CYREBRO

Incident Response Analysis Report

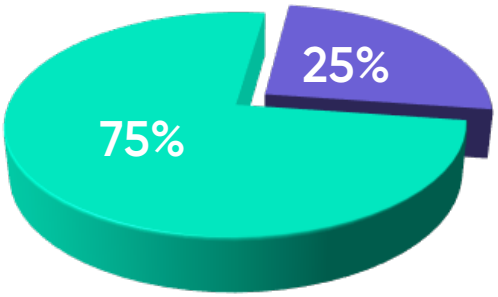
Why network and endpoint visibility is key to preventing cybersecurity incidents.

TABLE OF CONTENTS

Executive Summary

Security incidents are now endemic in the world of business. Unfortunately, without the right tools and processes, it is only a matter of time before your company succumbs to a cyberattack.

Several years ago, CYREBRO analyzed internal incident response (IR) reports and uncovered a staggering statistic: **75% of reported security incidents** were caused by inadequate investment in security solutions that caused blind spots in network visibility.



75% of incidents caused by inadequate security investment

Global cybercrime damage is predicted to reach $10.5 trillion annually by 2025. However, estimates also suggest that there are currently at least 3.5 million unfulfilled cybersecurity staff roles, and as businesses face a shortage of skilled help, automated tools have to bridge the gap to assist existing teams with network defense, patch processing, acting on threat intelligence, and managing the potential aftermath of a security incident.

It takes a single blind spot to put an entire business operation at risk. Unless you can adequately observe network traffic, access requests, endpoints, user behavior, and connected devices, and you are aware of what is happening in your enterprise environment, IT teams will struggle to establish adequate cybersecurity defenses.

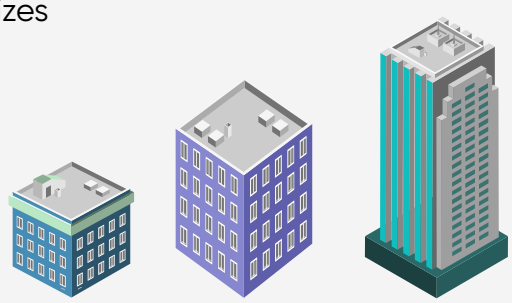
Investing in cybersecurity tools alone isn't enough. We know that there are consistent reasons that today's businesses fall prey to cyberattacks – and network visibility is a critical weakness that the enterprise needs to address.

Research Methodology

To find the common threads connecting businesses that have experienced a recent security breach, CYREBRO analyzed 50 incident response reports for correlations.

The reports we analyzed came from businesses across a wide range of industries, locations, and company sizes: we included enterprise firms with upward of 5,000 employees, SMBs with fewer than 15 employees, and everything in between. We also considered clients operating different network architectures, contrasting network sizes, and those with varying software and network management solutions.

Organization sample sizes



Our sample was deliberately diverse, yet we found that businesses experienced the same issues. Nevertheless, more often than not, we are making the same central recommendations to improve their security postures following a cyberattack.

The modern business should adopt the mindset of 'when' they will experience a breach, rather than 'if' they will. With this in mind, CYREBRO has provided commonalities we found in IR reports and our recommendations for improving network protection.

Key Findings

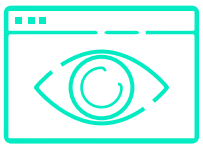
67% of the cases showed the attacker utilizing unpatched, outdated, or End-of-Life apps and systems in attacks.

64% of cases were the result of exposed ports, servers, and critical services.

78% of cases were due to lack of EDR or anti-malware solutions to monitor endpoints.

The Common Denominator: Network Blindness

Network visibility is an awareness of the components and data within an enterprise network. Therefore, network visibility can refer to the various tools that organizations use to increase awareness of their data and other network content. In many of the IR cases CYREBRO recorded, client networks had zero-to-no visibility over endpoints, servers, network devices, and critical corporate assets.



Before CYREBRO built its SOC Platform, 75% of IR cases CYREBRO recorded showed the breached network had low device and asset security tool visibility.

VISIBILITY PREVENTS CHAOS

Once an attacker obtains initial access into a corporate network, they are free to conduct malicious activities, including data theft, account hijacking, ransomware deployment, or even wholesale asset destruction.

If there is no network visibility or centralized endpoint protection solution, today's cyber attackers are more likely to be able to move undetected and laterally through a network. Malware could be left to propagate, unchecked, until it's too late.

These weaknesses are also exploited to perform supply chain attacks. SolarWinds and Kaseya are notable examples, in which cyber attackers were able to infiltrate an organization's network, undetected, and serve malware to a vendor's customers, thereby expanding the attack surface.

ATTACK SURFACE AND TECHNOLOGY GROW SIDE BY SIDE

59% of respondents to a 2020 SANS survey on network security said that a lack of network visibility poses a "high or very high risk" to business operations, and 64% of participants had experienced at least one security incident over 12 months.

Only 17% said they achieved high visibility into their network traffic. With the current shift to cloud technologies, SaaS, and remote working practices, this is nowhere near enough for adequate security hygiene.

Without the ability to view the attacker's actions live, security analysts cannot properly react to the attack in real-time, potentially leading to more extensive and damaging security incidents.

Leading Causes for High Impact Incidents

1. EASILY ACCESSIBLE PORTS AND SERVICES

CYREBRO's data analysis and research reveals that 64% of the security incidents resulted from critical ports and services being accessible from the internet with no filtering. Ports, servers, and critical services are open and exposed online too often. As an organization grows, so does its network. An extensive network often consists of servers used for various services and operations: including backend development, testing, applications & services, virtual private networks (VPNs), and customer relationship management (CRM) suites.

A number of these servers inherently need to be accessible from the internet. However, as these servers are part of the network and a domain, they will pose a security risk if they are not adequately secured.

If an attacker ever takes over these servers, they could be used as the point of entry to internal networks and resources.

64%

of the security incidents resulted from critical ports and services being accessible from the internet with no filtering.

CLOSING THE DOOR

Ports, servers, and critical services are open and exposed online too often. As an organization grows, so does its network. An extensive network often consists of servers used for various services and operations: including backend development, testing, applications & services, virtual private networks (VPNs), and customer relationship management (CRM) suites.

A number of these servers inherently need to be accessible from the internet. However, as these servers are part of the network and a domain, they will pose a security risk if they are not adequately secured.

If an attacker ever takes over these servers, they could be used as the point of entry to internal networks and resources.

CONNECTION, ACCESS MANAGEMENT IS KEY

Management connections to these servers should be allowed through firewalls only from internal network segments. Security tools such as EDR and DLP should also cover these servers. Their communication should go through an IPS or IDS to detect or prevent exploitation attempts, including brute force attacks and network-based attacks.

The basic task of checking for misconfiguration and improper external access controls can be managed quickly without costing businesses a single cent. However, a recent study suggested close to half of all S3 buckets online might be misconfigured. Properly securing AWS S3 buckets and ElasticSearch databases is often overlooked, and this could have disastrous consequences for businesses.

2. OUTDATED AND END OF LIFE SYSTEMS ARE LIKELY TO BE EXPLOITED

In 67% of the cases CYREBRO researched, our analysis showed the attacker utilizing unpatched, outdated, or End-of-Life applications and operating systems in attacks.

We investigated many cases in which the primary entry point to the network was an old, internet-facing server or device which had Windows 7 or 8, and several Windows XP devices

In most cases, these systems stopped receiving security updates years ago. Unfortunately, this allowed attackers to deploy scripts that automatically scan for systems susceptible to well-known vulnerabilities, including Eternal Blue, Bluekeep, Zerologon, and Proxylogon.

In other cases, we saw application and web servers hosting outdated versions of Jenkins, Oracle WebLogic, and IIS, which are vulnerable to Remote Code Execution (RCE) attacks, granting hackers complete control of infected systems.

67%

of the cases CYREBRO researched showed the attacker utilizing unpatched, outdated, or End-of-Life applications and operating systems in attacks.

THE MODERN LANDSCAPE

As noted in the 2022 Attack Vector Landscape report, an analysis of over one million computer entities and events, over 18,000 new vulnerabilities were documented in 2020. Furthermore, 40% of all security incidents that CYREBRO investigated began with a vulnerability exploit, including the recent Microsoft Exchange Server zero-day flaws, SQL injections, and bugs in legacy software.

Keeping your network updated is key to protecting your data and the integrity of your network. However, while updates for improved functionality and user experience are important, security fixes are essential. The moment a zero-day vulnerability in popular services or software becomes public, threat actors develop exploits to take advantage of them – and so overseers need to be in place to apply patches as soon as they are available.

IT MAINTENANCE = CYBERSECURITY

The takeaway? Maintaining proper patch processes and updating your operating system is always cost-effective – and avoiding investment in newer software and operating systems will not save you money in the long run.

Over 450,000 new malware samples are recorded every day, and a recent survey suggests that even when patches are available, organizations fail to update their systems promptly. In fact, over 55% of cybersecurity incidents occur because of failures to patch, and over half of organizations said it could take at least five weeks to patch high and critical importance vulnerabilities.

3. WEAK VISIBILITY DUE TO MISSING TOOLS

Of the cases CYREBRO research, 78% had no EDR or antimalware solution installed on endpoints, and 35% of the subjects had no IPS or IDS solution in their network.

Visibility is crucial, but missing cybersecurity tools makes defense more difficult

The majority of these cases could have been completely avoided if an Endpoint Detection and Response (EDR) solution was installed on the targeted devices. Additionally, most of the intrusion attempts utilized simple and known attack tools such as Meterpreter, CobaltStrike, and PowerShell Empire.

These tools and other legitimate software packages abused for malicious purposes should all be detectable by EDR solutions available on the market today.

As the pandemic spurred on the adoption of cloud platforms and SaaS solutions, the transition from on-prem to decentralized networks requires more oversight by EDR and network visibility solutions – and so quick incident detection and response is now of critical importance in addressing threats.

78%

of the cases CYREBRO researched had no EDR or antimalware solution installed on endpoints, and 35% of the subjects had no IPS or IDS solution in their network.

NETWORK SECURITY, LAYER BY LAYER

Combining an EDR with an IDP\IPS provides significant security layers to your network. Suspected network scans, brute force attacks, and exploitation attempts should be detected or even denied by the IDS\IPS. If the attacker somehow manages to go through it, the EDR should be able to detect most incoming attacks.

Although these are robust, standalone security solutions, we would be naïve to put our complete trust in their threat denial capabilities alone – we also need to collect threat intelligence along the way.

Other than the obvious malicious activity detection and prevention features of EDR and antivirus programs, many EDRs such as Carbon Black Defense, SentinelOne, Microsoft ATP, and CrowdStrike also collect event data generated from the devices they are installed on.

This feature allows security analysts to investigate most of the suspicious activity performed on a device. In addition, it will enable a clearer vision as to what was happening at the time of attacks and provides hashes for files and records related to network communication.

A security breach can be scoped and contained faster using an EDR by quarantining devices, blocking file hashes, blocking IP addresses, and more.

Today, a good security posture requires network visibility tools, endpoint protection, and IDP\IPS solutions. However, investing in only one area will create weaknesses that attackers can exploit. Cost savings may be made now by choosing not to adopt EDR tools but resolving otherwise preventable security incidents caused by a lack of suitable tools can result in substantial costs in the future.

SECURING THE NETWORK

The average cost of a data breach has increased by 10% year-over-year to $4.24 million, and when remote work was involved this caused an additional $1 million in damages.

It takes an average of 287 days to identify a breach, but if the right network visibility systems are in place, organizations are in a better position to contain security incidents.

Organizations must ensure that corporate assets, endpoint devices, internet-facing servers, and remote collaborative tools are all monitored. Once merged with a client's existing defenses, solutions like a SOC Platform can bridge network gaps, identify weaknesses, and make sure that defenders have access to the status of every endpoint in real-time.

Takeaways

64% of the security incidents recorded were caused by **open, exposed critical ports and services**

67% of samples, attackers were able to exploit **unpatched, outdated, or end-of-support** applications & operating systems

The leading cause surrounding incidents and breaches is **lack of visibility due to missing tools and reporting systems**

Some solutions can help: firewalls, EDR, IDS, IPS, UEBA, and more can contribute to network protection, but a monitoring system is essential

Improper cybersecurity practices such as these are what prevent sufficient network visibility which ultimately leads to breaches and IR cases

NETWORK VISIBILITY CAN BE ACHIEVED

Visibility is key. A network with good visibility gives security analysts a quick and decisive method of scoping and containing incidents and may allow them to stop an attacker in their tracks entirely.

Visibility can come in different forms. Solutions that defend different aspects of a network provide the best network coverage possible. These can include:

NETWORK VISIBILITY:

Firewalls: Firewalls can record all ingress and egress network sessions and provide essential network protection through allow and deny lists

IDS\IPS: Intrusion detection systems (IDS) and intrusion prevention systems (IPS) record all ingress and egress network sessions, analyze their content, and allow PCAP dumping. They can also detect suspicious network activity.

ENDPOINT VISIBILITY:

EDR: Endpoint detection and response (EDR) solutions can manage endpoint and server activity, including file execution, network connections, user activity, and more.

Auditing: Applications and operating systems should be configured to allow audit activity. These logs can be collected to a centralized aggregator and used as standalone logs in an investigation.

USER ACTIVITY VISIBILITY:

UEBA: User behavior analytics tools (UEBA) create visibility of user activity and be havior and can often flag suspicious activity.tion.

In 2021, Gartner recognized the need for cybersecurity "mesh" as a top trend in the enterprise. Rather than focus on standalone tools, today's organizations must ensure that solutions can work interoperably. In addition, with business technologies now often remote and off-prem, centralized visibility systems and controls are necessary to protect assets.

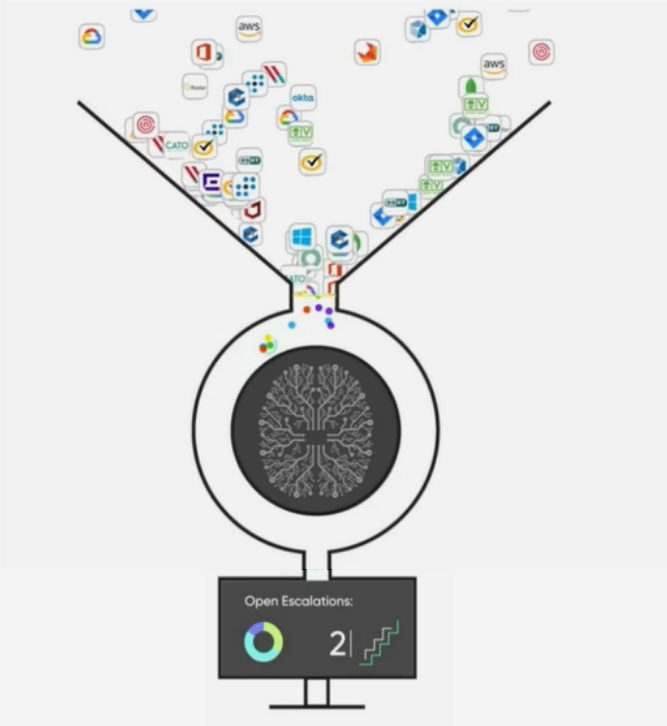
CYREBRO

Achieve Unparalleled Visibility with a SOC Platform

As is shown in our analysis, throwing money at cybersecurity defenses and hoping for the best is not going to keep your business safe. Focusing on the fundamentals and critical areas can mitigate the risk of cyberattack exposure – a worthwhile ROI for any business.

Nevertheless, attackers are very quickly adapting and learning to deceive point solutions. This leads to increased MTTD and MTTR, as the attack story is unclear when alerts indicate suspicious behavior is occurring in the network, costing businesses greatly in recovery and downtime.

The ability to connect all your business's security systems and tools into a single, central command will provide an unmatched level of visibility, context, and clarity about events in your network. CYREBRO's SOC Platform integrates the tools you're currently using, as well as any you decide to use in the future, and monitors your entire infrastructure, creating correlations between seemingly disparate events to create a full attack story and increase network visibility.



Recovering from an attack with limited visibility is difficult and takes time, but by adopting CYREBRO's SOC Platform, organizations can mitigate security incidents' potential cost and downtime and prevent future incidents from occurring.

Learn more about CYREBRO