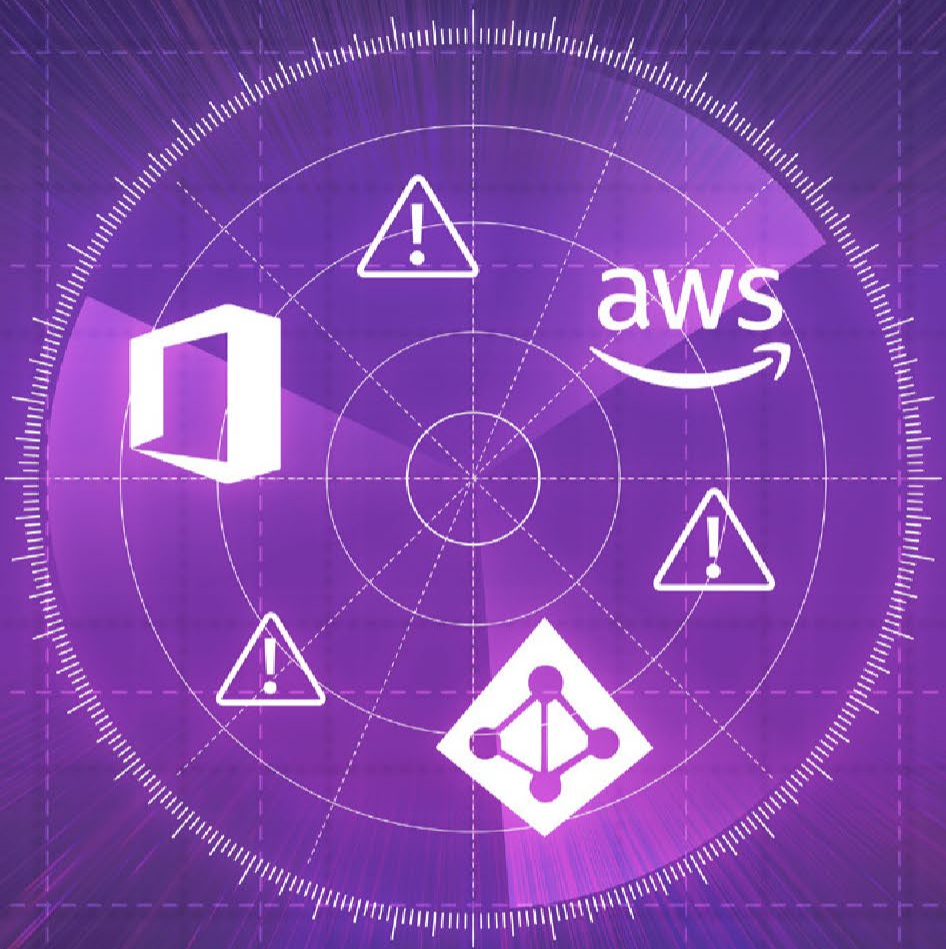
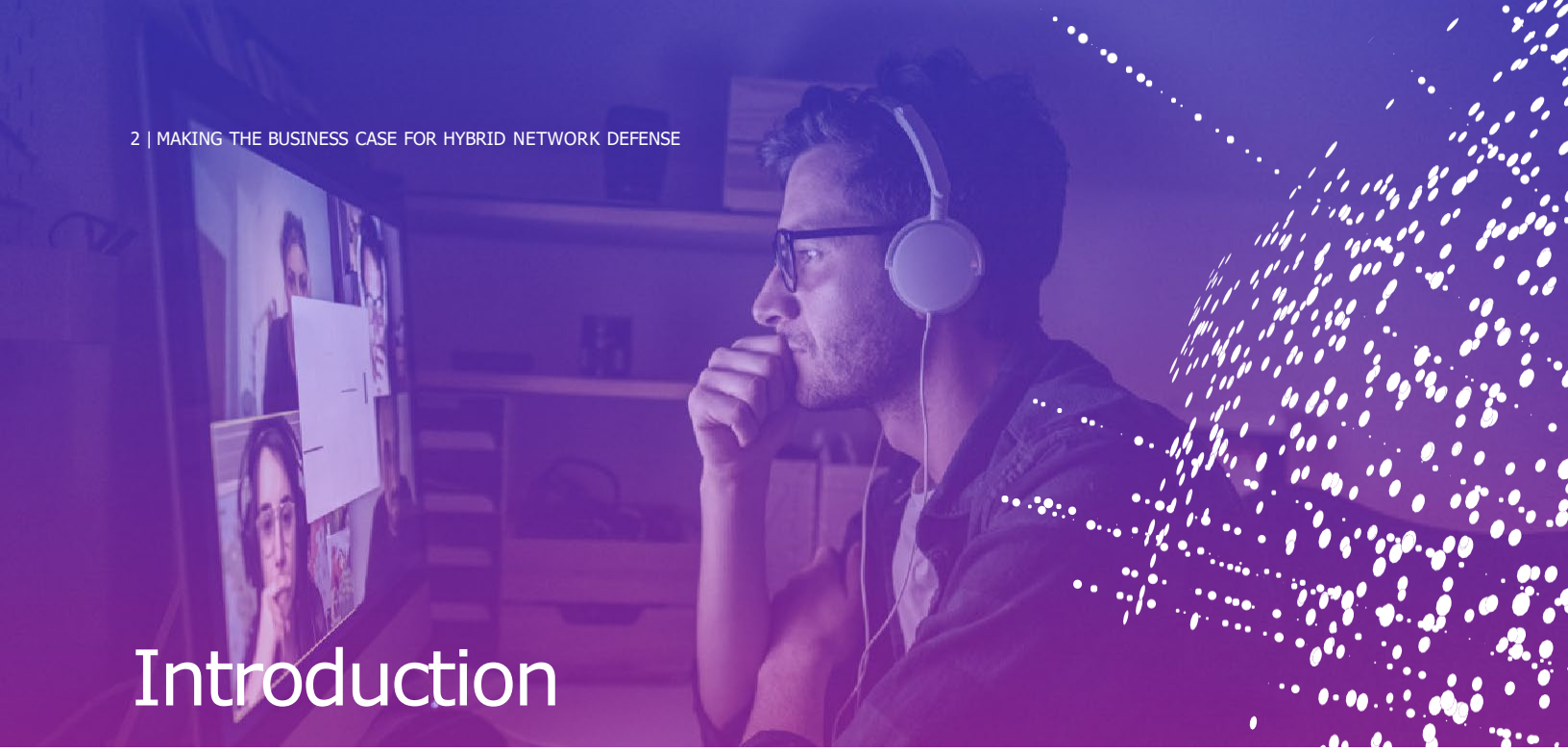
CyGlass




# Making the Business Case for Hybrid Network Defense



# Introduction

The equation for making the business case for purchasing cybersecurity tools is not straightforward and is usually underappreciated until something goes horribly wrong. Clearly, the importance of attack surface visibility and threat detection and response is easily defined for IT and Cyber professionals. Still, the business case that needs to be made to support these folks in receiving funding for badly needed people and technology remains a challenge.

One approach to building an investment business case is to reverse the traditional ROI model by detailing the cost of a successful attack on a company and accepting 100% of that predicted loss if no protection exists. The budget needed for cybersecurity tools and people will be the cost of investment (CI), and the gain for investment (GI) will be a percentage in the reduction of the 100% cost of the full cyberattack. The equation:

Full cost of cyber attack = $1 million
Cost of cybersecurity tools and staff (CI) = $400,000
Reduction in cost of attack is 50%, so Gain from investment (GI) = $500,000

ROI = (GI)-(CI)/CI X100
ROI = (500K-400K)/400K X 100
ROI = 25%

The challenge for IT/Cyber pros is that there is no easy linear way to define what that cost reduction is. The simple truth is a cyberattack can happen to anyone and requires multiple layers of tools and processes to protect against. So how do we assign that reduction % and build a solid business case? The good news is that our financial and business counterparts deal with this type of ambiguity every day as they create business plans to invest in a new production facility or product line. They have to build assumptions into the model on future outcomes like us.

The assumptions look something like this, "based on the sales of like products in that market, surveys of customer demand by analysts, and customer demographics, we believe the sales for the products over the next three years will be $1 million, and the cost of the plant will be $400K. We think we will win 50% of the deals based on the competition, and our ROI will be 25%. Remember, the ROI Calculation in a business plan is not meant to be perfect; it is a way to justify a business investment.

## Assumptions

For many years, it was challenging to capture an ROI on a security tool. The issue is that the ROI does not become apparent until an attack occurs, and just a few short years back, very few companies were being attacked. The advent of ransomware that targets everyone has changed all that.

Assumption 1, in any given three-year period, the likelihood of being targeted for a cyberattack is 100%. Three years is conservative; most reports claim 50% of businesses are hit every two years[1]. We will build our ROI for a three-year period.

Assumption 2, no single cybersecurity tool can prevent or stop a ransomware attack[2]. For example, a PurpleSec survey found that 75% of successful ransomware attacks were against companies with up-to-date EDR deployed.

Assumption 3, based on the fact that no single tool can stop a ransomware attack, we will assign discount values for each type of security tool based on threat surface coverage and the role of the tool. When building your ROI model, you can change these assumptions to your liking. In our model, we will focus on Firewalls, EDR, and NDR defined as Hybrid Network Defense. Our discount model:

| Tool | Discount | Logic |
|---|---|---|
| Firewall | 80% | Firewalls are rules based control tools with signature based detection. They a core to simple attack defense, but are challenged by more advanced attacks. They also suffer from rule error due to complexity. |
| Add EDR | 50% | EDR is the best defense for endpoints where a majority of attacks first attempt to gain a foothold. Weaknesses are the ability of modern attacks to buy pass them and the inability to cover IoT and other specialty devices. |
| Add Network Defense (NDR) | 40% | NDR covers risk reduction and threat detection across network and cloud environments. The attackers ability to succeed in a cyberattack relies on using the network and not being detected. Hybrid Network Defense offers greater chances of success over NDR because its reduction in complexity and cost enhance security operations. |

Simply put, when an endpoint is compromised, the attackers' next steps are to use command and control communications and reconnaissance techniques to search the network for the systems that hold valuable target data or services.

1 https://www.hiscox.com/blog/your-business-prepared-cyber-attack
2 https://purplesec.us/resources/cyber-security-statistics/

If you are not minimizing risk and watching for indicators of compromise (IOCs) on your network, you are an easy target.

To make our business case more realistic, we will use a real (unnamed) organization that suffered a real (unreported) ransomware attack. Our organization has 450 employees and operates across four locations, and the company has annual sales of $50 million.

The company had both firewall and EDR deployed for cyber defense. The Cyber/IT team consisted of two full-time employees. The attack used a malicious link in a social engineered email to compromise an endpoint. The attacker then easily moved through the network to find sensitive customer and employee data and then executed encryption ransomware on that data. Let's look in detail at the cost of that attack.

75% of companies successfully infected with ransomware were running up-to-dates endpoint defense [2]

## Detailing the costs of a cyberattack

In our equation, the "Gain from Investment" (GI) is built from the cost of the cyberattack. Our business case will argue that with the correct tools and staff, we could have had a fighting chance to prevent that attack. So we must start with understanding the costs.

Cost of a cyber attack = (Cost of Downtime + Cost of the Attack + Cost of reputation/customer loss + soft costs + business rating loss).

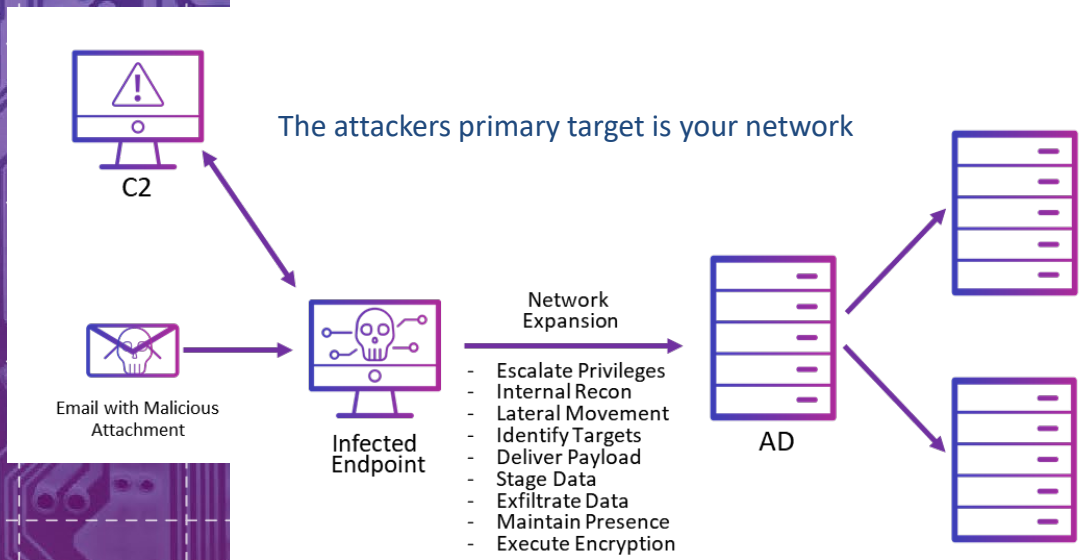



Fig. 1Ransomware stages focused on expansion through the network

CyGlass

## Cost of Downtime

All organizations use their IT systems and network to design, create, offer and support their goods and services. From law offices to community banks, manufacturers to retail sellers, if a cyberattack or ransomware attack shuts down services, the result is a loss of revenue. Downtime is defined as the loss in revenue from systems being offline. It is easy to calculate a revenue per hour number for any company. Our example company has $50 million in annual revenue. Divide the $50M by 2080 (the number of business hours in a year), so our company drives $24K per hour. This ransomware attack cost the company 15 days of downtime. That number is on the low end of the average for a ransomware attack is 15 days[3]. Downtime/lost revenue cost our company suffered is $2,884,615.

Downtime is almost always the largest single loss factor for an organization, and the more sales a company drives, the faster the downtime losses add up. These losses are why many small companies never recover from an attack and go out of business[4].

## Cost of the Cyber Attack

There are two primary ways for our midsize company that a cyberattack will cost money beyond the loss of revenue. The first is a demand for ransom on the data encrypted/stolen or systems shut down. The second is the costs related to recovery (cost to clean and repair IT systems, cost associated with managing exposed customer data, costs of any fines, cost of attorney fees, costs of incident investigation[5]. Those costs are close to the average of an attack on a midsize company for ransom - $170K[6], while recovery costs will be about $395K[6]. The average total costs for a ransomware attack are $565,000.

For our company, the ransomware payout cost was one bitcoin or $50,000. With the payout, the company was able to recover better than 90% of the lost data, which is much better than the industry average of 65%[7].

The cost of the post-investigation, cleaning systems (which took 45 days), paying attorney fees came to $128,000, well below the reported average but still significant.

65% of small business close their doors within 6 months of a ransomware attack[7]

3 https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/

4 https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf

5 https://dynasis.com/blogs-articles/price-security-how-much-cybersecurity-attack-actually-cost/

6 https://www.cpomagazine.com/cyber-security/ransomware-recovery-costs-more-than-double-in-a-year-now-average-1-85-million/

7 https://www.cloudwards.net/ransomware-statistics/#

Monitoring of backup systems for failure is a standard feature of Hybrid Network Defense

## Soft Costs

Soft costs are defined as the cost of reputation and customer loss, insurance increases, and credit rating loss increasing interest expenses. Soft costs are often hard to explain, but they are critical and expensive for some organizations.

The total soft costs for this attack were $210,924 and consisted of reputation and customer loss, an increase in cyber insurance rates, and an increase in our cost of capital and investment as our loan cost basis increased[8]. Here is how the soft costs break down.

**Reputation and customer loss** – The company sells in a business-to-business market and has long-term contracts. The damage in terms of lost contracts was less than 1% of revenue, but the company failed their third-party supply chain risk audit and lost a $200,000 customer due to the attack. The costs of reputational and customer losses are real and can be much higher for consumer-facing organizations. If you are using the worksheet to build your business plan, here is a CSO article that details actual reputation and customer losses[9].

**Insurance** – The company was forward-thinking and had purchased cyber insurance back in 2019. Our annual cost was $924 for $1 million in coverage with a $10,000 deductible[10]. The cyber insurance required cybersecurity and resilience tools and processes to be in place at the time of the attack for the policy to payout. Unbeknownst to this company, their backup system had gone offline some months earlier. Due to that policy violation, the cyber insurance **did not payout** on this attack.

**Credit Ratings Loss, Interest Increases** – Like most companies, this organization takes loans to cover cash flows on receivables and loans on some of the larger projects, especially as interest rates remain very low. When a breach occurs, a company's credit rating is expected to drop[11]. This company's interest rates increased 40 basis points, and loan servicing costs increased by $10,000[12].

8 https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

9 https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html

10 https://advisorsmith.com/cyber-liability-insurance/cost/

11 https://www.bankinfosecurity.com/moodys-warns-cyber-risks-could-impact-credit-ratings-a-8702

12 https://www.darkreading.com/risk/data-breaches-drive-higher-loan-interest-rates/d/d-id/1341215

## Total Cost of an Attack

Our total cost for the attack we suffered amounted to $3,25 3,539. If that number is surprisingly high to you, it should not be, and it falls in between the Verizon Data Breach Report[10] and different Ponemon studies[11] for the total costs suffered by a small business.

Cost of loss revenue = $2,884,615
Ransomware payout = $50,000
Cost of recovery = $108,000
Soft costs = $210,924
Total Cost of the attack = $3,253,539

## The Cost of Hybrid Network Defense

Hybrid Network Defense as a Service is an attack surface reduction and threat detection and response service that is sold through an annual subscription. The service will automatically monitor your network and cloud 24/7 with AI risk and threat detection services and remediation capabilities.

### Network Defense Risk Mitigation Services

Risk mitigation can also be defined in terms of threat surface reduction. Before any cyberattack occurs, there is a critical measure of how easy a target you are for the attacker. The more you understand and fill the gaps and vulnerabilities across your network, the smaller your attack surface and the harder you are to attack. This aligns with a strategy by industry guru Dan Geer "you do not need to make your car theft-proof, you just need to make it harder to steal than your neighbors." The adversaries will almost always target softer targets because they are less costly and offer the potential for a greater return.

10 https://www.verizon.com/business/resources/reports/dbir/
11 https://www.scmagazine.com/analysis/ransomware/as-ransoms-on-malware-attacks-grow-financial-firms-lack-confidence


Fig. 2The Cloud Native CyGlass Hybrid Network Defense Platform covers a variety of cloud and traditional attack surfaces.

In our example, the company had deployed both Firewalls and EDR tools as part of their cyber defense strategy. In making our business case for Hybrid Network Defense (NDR), we will look at the RIO for each of those tools and, more importantly, the incremental increase in RIO as each tool and as NDR is deployed. We will start by understanding what NDR is and why it is valuable.

## Introduction to Hybrid Network Defense

NDR offers network and cloud risk visibility, threat surface reduction, and threat detection and remediation. The service identifies and tags all the devices on your network and calculates an AI-defined risk score based on the device profile and network flows. The AI will identify your mission-critical devices and services and tell you where gaps and risks need fixing.

Gaps and risks can include failed backup services, unprotected devices including IoT devices, and new/rogue devices. Tagging devices (including servers, directories, endpoints) in terms of zero-trust security zones allows the network defense service to watch and alert on zero trust violations, further reducing your attack surface.

NDR' unique ability to ingest and monitor Azure, AD and M365 logs adds an additional layer of identity and cloud risk visibility.

Services include Microsoft Azure, AD and Outlook alert prioritization, user and admin misconfigurations. All of these risk visibility and mitigation services are working 24X7. Automated scorecard reporting allows you to set threat surface reduction goals and shows your progress in reducing your network risk.

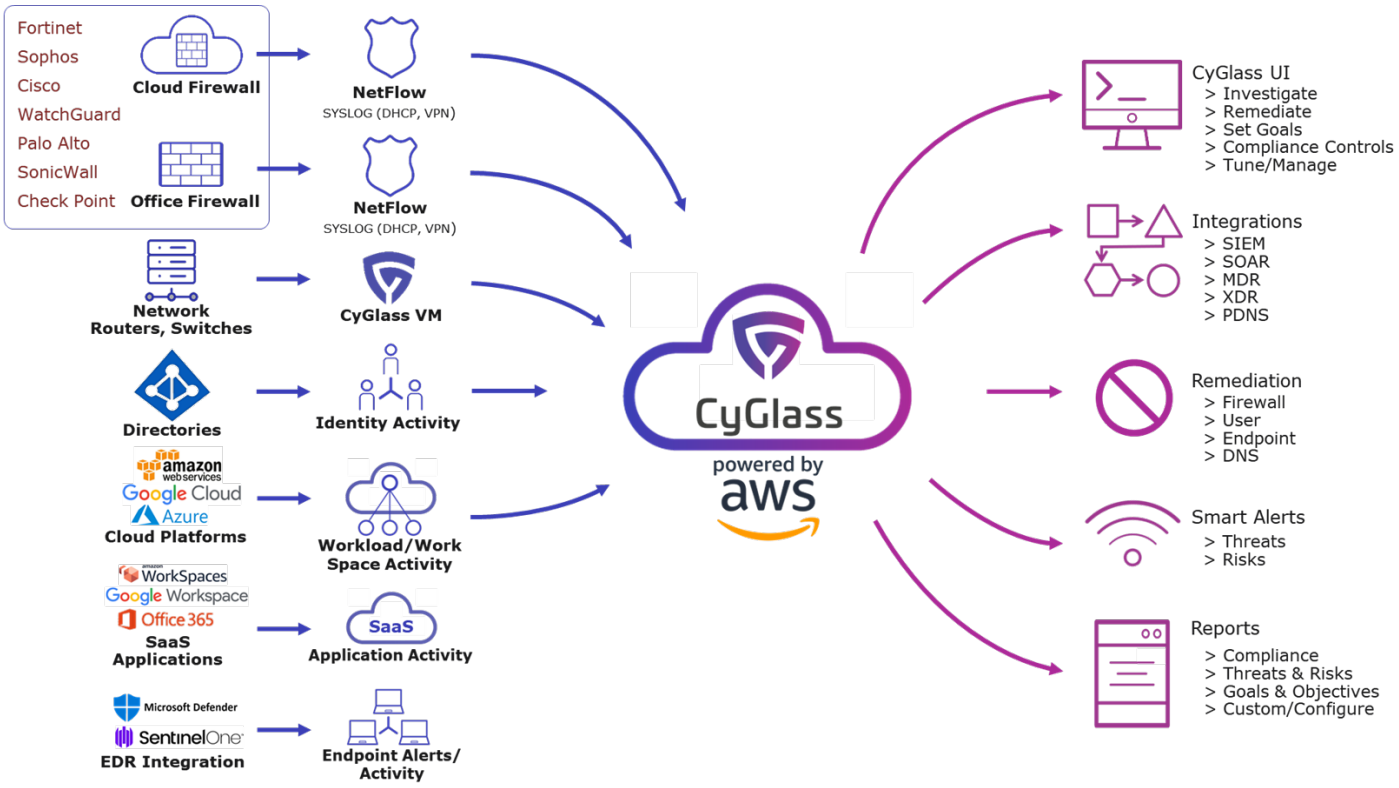



Fig. 3 The CyGlass NDR visibility, threat detection, and remediation process with the CyGlass AI engine operating within an AWS Cloud.

## Threat Detection and Remediation

The NDR platform offers threat detection and remediation across multiple attack types and stages. Because data ingest includes Azure, AD and M365, NDR AI models and threat intelligence watch, surface and correlate identity-related indicators of compromise (IOCs) including brute force password attacks (Azure/AD), account takeover (Azure/AD), unauthorized access/data share (Azure/M365).

Network IOC analytics include: probing and reconnaissance (including tunneling), command and control, lateral movement, data staging, data exfiltration, and suspicious VPN/RDP activity. The platform also includes threat intelligence and analytics that specifically watch for an alert on ransomware IOCs.

The enterprise-class AI engine in NDR will support small team operations by eliminating alert fatigue and focusing the team on a small number of significant risks and threats.

The NDR platform also uniquely offers immediate remediation when an event reaches an untenable risk level. With a click of a button, firewall rules can be changed and IP addresses blocked, users can be isolated, and endpoints can be quarantined. These immediate blocking controls are imperative in stopping a ransomware attack before an encryption payload can be injected.

In a small or medium business, where business operations are often not 24X7, and staff go home at night, the ability to quickly stop an attack from any remote location is critical in minimizing the damage and cost.

## The Cyberattack & NDR

In reviewing the post-investigation data of our example attack, CyGlass detected the failure of the backup system (which may have been an early action by the attackers).

# Network Defense Costs

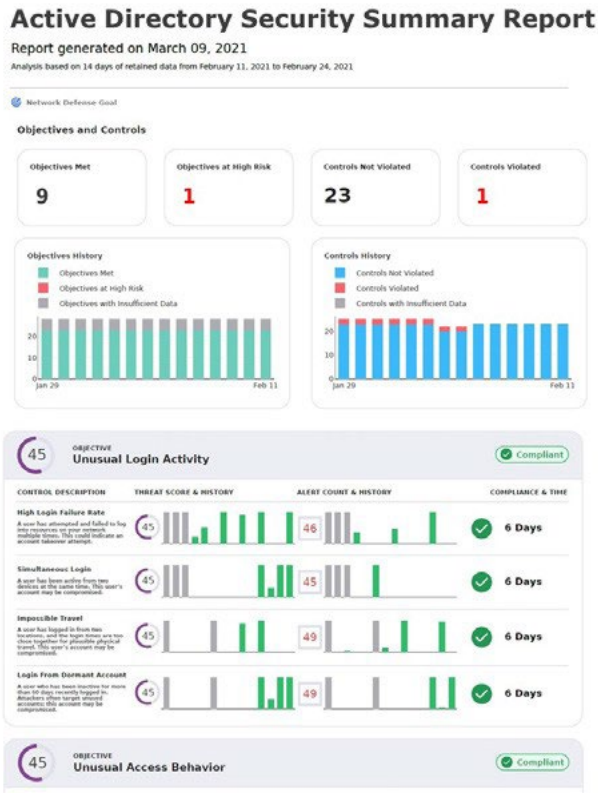



Fig. 3 CyGlass Active Directory Security Reports covers both on premise AD and AD/AZURE, and includes multiple user authentication and access risks and threats.

CyGlass would have also detected command and control communications and anomalous lateral movement from the infected endpoint to servers on the network. If NDR was deployed, it is highly (90%) likely that the attack would been detected and stopped before encryption occurred. It is 100% likely that the backup system failure would have been detected, the systems up running and the $1 million insurance policy paid.

## Costs of EDR & Firewall Investments

Our company had both Firewalls and EDR deployed at the time of the attack. The EDR protection across 530 endpoints costs $140,000 annually, and Firewalls across the four locations cost us $120,000 annually. The IT team consists of 2 dedicated security staff to operate those systems at a cost of $300,000 annually. At the time of the attack, total annual security costs were $560,000.

## Hybrid Network Defense as a Service Licensing and Pricing

The cost of CyGlass NDR – list price - is $4.99 per user per month. For the 450 employees (we will assume they paid the list price), that comes to $26,946 annually and is the entire cost of the service. There is no additional hardware, software, integration, upgrade, report creation, or other surprise costs. Our example company can add NDR without adding any headcount as a SaaS offering.

When you combine all three components (including NDR at $26,946), the total annual investment cost is $586,946.

Annual Cost of Cyber Security= $586,946

Three Year Investment = $1,760,820

CyGlass

# Calculating Three Year ROI

We are using a three-year ROI to assure a 100% chance of being hit with a cyberattack, and we can account for the SaaS licensing models of today's tools and headcount. The three-year ROI gives us a much more realistic view of investments and gains for our business plan.

The ROI calculation is "gain from investment" (GI) minus "cost of investment" (CI) with that amount divided by the CI and their time 100 to give us the ROI percent.

ROI (%) = [ (GI – CI) / CI ] × 100

Our GI = (Cost of Downtime + Cost of Attack + Soft Costs) = $3,253,539. Remember, if our cyber defenses are perfect, we would 100% block the attacks and save the full amount the attack cost the company. Since no cybersecurity is 100%, we discount this number for our business plan. In this calculation, we account for the deployment of EDR, Firewall, NDR and for headcount.

Including all tools, our discount is 40% (see page 3). Our discounted GI becomes $1,952,124 (which is 60% of the total cost of the attack.

CI = (EDR + Firewall + NDR+ Headcount) = $586,940 annually. Over 3 years = $1,760,820.

**ROI 11% = [(1,952,124 – 1,760,820) / 1,760,802] × 100**

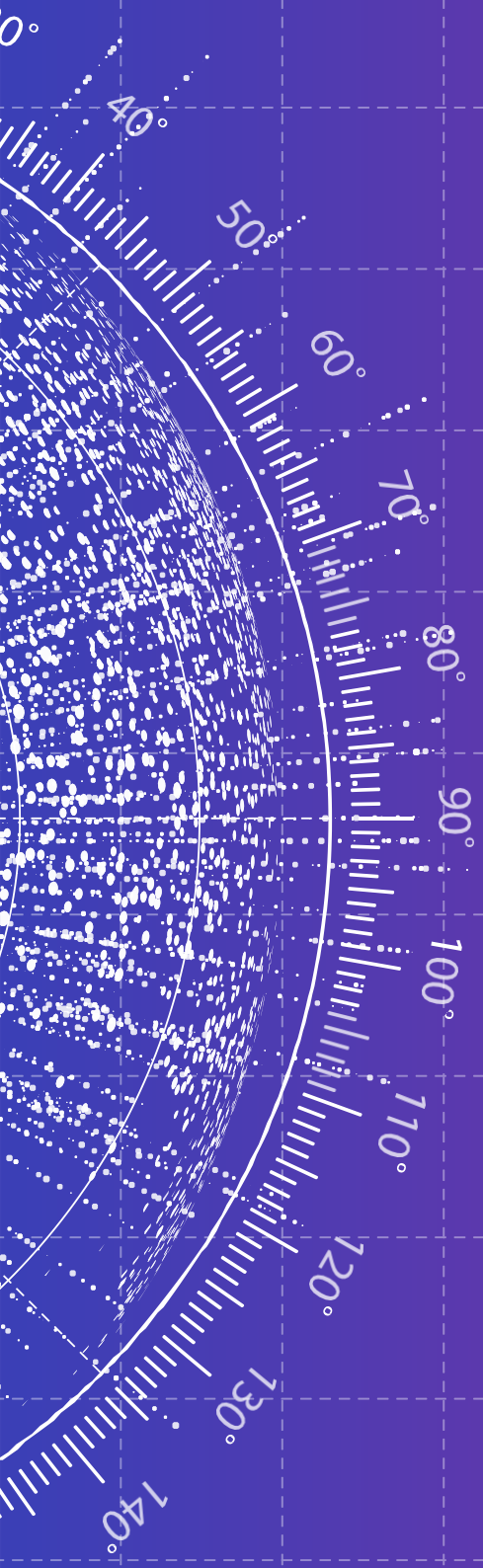
11% ROI makes for a strong business case, but that is only the beginning of the discussion. We can also look at the incremental ROI from investments in firewall, EDR and NDR based on the costs and the varying threat coverage assumptions and discounts we applied back on page 3 (Fig 4 below). This calculation measures how much return I get for each additional dollar I spend. Investing in firewalls alone will not prevent a ransomware attack and the ROI reflects that at -24%. Adding EDR offers an incremental and solid ROI of 12%, increasing our overall ROI to -3% as we are still very vulnerable to attack.

When you combine the threat surface coverage with the relatively low cost to operate, NDR, incremental ROI stands alone as an outstanding value at over 300% and takes our overall ROI to a solid 11%

| Component | Option 1 | Incremental | Option 2 | Incremental | Option 3 |
|---|---|---|---|---|---|
| Protection Level | Firewall | | +EDR | | +NDr |
| Cost of Investment | $810,000 | | $1,680,000 | | $1,760,820 |
| Gain from Investment | $650,708 | | $1,626,770 | | $1,952,124 |
| Net Return | $(159,292) | | $(53,230) | | $191,304 |
| Overall ROI | -24% | | -3% | | 11% |
| Incremental Investment | | $870,000 | | $80,820 | |
| Incremental Gain | | $976,062 | | $325,354 | |
| Incremental Net Return | | $106,062 | | $244,534 | |
| Incremental ROI | | 12% | | **303%** | |

Fig. 4 Three year full and incremental ROI measures for Firewall, EDR and Network Defense investments

CyGlass




# Summary & Takeaways

Making the business case for increased spending on cybersecurity tools and staff is not trivial. Yet, it is critically important for IT/Cyber staff to protect their organization from an increasingly dangerous cyber world. This paper offers a model to use that supports making the investment case.

Even though many articles, surveys, and reports have been written that detail the costs of a successful attack and how often attacks occur, the message often falls on deaf ears. By using an actual attack against a small company and reflecting the real numbers they paid in detail, the hope is that the information can be of value to others needing to further invest in the defense of their organization. Understanding where your costs will be most significant for your organization will help determine how to prioritize investments.

Cyber insurance is a critical part of a company's reliance strategy for ransomware defense, along with system backups. Still, neither is guaranteed as both failed to add value in a real-life attack. Backup failure, in this case, was due to a lack of automated monitoring and alerting for a small team who lost track of their manual checks. The cyber insurance policy failure was due to a poor understanding of the policy requirements and an alignment of the policy requirements to team priorities. There is a solid case to be made in automating monitoring and alerting across all types of systems and processes.

Building return on investment models to support technology and people investments will remain a challenge for most IT/Cyber professionals. Hopefully, the model in this paper and the attached worksheet will make those efforts easier. Most notably in building these models is to use your expertise to make sound assumptions. In this model, the assumptions around the likelihood of an attack, the best mix of defensive tools and the relative value of those tools can all be adjusted to fit your organization and points of view. The goal is not to create perfection; it is to make a solid business case that you can take to the management team and defend when questioned.

Cybersecurity is unique in the IT market because it takes multiple and sometimes overlapping tools to create an effective defense. Calculating incremental ROI – the return you get on the next dollar spend – is critical to building your business case when you already have tools in place.

Network and cloud visibility and defense are critical but often overlooked investments. The threat surface coverage offered by a product like CyGlass NDR is extensive and significantly reduces your chance of being attacked and data loss during an attack and improves your overall resilience after an attack. For these reasons, the incremental ROI for network defense is more favorable than an EDR or Firewall investment.

CyGlass NDR offers the added values of no new hardware or software, no new headcount needed to operate and its combination of AI-driven risk visibility, threat detection and response, 24X7 automated continuous monitoring and immediate attack remediation creates an ROI that is even stronger than legacy hardware-based NDR

CyGlass

# Input Worksheet Complete

**Cost of Technology**

| Category | Annual Cost | Three Yr. Cost |
|---|---|---|
| Tool 1 (Firewall) | 120,000 | 360,000 |
| Tool 2 (EDR) | 140,000 | 420,000 |
| Tool 3 (NDR) | 26,940 | 80,820 |

| **Current Staff** | Annual Cost | Three Yr. Cost |
|---|---|---|
| FTE Count | 2 | 2 |
| FTE Annual Cost | 150,000 | 450,000 |
| Staff Costs | 300,000 | 900,000 |

| **Additional Staff Required** | Annual Cost | Three Yr. Cost |
|---|---|---|
| New FTE Required | | |
| New FTE Cost Tool 1 | | |
| New FTE Cost Tool 2 | | |
| New FTE Cost Tool 3 | | |

| Total Cost of Investment | Annual Cost | Three Yr. Cost |
|---|---|---|
| Tool 1 + Staff (Current + New) | 270,000 | 810,000 |
| Tool 1 + 2 + Staff (Current + New) | 560,000 | 1,680,000 |
| Tool 1 + 2 + 3 + Staff (Current + New) | 586,940 | 1,760,820 |

**Defining Cybersecurity Tool Value**

Critical to our ROI calculation is the concept that no single cybersecurity tool can 100% stop a cyberattack. Every tool has varying levels of value in the process. The ROI model uses the Gain of Investment as the value of "not paying some or all of the costs calculated as the cost of the attack." Each tool helps reduces the chance of an attack and we are correlating that to reducing the amount the attack costs. The value of each tool is considered additive in the equation, and the incremental value of each tool can also be calculated. The discount is a estimation based on your experience combined with market data. A firewall for example, is core component in a cybersecurity infrastructure, but alone its value is very low, our estimation is 10% so the discount is 90%. The incremental ROI is based on the cost of adding the tool.

**Value of each tool relative to the project - discount of the tool versus other tools**

| Tool | Discount | Logic |
|---|---|---|
| Firewall | 80% | Firewalls are rules based control tools with signature based detection. They a core to simple attack defense, but are challenged by more advanced attacks. They also suffer from rule error due to complexity. |
| EDR | 50% | EDR is the best defense for endpoints where a majority of attacks first attempt to gain a foothold. Weaknesses are the ability of modern attacks to buy pass them and the inability to cover IoT and other specialty devices. |
| NDR | 40% | NDR covers risk reduction and threat detection across network and cloud environments. The attackers ability to succeed in a cyberattack relies on using the network and not being detected. NDR offers greater chances of success over NDR because its reduction in complexity and cost enhance security operations. |

| | | |
|---|---|---|
| Cost of a Cyberattack | 2080 | Business hours in a year 5 days a week, 8 hours a day |
| Categories | 8760 | Total hours in a year (for a 24x7 business) |

**Cost of downtime**

| | | |
|---|---|---|
| Annual Revenue for organization | 50,000,000 | |
| Annual rev/Hrs of work per year | 2080 | Rev/Hr. |
| Revenue/Hour | 24,038 | |
| Hours of down time | 120 | |
| **Total cost of down time** | 2,884,615 | |

**Cost of the attack**

| | | |
|---|---|---|
| Ransomware paid | 50,000 | |
| Cost in investigation | 26,000 | Internal + third party |
| Cost to clean/repair IT systems infected | 42,000 | Internal + third party |
| Cost to manage exposed customer data | 18,000 | Communications, PR, Credit Monitoring |
| Cost of fines | - | State, Federal, PCI |
| Cost of legal fees | 22,000 | |
| **Total Cost of the Attack** | 108,000 | |

**Soft Costs**

| | | |
|---|---|---|
| Reputation & Customer Loss | 200,000 | |
| Increase in cyber insurance rates | 924 | |
| Insurance deductible paid | - | |
| Increase in loan servicing rates | 10,000 | (interest or penalties) |
| Total Soft Costs | 210,924 | |

Insurance

| | | |
|---|---|---|
| Policy payout | $ - | Reduce cost by payout |
| Total Cost of the Cyber Attack | 3,253,539 | |

| | | |
|---|---|---|
| Discounted Cost of attack Tool 1 | 650,708 | (Total Cost of Cyber Attack) X (1-Tool discount) |
| Discounted Cost of attack Tool 2 | 1,626,770 | (Total Cost of Cyber Attack)X(1-Tool discount) |
| Discounted Cost of attack Tool 3 | 1,952,124 | (Total Cost of Cyber Attack)X(1-Tool discount) |

## Three Year ROI

| Component | Option 1 | Incremental | Option 2 | Incremental | Option 3 |
|---|---|---|---|---|---|
| Protection Level | Firewall | | EDR | | NDR |
| Cost of Investment | $ 810,000 | | $ 1,680,000 | | $ 1,760,820 |
| Gain from Investment | $ 650,708 | | $ 1,626,770 | | $ 1,952,124 |
| Net Return | $ (159,292) | | $ (53,230) | | $ 191,304 |
| Overall ROI | -24% | | -3% | | **11%** |
| Incremental Investment | | $ 870,000 | | $ 80,820 | |
| Incremental Gain | | $ 976,062 | | $ 325,354 | |
| Incremental Net Return | | $ 106,062 | | $ 244,534 | |
| Incremental ROI | | 12% | | **303%** | |

CyGlass

# Input Worksheet Complete

**Cost of Technology**

| Catagorey | Annual Cost | Three Yr. Cost |
|---|---|---|
| Tool 1 (Firewall) | | |
| Tool 2 (EDR) | | |
| Tool 3 (NDR) | | |

| **Current Staff** | Annual Cost | Three Yr. Cost |
|---|---|---|
| FTE Count | | |
| FTE Annual Cost | | |
| Staff Costs | | |

| **Additional Staff Required** | Annual Cost | Three Yr. Cost |
|---|---|---|
| New FTE Required | | |
| New FTE Cost Tool 1 | | |
| New FTE Cost Tool 2 | | |
| New FTE Cost Tool 3 | | |

| Total Cost of Investment | Annual Cost | Three Yr. Cost |
|---|---|---|
| Tool 1 + Staff (Current + New) | - | - |
| Tool 1 + 2 + Staff (Current + New) | - | - |
| Tool 1 + 2 + 3 + Staff (Current + New) | - | - |

**Defining Cybersecurity Tool Value**

Critical to our ROI calculation is the concept that no single cybersecurity tool can 100% stop a cyberattack. Every tool has varying levels of value in the process. The ROI model uses the Gain of Investment as the value of "not paying some or all of the costs calculated as the cost of the attack." Each tool helps reduces the chance of an attack and we are correlating that to reducing the amount the attack costs. The value of each tool is considered additive in the equation, and the incremental value of each tool can also be calculated. The discount is a estimation based on your experience combined with market data. A firewall for example, is core component in a cybersecurity infrastructure, but alone its value is very low, our estimation is 10% so the discount is 90%. The incremental ROI is based on the cost of adding the tool.

**Value of each tool relative to the project - discount of the tool versus other tools**

| Tool | Discount | Logic |
|---|---|---|
| Tool 1 | xx% | |
| Tool 2 | xx% | |
| Tool 3 | xx0% | |

| | | |
|---|---|---|
| Cost of a Cyberattack | 2080 | Yearly business hours in 5 days a week, 8 hours a day |
| Catagories | 8760 | Total hours in a year (for a 24x7 business) |

**Cost of downtime**

| | | |
|---|---|---|
| Annual Revenue for organization | | |
| Annual rev/Hrs of work per year | | Rev/HR |
| Revenue/Hour | | |
| Hours of down time | | |
| **Total cost of down time** | | |

**Cost of the attack**

| | | |
|---|---|---|
| Ransomware paid | | |
| Cost in investigation | | Internal + third party |
| Cost to clean/repair IT systems infected | | Internal + third party |
| Cost to manage exposed customer data | | Communications, PR, Credit Monitoring |
| Cost of fines | | State, Federal, PCI |
| Cost of legal fees | | |
| **Total Cost of the Attack** | | |

**Soft Costs**

| | | |
|---|---|---|
| Reputation & Customer Loss | | |
| Increase in cyber insurance rates | | |
| Insurance deductible paid | | |
| Increase in loan servicing rates | | (interest or penalties) |
| Total Soft Costs | | |

Insurance

| | | |
|---|---|---|
| Policy payout | $ - | Reduce cost by payout |

| | | |
|---|---|---|
| Total Cost of the Cyber Attack | - | |

| | | |
|---|---|---|
| Discounted Cost of attack Tool 1 | | (Total Cost of Cyber Attack) X (1-Tool discount) |
| Discounted Cost of attack Tool 2 | | (Total Cost of Cyber Attack)X(1-Tool discount) |
| Discounted Cost of attack Tool 3 | | (Total Cost of Cyber Attack)X(1-Tool discount) |

**Three Year ROI**

| Component | Option 1 | Incremental | Option 2 | Incremental | Option 3 |
|---|---|---|---|---|---|
| Protection Level | | | | | |
| Cost of Investment | | | | | |
| Gain from Investment | | | | | |
| Net Return | | | | | |
| Overall ROI | | | | | |
| Incremental Investment | | | | | |
| Incremental Gain | | | | | |
| Incremental Net Return | | | | | |
| Incremental ROI | | | | | |

CyGlass