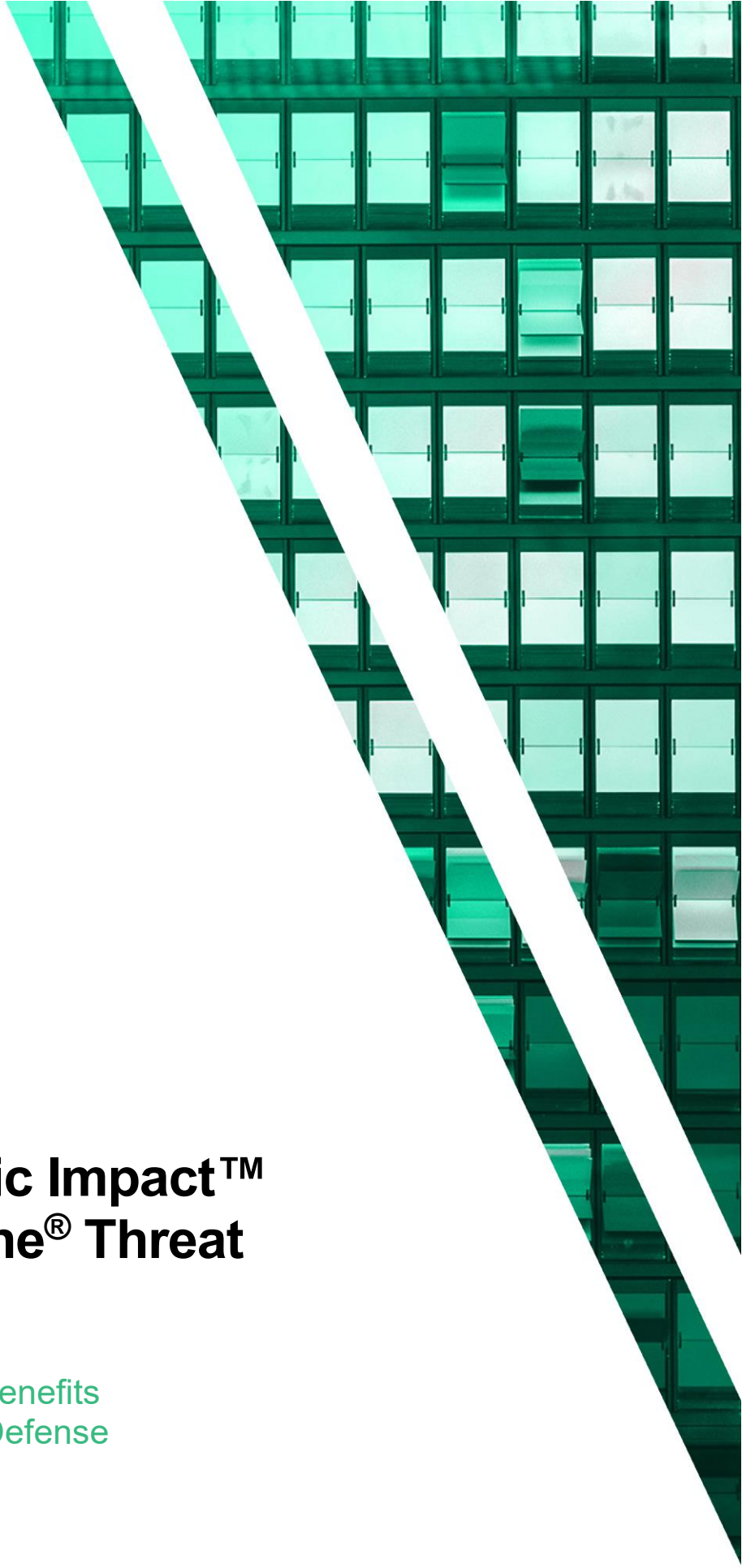
FORRESTER®



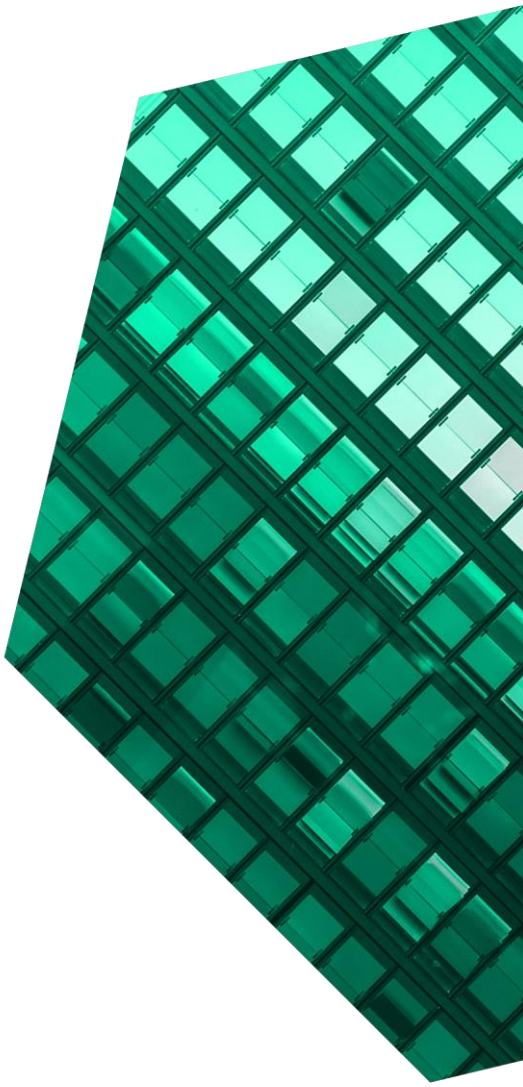
The Total Economic Impact™ Of Infoblox BloxOne® Threat Defense

Cost Savings And Business Benefits Enabled By BloxOne Threat Defense

FEBRUARY 2021

Table Of Contents

Consulting Team: Henry Huang
Luca Son



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

© 2021, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

Infoblox BloxOne Threat Defense is a DNS-based security tool that covers security blind spots left behind by next-generation firewalls (NGFWs) and endpoint detection and response (EDR) tools, while protecting the enterprise network and those working remotely regardless of device or location. BloxOne finds anomalies earlier in the threat life cycle and empowers organizations to detect and remediate with higher efficacy using automation and security orchestration and response while requiring fewer people resources.

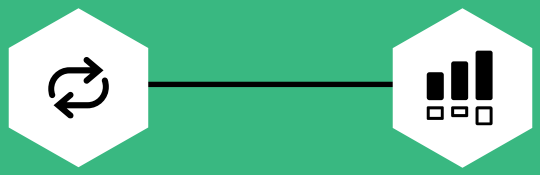
Infoblox commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying BloxOne Threat Defense. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of BloxOne Threat Defense on their organizations as an integral part of a comprehensive cybersecurity defense strategy.

Threat actors are becoming more complicated in attacks and corporate data is increasing in value. Organizations need to find ways to sharpen their defenses and plug gaps, especially in backdoors such as the DNS, which doesn't always have the best visibility or inspection given the shortcomings of traditional measures and the majority of traffic being assumed as standard internet traffic. Use of the DNS layer as a malware communication and data theft channel is increasingly common and difficult to protect against.

Making the situation worse, cybersecurity teams at organizations are shorthanded and difficult to hire for. DNS security such as BloxOne Threat Defense complements traditional security solutions and effectively works to ease the detection, response, and remediation steps which are crucial for organizations to maintain a positive security posture today.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with experience using BloxOne Threat Defense. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

KEY STATISTICS



Return on investment (ROI)
243%

Net present value (NPV)
$669K

Prior to using BloxOne Threat Defense, the customers had a wide range of security tools, ranging from NGFWs and intrusion prevention system (IPS) devices to advanced EDR solutions. However, even with this bevy of tools and capabilities to protect against malicious activity, customers were missing out on key benefits a DNS security solution could provide: the detection, blocking, and addressal of

Security operations using BloxOne reduce total effort by:

34%

> **Blocking at the DNS level is what I call protocol-agnostic — whether it's a TCP connection or UDP connection. If it uses DNS, you have the capability of blocking it. So, while there's a lot of layers in our security tools, most are protocol specific or attack method specific. Infoblox is more. It becomes a pivotal place where you can block things.**
>
> – Director of security operations, insurance organization

frontline threats, which are undetectable by the remainder of the security stack. Trying to block data exfiltration via DNS tunneling was a near impossibility. Other matters such as the automatic blocking of malicious domains were also lacking, leading ultimately to a reduction in business user productivity. Most importantly, however, the costly loss of data took top priority as it wasn't entirely addressable, even with modern data loss prevention (DLP) methods.

Following the investment in BloxOne Threat Defense, customers gained peace of mind above all else on intrusions and potential data loss. This was done because DNS security provided a first line of defense which minimized data loss before all other security solutions. The risk of newsworthy data loss incidents was also significantly reduced due to DNS channels now being monitored. Additively, the entire process of security monitoring and resolution became easier, with key insights being drawn from BloxOne Threat Defense so that the entire security stack and its operators had the crucial information to eliminate the issues at hand.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Security operations (SecOps) gain 19% of their time back using contextualized BloxOne Threat Defense intelligence on investigations.** BloxOne Threat Defense provides critical telemetry to threats by acting as the first line of defense for organizations. With each attack, the what, when, and why of each threat is presented with deep insight so that SecOps can deterministically neutralize the threat, if it is not neutralized already. Less investigative time is spent drilling down on logs, and triage work is parsed down significantly. In addition, false alerts are now reduced due to additive information being provided by the Infoblox set of tools. In all, SecOps at the composite organization is able to realize a PV savings of $292,786 in effort over three years.

- **Reduced risk of material breach by 5% or the equivalent of $456,753 PV.** With the cost of a material security breach reaching over $1 million per incident, and with the number of incidents likely to occur per year up to five times, security tool stacks need to work in conjunction to prevent threat infiltration and threat proliferation in and out of the network. Infoblox provides a layer that blocks malicious activity from moving critical data in and out of the network in situations like data exfiltration through DNS, which existing tools cannot effectively detect. BloxOne Threat Defense plays a vital role in the security stack by plugging security holes and pathways, through which certain malicious software operate. Over a three-year period, a PV savings of $456,753 is achieved.

Reduce the risk of material breaches potentially costing:

$457K

- **End-user productivity loss is reduced on small scale infections and incidents by 1,897 hours per year.** In using BloxOne Threat Defense, end-user productivity is maintained through a higher rate of malicious domain blocking, which is normally not filtered through typical EDR platforms. Forrester estimates that in workforce situations involving both on-site (50%) and remote workers (50%), business end users save an average of 6 hours per incident. EDR solutions can block as much as 98.6% of threats, but DNS security like BloxOne complements EDRs to detect an even greater percentage of threats. The avoidance of user productivity loss due to malicious threats is $194,726 PV.

Unquantified benefits. Benefits that are not quantified for this study include:

- **Decreased load on existing security tools and infrastructure.** As a first line of defense, BloxOne Threat Defense will filter out a majority of events and threats before they reach network security devices, reducing the computational and bandwidth load that these devices normally need to filter through.
- **Improved endpoint performance by being agentless.** Eliminating the need for endpoint agents reduces parasitic overhead. Business end users experience fewer alerts and events, and they thus benefit from snappier performance. Virtual environments also benefit from the elimination of the need to provision additional agents.

Costs. Risk-adjusted PV costs include:

- **Licensing and implementation costs.** The cost of implementation and licensing is straightforward, with three levels of capability. Implementation guidance and services are virtually delivered and activated by Infoblox technicians. With integration and optimization taken into account, the total PV cost of bringing Infoblox into the security portfolio is $274,888 for a three-year analysis period.

The customer interviews and financial analysis found that a composite organization experiences benefits of $944K over three years versus costs of $275K, adding up to a net present value (NPV) of $669K and an ROI of 243%.

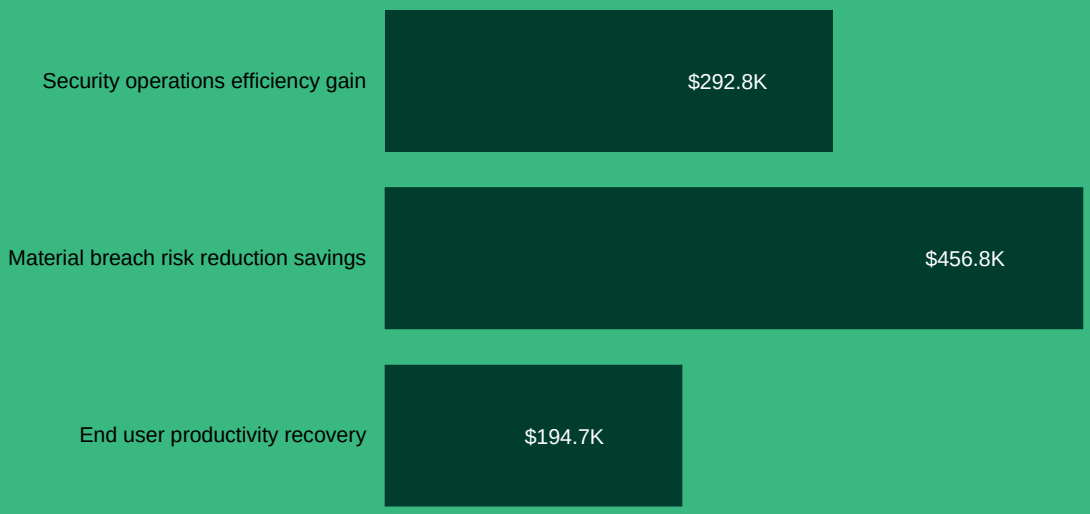
ROI
243%

BENEFITS PV
$944K

NPV
$669K

PAYBACK
<6 months

Benefits (Three-Year)



Security operations gain 34% efficiency through decreased alerts, better context behind alerts, and automation.

The likelihood of material risk reductions is reduced with the added layers of defense from BloxOne Threat Defense by +5%.

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in BloxOne Threat Defense.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that BloxOne Threat Defense can have on an organization.

DUE DILIGENCE

Interviewed Infoblox stakeholders and Forrester analysts to gather data relative to BloxOne Threat Defense.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using BloxOne Threat Defense to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewed organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Infoblox and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in BloxOne Threat Defense.

Infoblox reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Infoblox provided the customer names for the interviews but did not participate in the interviews.

The Infoblox BloxOne Threat Defense Customer Journey

Drivers leading to the BloxOne Threat Defense investment

Interviewed Organizations

Industry	Region	Interviewee	Organization size
Life sciences	US HQ, Global	Head of IT	3,500 FTEs
Insurance	Global	Director of security operations	11,700 FTEs
Life sciences	Americas	Network engineer	500 FTEs
Insurance	Americas	• Senior security engineer • Cyber security engineer	450 FTEs

KEY CHALLENGES

Security has always been top of mind for the interviewees in this study, and it was of even greater concern prior to their investment in BloxOne Threat Defense. Prior security solutions lacked scalability that was independent of significant human labor. This was especially true for customers that were seeking additive security in the wake of the COVID-19 pandemic, where work-from-home situations meant that adding more traditional security tools would only be marginally more effective. As interviewed customers considered an investment in Infoblox BloxOne Threat Defense, Forrester noted the following common challenges:

- **Consistently shorthanded with security operations personnel.** As security has become a more prominent concern for organizations, the talent required to keep up with the level of protection has not been progressing in sync with the experience levels of security practitioners. The interviewed organizations were forced to invest in either process or technology as the people element was simply unavailable.
- **Overreliance on endpoint and network security segments.** Traditional measures of security, focusing on both network security and endpoints, are the workhorses of the

"The problem that we had was with the lack of visibility. Infoblox gave us that discoverability on what was going in and out of the network. In fact, we had very little idea where the networks sat and trying to pinpoint things was an all-manual process trying to figure it out."

Network engineer, life sciences

"Using a free model of DNS and threat intel [that comes with the server OS] really isn't enough, because it doesn't thread all the data together. Having to build the methodology to bring the information together to generate logs, reports, and alerts was just a lot of work. Infoblox brings it all together as a singular networking fabric. With this approach, our monitoring, detection, and response schema with their enriched data is much simpler."

Director of security operations, convenience chain

cybersecurity segment. But what else is there? While defenses such as NGFWs have advanced to read at the application layer, along with EDR solutions filtering a lot of the traffic, the question of malware that uses DNS as a command-and-control channel — that is typically undetected by all other security measures — remains. Data exfiltration and data loss prevention were top of mind for many of the customers that could not regulate via their traditional security stack.

- **Aggregation of usable contextual security information.** Triages and investigational work were only as good as: 1) the people and their experience in working with exploits and 2) the amount of usable information that security tools gave. Often this came in the form of logs that required deep investigations, but these organizations sought something better, perhaps in the form of usable insights rather than terabytes of unstructured data.

"Our objective with Infoblox was about making sure that the network is resilient, making sure that we have very good visibility at all times so we can quickly diagnose and triage issues and be scalable. As we have growing environments and increasingly complex networks, their solution supports all our efforts to make growth of the business easier."

Director of security operations, insurance

SOLUTION REQUIREMENTS AND OBJECTIVES

The interviewed organizations searched for a solution that could:

- **Improve security without overextending existing security FTEs.** The interviewed customers share a common question, "How do we improve our defenses without having to hire more people." Yes, added sensors and logs would provide greater visibility, but at a cost that surpassed the budget allowance on people and technology.
- **Enable defenses at a layer sooner in the threat defense cycle.** Organizations felt that while there were security defenses at the network layer internally, the DNS layer was greatly deficient in blocking malicious domains and data exfiltration.

  Relayed by the senior security engineer of an insurance company: "The first requirement we had is how to protect against the data [exfiltration] from our organization and how it runs through our DNS. Our second requirement was how to get a good threat feed so that we can be on top off new domains, or uncategorized domains of high-level threat domains, and secure that at the beginning of the entire threat journey."
- **Scale security without purchasing additional physical infrastructure.** Due to the growth that the organization expects in the ensuing years, the composite organization would like to: 1) find a solution that can easily scale without extraneous physical deployments while workloads increased and 2) consolidate as much as possible on the specific segments of network security so that everything is on a single pane of glass.

Shortly after a RFP and business case process evaluates multiple vendors, the interviewed organizations chose BloxOne Threat Defense and began their deployment. Being that the Infoblox solution was largely a cloud-deployed solution, the

implementation period was rather fast, with it taking less than three months.

> **"A lot of our security was [on-premises]. We then found exploitation at the DNS security level, and it changed our mindset on where to focus to, 'Okay, let's take the security at the DNS layer, where the infiltration starts, instead of letting it make its way to layer 3, the network layer.' We can mitigate or control from the initial stage of where it all starts from. So, that's a way we change our mindset."**
>
> *Senior network engineer, insurance*

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a global financial services and insurance (FSI) organization that is held to both financial- and privacy-based regulations such as SOX, PCI-DSS, and GDPR in the geographies they operate in.[1] Hence, it requires the highest of security standards for continued operations. Cybersecurity continues to be a pain point for the composite organization as evidenced by the number of major material breaches across the globe in the past year — especially with the SolarWinds breach fresh on everyone's minds. With many breaches now going subsurface to avoid standard defense measures, the composite organization sought out DNS protection to upright defenses throughout.

The composite organization's current team of less than 10 security operations personnel distributes its members in the fields of incident response (IR), code/policy rebuild, and threat hunting. With three FTEs dedicated to IR, the task is daunting given the number of alerts that are delivered. Increasing this base of personnel is largely difficult due to the extreme demand for qualified security professionals. Additionally, the societal shift to hybrid in-office and work-from-home models means that security issues need to be addressable from security tools that aren't connected to the network.

Deployment characteristics. Following a rapid proof-of-concept, the composite organization realized that adding a dedicated defense layer at the DNS level provides benefits to security professionals, existing security infrastructure, and end users. The rollout of the Infoblox BloxOne Threat Defense solution took place quickly across the composite organization's entire landscape, and it was aided by quick and consistent policy distribution at the cloud level.

Key assumptions

- **Financial services organization**
- **5,000+ FTEs with multiple locations**
- **50:50 remote to in-office workers**
- **Lean cybersecurity staff of five FTEs**
- **Leveraging existing cybersecurity defenses like NGFWs, EDR tools, and threat intelligence**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Security operations efficiency gain	$117,734	$117,734	$117,734	$353,201	$292,786
Btr	Material breach risk reduction savings	$178,600	$183,958	$189,478	$552,036	$456,753
Ctr	End-user productivity recovery	$73,984	$78,503	$83,308	$235,794	$194,726
	Total benefits (risk-adjusted)	$370,317	$380,519	$390,480	$1,141,031	$944,265

Benefits Detailed By Category

SECURITY OPERATIONS EFFICIENCY GAIN

Evidence and data. Alerts, alerts, and more alerts was the bane of security analysts at organizations that Forrester interviewed. Larger firms were getting thousands of alerts per day, and the whole process of performing a holistic investigation, which included digesting logs, was time-consuming. Using BloxOne Threat Defense, security professionals observed:

- A 10% to 25% reduction in security false alerts, meaning that these were eliminated altogether.
- Due to the increased context being collected at the DNS level, true alerts were complemented with additive information for security professionals to pursue in their investigative work. Forrester noted a 7% to 25% change depending on organization's existing maturity.
- With Infoblox, the interviewed organizations built a more comprehensive and holistic view of threats across all security infrastructures and services; all of the collected intel was consolidated into their security information and event management (SIEM) teams. Rather than looking through logs and piecemealing information together from various logs, security analysts were able to find advanced telemetry behind attacks and resolve issues faster before damage proliferated through the network. With a greater level of certainty, security orchestration and response (SOAR) was leveraged more to provide time savings to the security professionals.

> **"I think it's one of those tools that's — because of the ease of deployment and for a leaner team like ours — I think it's a no brainer, and even for larger companies it's still true. It's easy to deploy, and it doesn't have a lot of [training] — some of the security solutions as you know, require a lot of training."**
>
> *Head of IT, life sciences*

- Overall, the gain in security efficiency resulted from a combination of two factors: fewer false alerts and increased fidelity to landed threats.

Reduce SecOps effort on incidents by **34%** with Infoblox.

Modeling and assumptions. For the composite organization that Forrester has formed, the following have been factored into the results:

- The metrics used within this and other benefit calculations are based on current and short-term future projections of organizations' current work-from-home models, which involve workforces being split between in-office work (50%) and remote work (50%). Forrester's analysis found that increased remote work exposes new threat surfaces and exploitation vectors. Firms should adjust accordingly based upon their organizational situations.
- False alerts are reduced by 15%, eliminating the loss of time and effort.
- DNS level context brings an additive level of information to investigations, and it shortens the investigation and triage portions by 19%.
- Security personnel responsible for IR should be scaled to the reader's organization, but they should note that the benefits diminish once a large labor force is applied.

Risks. Potential risks can negatively impact benefit categories. Specifically, organizations may realize the following risks:

- Threat intelligence coming in from other sources, that include DNS information, may reduce the incremental improvement that Infoblox threat intelligence can provide to security professionals.
- The use of managed security service providers (MSSPs) can directly replace in-house security professionals, which may alter the overall benefit.

"We've been running BloxOne for quite some time. When we did our validation through continuous attack simulations, the catch rate on the domains was high — above 70%, which is pretty impressive. Adding Infoblox roughly doubled how much we were blocking."

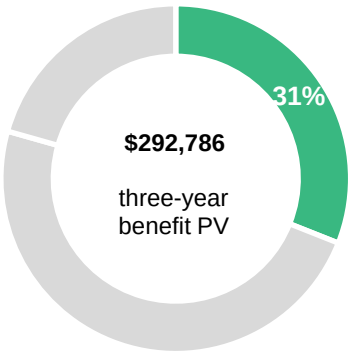
Director of SecOps, insurance

Additionally, MSSPs may provide tools and insights that are similar to that provided by BloxOne Threat Defense.

- Assuming that the use of managed services is minimal, Forrester estimates the benefit to have a small degree of variance.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $292,786.

Security Operations Efficiency Gains



Security Operations Efficiency Gain					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
A1	Reduction in threat alerts and false alerts due to BloxOne Threat Defense	Interviews	15%	15%	15%
A2	SecOps effort reduction due to improved contextual threat information	Interviews	19%	19%	19%
A3	SecOps FTE dedicated to incident and threat response	Composite	3	3	3
A4	SecOps FTE annual compensation, fully loaded	$90K*1.35X modifier	$121,500	$121,500	$121,500
At	Security operations efficiency gain	(A1+A2)*A3*A4	$123,930	$123,930	$123,930
	Risk adjustment	↓5%			
Atr	Security operations efficiency gain (risk-adjusted)		$117,734	$117,734	$117,734
	Three-year total: $353,201			**Three-year present value: $292,786**	

MATERIAL BREACH RISK REDUCTION SAVINGS

Evidence and data. Infoblox's specialization at the DNS level stops breaches before they cause material damage. Forrester noted the following from their customers:

- Material breaches were a real consideration for the interviewed organizations. One organization suggested that while they knew of several material breaches in previous years, there could be more that were still unidentified. They stated that any solution which didn't require heavy lifting from internal resources and or high overhead was at the top of their list — with Infoblox being one of the key pieces.
- Data exfiltration was a large concern for many organizations. BloxOne Threat Defense is able to stop malicious traffic before it leaves the organization using user behavior analysis and DNS intelligence. This allows organizations to wrest control of that data before any material breaches can manifest.
- For a senior security engineer at an insurance organization, "Between the [automatic] feeds, the customer block lists, and the ability to detect data [exfiltration] at a deeper level, I sleep a bit easier at night knowing that we have a tool in place that will provide that coverage."

Infoblox's DNS threat intel **produces an additional protection layer to reduce the likelihood of a material breach,** even with a comprehensive security stack already in place.

Modeling and assumptions. For the composite organization, Forrester assumes that:

- Breaches will happen, and they will sometimes go unnoticed. Forrester defines a breach as an incident resulting in the loss or compromise of data, accompanied by material remediation costs. The data represented here is based upon the breach activity of an insurance organization, or what Forrester categorizes as an FSI organization. According to Forrester's 2020 "Cost Of A Security Breach" survey, FSI organizations were likely to see five material breaches per year.[2]

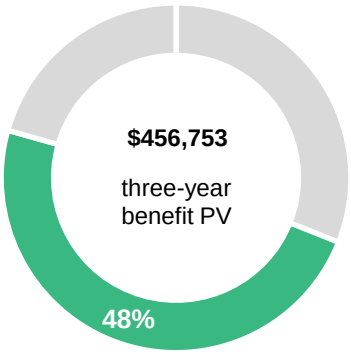
- Further findings from Forrester's "Cost Of A Security Breach" survey indicate that the number of breach occurrences were only slightly affected by the company size or revenue, but the cost of recovery from a breach was highly correlated to the size and revenue of organizations.
- For the composite organization, the average cost is $815,000 per material breach. With the cost of lost business user productivity, the cost per breach surpasses $1M.
- Using Infoblox BloxOne Threat Defense and taking into account that defenses such as NGFW, EDR, and cloud access security broker (CASB) products are already in place, the overall reduction in the likelihood of a breach is an additive 5% beyond all other solutions in place.

Risks. Risks that can impact the realization of this benefit include:

- The importance of the data at the composite organization, relative to other financial institutions, can materially affect the cost of a breach.
- The severity of breaches (such as east-west proliferation or critical application services) can affect internal business users.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $456,753.

Material Breach Risk Reduction Savings



Material Breach Risk Reduction Savings					
Ref.	**Metric**	**Calculation**	**Year 1**	**Year 2**	**Year 3**
B1	Average number of data breaches per year	Forrester data, FSI	5.0	5.0	5.0
B2	Average potential cost of data breach ($163/employee, FSI), excluding internal user downtime	Forrester data, FSI	$815,000	$839,450	$864,634
B3	Reduced likelihood of a breach		5%	5%	5%
B4	Avoided costs of remediation, customer resolution, fines, brand rebuild, and all other external-facing costs	B1*B2*B3	$203,750	$209,863	$216,159
B5	Number of internal business users	Composite	5,000	5,150	5,305
B6	Average salary - business user (hourly)	$60K*1.35X benefits modifier/2,080 hours	$39	$39	$39
B7	Diminished/eliminated internal user productivity hours per breach	Forrester data, FSI	4.0	4.0	4.0
B8	Average percentage of employees affected per breach	Assumption	10%	10%	10%
B9	Cost of reduced internal productivity	B1*B3*B5*B6*B7*B8	$19,500	$20,085	$20,688
Bt	Material breach risk reduction savings	B4+B9	$223,250	$229,948	$236,847
	Risk adjustment	↓20%			
Btr	Material breach risk reduction savings (risk-adjusted)		$178,600	$183,958	$189,478
	Three-year total: $552,036			**Three-year present value: $456,753**	

END-USER PRODUCTIVITY RECOVERY

Evidence and data. The additional layer of security from Infoblox reduces the need for end-user investigation and remediation because of the improved removal of malware and DNS-based threats.

- Before deploying Infoblox, interviewees' organizations landed regularly on malicious domains, which was mostly unintentional. However, this is the exact behavior that bad actors seek to exploit. The theme for the interviewed organizations was to prevent early and prevent often.

  According to one interviewee: "We look at Infoblox as something that is a heavy blocker of malicious requests. The number of blocked connections for us is in the millions per day."

- With Infoblox working in conjunction with EDR tools, BloxOne Threat Defense blocks an additional 47% beyond what traditional EDR tools will pick up, especially activity at the DNS level.
- While the blocking rate of Infoblox was above 70% in many instances, some of these instances were also blocked by EDR solutions, resulting in what interviewees characterized as additive incident prevention.
- Previous incidents required as much as 4 hours of time used by all parties on incidents. For work-from-home individuals, the time was even higher due to the required shipping of systems.

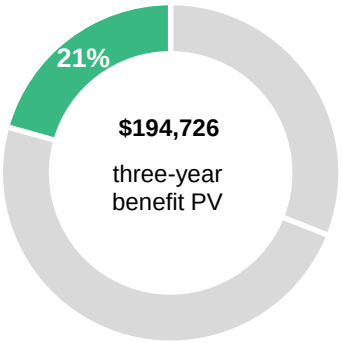
Modeling and assumptions. For the composite organization, Forrester assumes that:

- End users are impacted traditionally by 1.4% of the threats that become incidents. The added layer of security from BloxOne Threat Defense brings down incidents by another 47%.
- The average fully burdened salary for end users is $81,000 per year or $39 per hour.
- End users are impacted differently, depending on whether they work in the office or from home. For instance, employees that work from home may require the shipment of a loaner laptop, whereas if that employee were on-site the loaner would be readily available.
- The modeling is done with the consideration that an organization's workforce is split between employees working in the office versus those that are working from home.
- Total loss of productivity is expressed in dollars per hour multiplied by the hours of productivity lost due to security incidents requiring attention.

Forrester found a three-year, risk-adjusted total PV of $194,726.

Reduce security related endpoint downtime by **47%** with Infoblox.

End-User Productivity Recovery



End-User Productivity Recovery

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Business end users	Composite	5,000	5,150	5,305
C2	Endpoint time-to-remediation after landing on malicious domains, in hours		6.0	6.0	6.0
C3	Incidents landed per year, per user	Forrester data	9.61	9.90	10.20
C4	Likelihood of failure to contain by EDR solution, DNS-specific attacks not picked up by EDR	Forrester data	1.4%	1.4%	1.4%
C5	BloxOne Threat Defense blocking of domains effective rate	Customer interviews	47%	47%	47%
C6	Business end-user hourly compensation	$60K*1.35X benefits modifier/ 2,080 hours	$39	$39	$39
Ct	End-user productivity recovery	C1*C2*C3*C4* C5*C6	$73,984	$78,503	$83,308
	Risk adjustment	0%			
Ctr	End-user productivity recovery (risk-adjusted)		$73,984	$78,503	$83,308
	Three-year total: $235,764			**Three-year present value: $194,726**	

UNQUANTIFIED BENEFITS

One additional benefit that customers experienced but were not able to quantify includes:

- **Prolonging or increasing the utilization of the existing security infrastructure.** As Infoblox stops threats earlier in the threat life cycle, less threats, alerts, and ultimately incidents surface on user endpoints. While this is difficult to calculate, due to organizations having different retirement or update cycles on physical equipment, it has a positive effect that will drive down costs and decrease bandwidth throughput due to not overutilizing infrastructure that is already overloaded.

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement BloxOne Threat Defense and later realize additional uses and business opportunities, including:

- **Stop threats early in development environments and shift-left on the software development life cycle.** When software developers create workloads and services, they are able to interactively experience where domains would be blocked from the DNS protection, thus eliminating these as points of entry further down the road in the software development life cycle (SDLC). Rework and investigation work is avoided altogether.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	BloxOne Threat Defense licensing and implementation costs	$56,709	$85,313	$87,872	$90,508	$320,402	$274,888
	Total costs (risk-adjusted)	$56,709	$85,313	$87,872	$90,508	$320,402	$274,888

BLOXONE THREAT DEFENSE LICENSING AND IMPLEMENTATION COSTS

Evidence and data. BloxOne Threat Defense is a subscription service that operates largely in the cloud. As such, costs are based on the number of users at the organization and carry very little capital expenditure.

- Customers of Infoblox indicated a quick implementation, even with some locations that had a hybrid cloud architecture.
- For organizations that had significantly more remote locations, the cost did not vary significantly as policies and controls could be set centrally and applied once across the cloud devices from Infoblox.
- Internal testing and optimization to reach a steady state was already relatively easy. Whitelists and blacklists were not much of a concern for the customers.
- Integration by the customer organizations was mostly done through provided APIs, and it took less than a month to be operational.
- Given this, Forrester combined the internal costs as well as the costs borne from the Infoblox licenses, resulting in a PV cost for three years of $261,798.

Risks. Risks that may be of consideration for potential customers of Infoblox include:

- The number of security tool integrations. While Infoblox connects easily with most major solutions, homegrown solutions may take a different path.
- Organizations in specific verticals may need more time for a proper setting of steady state due to the variation in domains that they interface with.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $274,888.

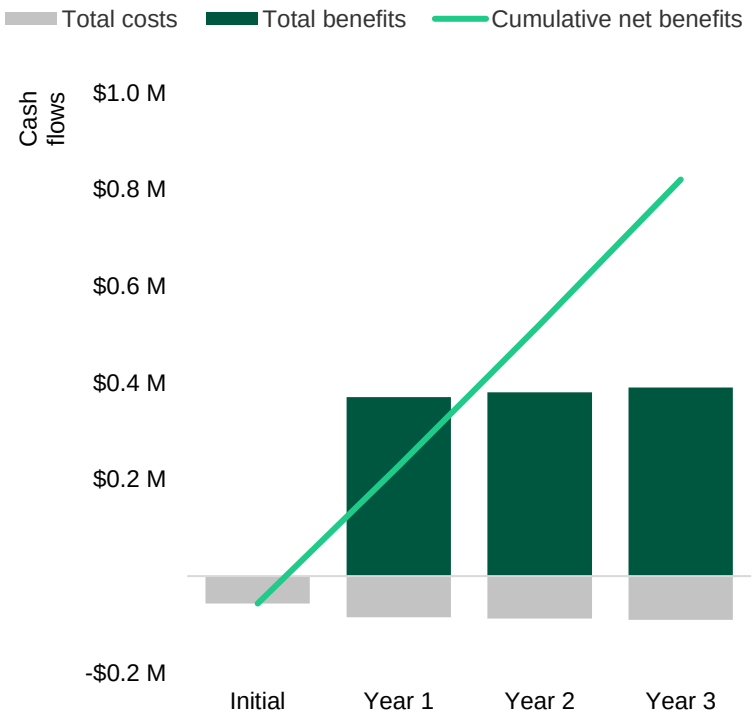
Costs of Infoblox licensing account for **under one-third** of total costs.

BloxOne Threat Defense Licensing And Implementation Costs						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Total users			5,000	5,150	5,305
D2	BloxOne Threat Defense cost per user			$16.25	$16.25	$16.25
D3	Professional services - Quick Start		$2,595			
D4	Cost of one internal SecOps FTE, per week	$121.5K annual salary/52 weeks	$2,337	$2,337	$2,337	$2,337
D5	Internal testing, configuration, and policy optimization effort costs	6 weeks, 1 FTE's effort	$14,022			
D6	Integration with third-party security tools effort costs	8 weeks, 2 FTEs' effort	$37,392			
Dt	BloxOne Threat Defense licensing and implementation costs	(D1*D2)+D3+D5 D6	$54,009	$81,250	$83,688	$86,198
	Risk adjustment	↑5%				
Dtr	BloxOne Threat Defense licensing and implementation costs (risk-adjusted)		$56,709	$85,313	$87,872	$90,508
	Three-year total: $320,402			**Three-year present value: $274,888**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($56,709)	($85,313)	($87,872)	($90,508)	($320,402)	($274,888)
Total benefits	$0	$370,317	$380,195	$390,519	$1,141,031	$944,265
Net benefits	($56,709)	$285,001	$292,306	$299,969	$820,567	$669,329
ROI						243%
Payback period						<6 months

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[1] SOX: Sarbanes-Oxley Act; PCI-DSS: Payment Card Industry Data Security Standard; GDRP: General Data Protection Regulation.
[2] Source: “Cost Of A Security Breach,” Internal Forrester Survey Data, November 2020.


FORRESTER®