companies. Our vision was validated this past year when Gartner, the leading analyst for cybersecurity products and solutions, wrote its report entitled "Innovation Insight for Extended Detection and Response," strongly recommending that cyber security management deploy XDR in their computer networks and clouds. [13]



CLOUDJACKET

Managed Multi-Layered | Security-as-a-Service Platform

- Vulnerability Management
- Intrusion Detection System
- Intrusion Prevention System
- Internal Threat Detection
- Lateral Threat Detection*
- Data Loss Prevention
- CJX + Managed SIEM

Managed 24/7 by
Security Operations Center
with Real-Time Dashboards

About CloudJacket XDR

CloudJacket XDR is our proprietary extended detection and response (XDR) platform providing unified security, automatically collecting, normalizing and correlating logs and other data from numerous network, cloud and security components. This data is digested and analyzed through our patented and patent-pending advanced intelligence engine, with the results provided to our U.S.-based Security Operations Centers (SOCs) security analysts, monitoring our clients 24/7.

[13] Gartner report: ID G00718616, Refreshed 8 April 2021, Published 19 March 2020.

SECNAP
NETWORK SECURITY

Get a complimentary and customized consultation regarding your organization’s cybersecurity strategy.

About SECNAP Network Security

Since 2001, SECNAP Network Security has been combining human intelligence with innovative technology to protect organizations of all sizes against cyberthreats, including ransomware, data breaches, phishing, and advanced persistent threats (APTs).

CloudJacket XDR is our proprietary extended detection and response (XDR) platform providing unified security, automatically collecting, normalizing and correlating logs and other data from numerous network, cloud and security components. This data is digested and analyzed through our patented and patent-pending advanced intelligence engine, with the results provided to our U.S.-based Security Operations Centers (SOCs) security analysts, monitoring our clients 24/7.

As an alternative to full XDR services, our CloudJacketX managed security-as-a-service platform also can be highly-customized to precisely fill customers’ needs. Network security assessments can be combined with MDR (managed detection and response) services, advanced SIEM solutions, and/or our intrusion detection and prevention systems (IDS/IPS), to provide multiple layers of detection and protection. To learn more visit www.secnap.com or call 844-638-7328.

AICPA SOC aicpa.org/soc4so

GSA Advantage!

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM