



The Financial Consequences of Risk Acceptance Security Strategies

CRITICALSTART 





Question:
**How much risk
should you accept?**

Answer:
None.

CRITICALSTART reduces endpoint risk to levels unachievable by traditional Managed Detection and Response (MDR) service providers and security tools alone. Our unique and leading-edge Trust-Oriented model is based on resolving every alert, the only way to reduce risk with confidence.

The volume and sophistication of new attacks, the cost of security tools, the shortage of security expertise and limited security budgets complicates risk management for today's security leaders. Managing risk has become an exercise in trade-offs and risk acceptance.

Threat actors target hosts and servers to disrupt business operations and exfiltrate sensitive data. This can have significant financial impact and even threaten the survival of many businesses. Security leaders need to reassess their security strategies and the MDR service providers they entrust their organization to. They need to evaluate the financial impact of security events and how to best apply their limited resources to reduce risk.

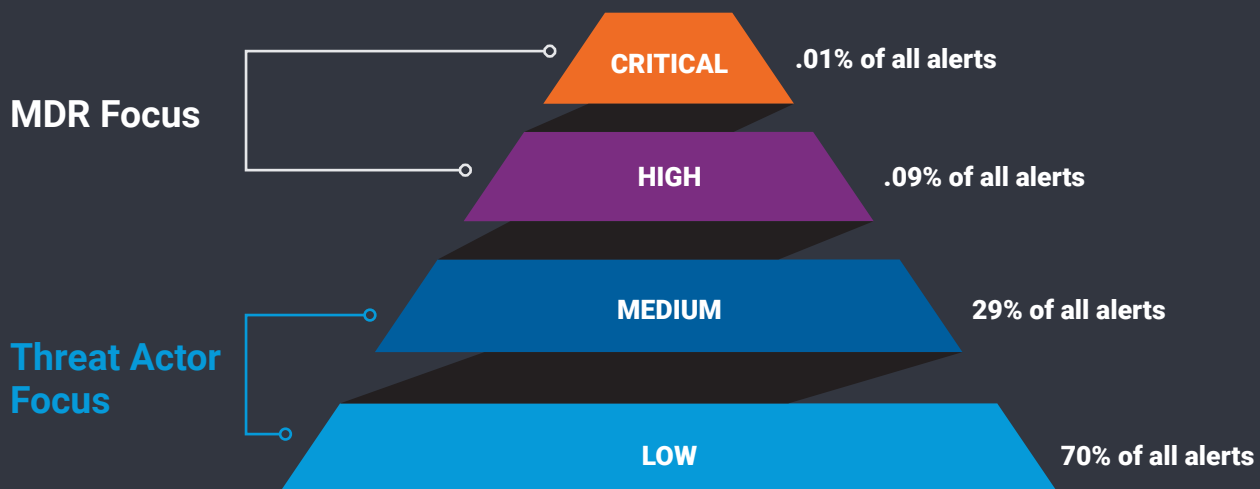


The Importance of Resolving Every Alert

Threat actors are relentless in their development of new attacks. They continuously analyze how in-house security teams use security tools and how to evade detection. Threat actors have learned that security teams focus on critical alerts and are good at responding to them. They have also learned that security teams lack the scalability to respond to medium and low priority alerts. As a result, they are developing attacks that hide in the noise of these lower priority alerts, knowing they will be ignored.

Figure 1



Over six months, CRITICALSTART observed that .01% of all alerts were identified as a Critical priority by security tools. High priority alerts accounted for .09%. Medium alerts made up 29%. Low priority comprised 70% of all alerts. (July 1, 2020 through December 31, 2020).





CRITICALSTART does not believe in any strategy that involves risk acceptance. Our unique and leading-edge Trust-Oriented model is based on resolving every alert – the only way to reduce risk with confidence.





Traditional MDR providers lack the scalability to investigate and resolve all alerts for all their clients.

CRITICALSTART believes that resolving every alert is the only way to reduce risk with confidence. We recognize that this creates a scalability nightmare for security teams. You need to “open the spigot” to collect all alerts from security tools, regardless of priority.

Over a six-month period, the CRITICALSTART Security Operations Center (SOC) recorded over 100,000 alerts per client per week. These alerts are ingested into ZTAP (Zero Trust Analytics Platform), our proprietary analytics and automation platform. Assuming an average of 10 minutes to investigate and resolve each alert, it would take an in-house security team 16,666 hours to resolve every alert.

$$16,666 \text{ hours} = \frac{10 \text{ minutes per alert}}{60 \text{ minutes per hour}} \times 100,000 \text{ alerts}$$

This would require 416 FTEs at a cost of over \$37.4 million. This is far beyond the budget and staffing ability of today's organizations.

$$\text{\$37.4M} = \frac{416 \text{ FTEs} \times \$90\text{K/analyst/year}}{16,666 \text{ hours} / 40 \text{ hours per week per analyst}}$$

Because of this, security leaders often turn to managed security service providers. However, scalability is an even bigger problem for them. Extending the calculations from above, for every 100 clients it would take a traditional MDR 1,666,000 hours and 41,600 FTEs to investigate and resolve every alert. Obviously, these numbers are far beyond achievable.



To solve the scalability problem, traditional MDR providers apply Alert Suppression, increasing risk acceptance on behalf of their clients.

Traditional MDR providers apply alert suppression to reduce the volume of alerts. Common practices include modifying detection policies, disabling inputs and changing alert thresholds. They also turn to ignoring lower priority alerts. There are several problems with this approach. First, security tools lack the business context to accurately assign priority. Second, it assumes that the most risk is associated with Critical and High priority alerts which is not supported by data. In fact, we are observing the opposite.

These tactics may prove effective in reducing alert fatigue and increasing scalability, but at a cost – risk acceptance. They introduce the risk of missing malicious activity and false negatives.

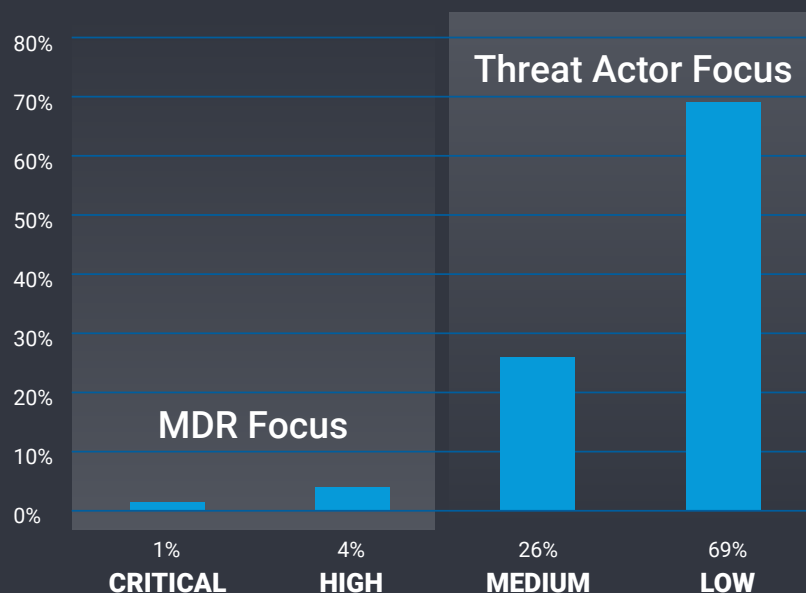
These providers are making decisions that force risk acceptance on their clients, often without client awareness or consent. They are essentially asking their clients to expose their environments to solve their scalability problem. Is this a trade-off you want to make?

Figure 2

CRITICALSTART

investigates all unknown alerts. We escalate the alerts that require action by the client. Over six months, 1% of all escalated alerts were identified as a Critical priority. High priority alerts accounted for 4%. Medium alerts made up 26%. Low priority comprised 69% of all alerts. (July 1, 2020 through December 31, 2020).

Escalated Alerts





The “noise” generated by security tools is not in lower priority alerts – **it’s in false positives.**

Alert suppression is applied to reduce the “Noise” generated by security tools and increase scalability. Providers generally conclude that the source of this noise are lower priority alerts. As Figure 2 highlights, filtering out Medium and Low priority alerts plays into the strategies and tactics used by threat actors, increasing the reliance on risk acceptance.

CRITICAL**START** believes that lower priority alerts are not “noise”. They are data. We have learned that the real “noise” comes from false positives. After opening the spigots to collect every alert, we consistently see 99% are false positives. Continuing our example above, 100,000 alerts/client less 99% false positives leaves 1,000 alerts to be investigated.

Resolving false positives delivers the scalability MDRs need without requiring their clients to accept risk.
But where do you find the scalability to investigate 99,000 false positives?

10 minutes/alert

60 minutes/hour X 1,000 alerts =

166 hours/40hours/week = 4 FTEs





CRITICALSTART automatically resolves false positives and escalates only the alerts that matter, safely and with scale.

Since our founding in 2012, CRITICALSTART recognized the need for an MDR service that denies risk acceptance. CRITICALSTART reduces risk to levels unachievable by traditional MDRs and security tools alone. Our unique and leading-edge Trust-Oriented model is based on resolving every alert, the only way to reduce risk with confidence.

CRITICALSTART MDR is driven by ZTAP, the Zero Trust Analytics Platform. ZTAP features the Trusted Behavior Registry (TBR), the largest registry of known good alerts (false positives). It delivers the scalability to resolve every alert.

Every alert ingested from security tools into ZTAP is matched against known good alerts in the TBR. If a match, the alert is automatically resolved. If no match, then the alert is investigated by the CRITICALSTART SOC. On average, we escalate 0.1% of all alerts to the client. ZTAP details what was observed, what is the risk and recommended actions, to the client for additional action.

Using the CRITICALSTART Trust-Oriented model - 0.1% of 100,000 alerts/client yields 100 escalated alerts/week.

10 minutes/alert

60 minutes/hour X 100 alerts =

16 hours/40 hours/week = <1 FTEs





Scalability problem solved – Zero risk accepted – Only with CRITICALSTART!

Economic models are effective tools for communicating the value of a security solution to the key stakeholders in your organization. The CRITICALSTART risk model calculates the value to place on risk acceptance.

Organizations are exposed to risk from data breaches. Risks include restitution, legal fees, fines and the cost of restoring reputation and trust. The latest Ponemon report estimate these risks add up to \$242 per record.¹

Organizations are also exposed to prolonged business stoppage from ransomware. Risks include lost revenue and productivity from prolonged downtime. According to Coveware, the average downtime from ransomware is 16.2 days.² Extend that to an organization doing \$2M in revenues per day (\$500M annual across 250 business days).

\$2,000,000 revenue/day X

16 days downtime =

\$36,000,000 revenue risk

By applying
the probability of
escalating an alert
shown in Figure 2, we
can calculate risk
acceptance for each
alert priority.

¹ Ponemon Institutes "Cost of a Data Breach 2019"

² Coveware Q4 Ransomware Marketplace Report 2019



Cost of Risk Acceptance

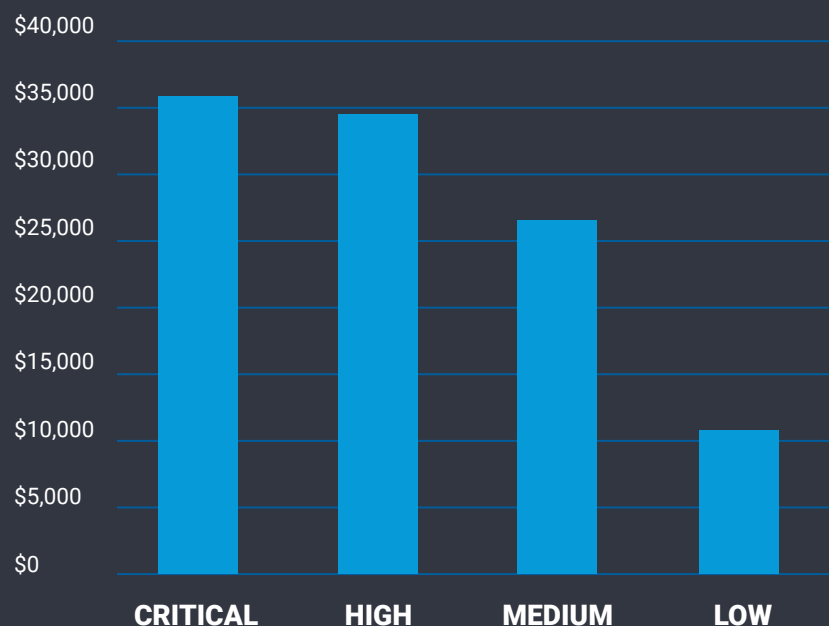


Figure 3

Risk acceptance can be monetized by alert priority. In our example of \$36 million in revenue risk, Critical alerts make up only 1% of total escalations. Resolving these alerts reduces only \$360,000 in risk, leaving \$35,640,000 in accepted risk. Resolving High priority alerts leaves \$34,560,000 in accepted risk. Resolving Medium priority alerts results in \$26,640,000 in accepted risk. Resolving Low priority alerts leaves \$11,160,000 in accepted risk. CRITICALSTART MDR resolves all alerts resulting in \$0 in risk acceptance. See below for calculations.

Critical priority alerts

$\$36,000,000 \times .01 \text{ escalations} = \$360,000 \text{ alerts resolved} = \$35,640,000 \text{ accepted risk}$

High priority alerts

$\$36,000,000 \times .04 \text{ escalations} = \$1,440,000 \text{ alerts resolved} = \$34,560,000 \text{ accepted risk}$

Medium priority alerts

$\$36,000,000 \times .26 \text{ escalations} = \$9,360,000 \text{ alerts resolved} = \$26,640,000 \text{ accepted risk}$

Low priority alerts

$\$36,000,000 \times .69 \text{ escalations} = \$24,840,000 \text{ alerts resolved} = \$11,160,000 \text{ accepted risk}$

CRITICALSTART = $\$36,000,000 \text{ alerts resolved} = \0 accepted risk



CRITICALSTART MDR

Delivers Unmatched Value

By resolving every alert and never engaging in alert suppression, CRITICALSTART reduces risk acceptance for our clients. We provide the only MDR service enabled by the ZTAP, the most sophisticated analytics and automation platform, and backed by a SOC team expert in the Trust-Oriented model.

Figure 4

By suppressing alerts to investigate and resolve Critical priority alerts, MDRs impose costly risk acceptance on their clients. CRITICALSTART, by leveraging the power of ZTAP, resolves every alert with scale and reduces risk acceptance. CRITICALSTART provides the only MDR service that delivers on this promise.



CRITICALSTART delivers the outcomes that security teams need in an MDR service provider. Our Trust-Oriented model based on resolving every alert:

- Reduces risk acceptance and delivers the most protection against security breaches.
- Reduces staffing requirements for hard-to-find Security Analysts.
- Eliminates alert fatigue, leading to greater job satisfaction and security team retention.
- Provides complete visibility to improve your security posture.

To see how we can reduce risk acceptance with confidence, contact us at criticalstart.com

