IDC
ANALYZE THE FUTURE

Sponsored by: **iboss**

Authors:
Frank Dickson
Matthew Marden

January 2020

The Business Value of iboss cloud Enterprise Security Solutions

Business Value Highlights

275%
three-year ROI

37%
lower three-year cost of operations

4 months
to breakeven

51%
more encrypted traffic inspected

38%
lower risk of impactful security events

3.5
productive hours gained per user per year

16
appliances retired/avoided per interviewed organization

35%
more efficient IT security teams

EXECUTIVE SUMMARY

Traditional business and IT operations are being disrupted as digital transformation (DX) has produced more than cosmetic effects on enterprise networks. The future of cybersecurity is coalescing around four central control points as security is increasingly needed to conform to where work is being done, and on-premises, perimeter-centric security measures are becoming ever more permeable. The implication presented by new cybersecurity control points is not just where security is applied but also how security is applied. Simply extending on-premises security tools to a digitally transformed, location-agnostic constituency creates problems. To address the web security and user experience needs of digitally transforming organizations, iboss architected its iboss cloud solution in the cloud and for the cloud by minimizing latencies and the subsequent costs correlating with latency.

IDC spoke with organizations about their experiences of using iboss cloud enterprise security solutions (iboss cloud). Interviewed iboss customers reported that they have gained crucial ability to inspect and secure network traffic that has enabled them to significantly reduce business and operational risks. They also linked the use of iboss cloud to establishing a more cost-effective security environment by optimizing their use of hardware appliances and bandwidth. In total, IDC quantifies the value that interviewed organizations will achieve at an annual average of $1.18 million per organization ($89,100 per 1,000 devices) by:

- **Improving employee productivity levels** by reducing latency and delivering more bandwidth, leading to improved application performance, especially for mobile users
- **Generating efficiencies for security teams** by providing visibility into and actionable detail on network traffic, allowing IT teams responsible for security to react more efficiently and effectively to threats
- **Lowering security-related costs** by avoiding the need for hardware appliances, reducing bandwidth consumption for backhauling network traffic, and retiring less cost-effective security solutions

IDC
ANALYZE THE FUTURE

More importantly, study participants spoke about substantially improving their security postures with iboss cloud because they can more readily inspect network traffic and take steps to address malware and other potential threats. While these benefits are often challenging to quantify financially, interviewed iboss customers reported reducing risk associated with impactful security breaches, regulatory noncompliance, and revenue-impacting security events. Thus they not only avoided potential significant revenue losses, fines, and employee-impacting outages but also limited the likelihood of the occurrence of reputation-damaging events.

SITUATION OVERVIEW

Over 80% of organizations are undergoing a digital transformation, and traditional business and IT operations are disrupted as a result. Digital transformation has produced more than cosmetic effects on enterprise networks. DX has driven these networks to become highly heterogeneous, incorporating elements of mobile, Internet of Things, public/hybrid clouds, and SaaS applications with internal and remote access by employees and a burgeoning assortment of third parties from an equal assortment of devices, points of origination, and circumstances.

Enterprises need to rethink cybersecurity and digital trust measures overall at a time when ongoing digital transformation initiatives have helped businesses rapidly create new products and services. Many point to a looming "trust crisis" that threatens to disrupt the pace of innovation.

IDC believes that digital trust will drive the success of digital transformation, and thus enterprise security strategies must adapt to the needs of DX. The DX platform initiatives progressively rely on the integrity and resiliency of interconnected systems and a secure pipeline to enable sensitive data streams that enrich business intelligence (BI) systems and advanced analytics repositories. Digital transformation also requires enterprise security teams and application owners to incorporate business partner risk management capabilities to gain a greater awareness of business partner and supplier risks and shared responsibilities.

DX realities have changed cybersecurity as the future is coalescing around four central control points as security is increasingly needed to conform to where work is being done and on-premises, perimeter-centric security measures become ever more permeable. The four central control points are:

- **Identities.** Digital transformation means a higher level of connectivity between applications and business processes with the aim of improving business agility and connecting more readily with customers and business partners. It is expected that users have 24 x 7 uninterrupted experiences. Digital transformation can come in many forms. Things that were once not connected are now connected, and services now operate as one big machine. The goal is to integrate trust into the "machine." In such a context, identity becomes the new perimeter.

- **Applications.** As applications are more and more disassociated from specifically defined servers, networks, and infrastructure, network-centric security measures are increasingly becoming ineffective; the only way to compensate is to apply security at the application. For security applications, Layer 7 is the new Layer 3.

- **Data.** Data is the fuel of the DX machine; data is also the bounty of choice for cybercriminals everywhere. Protecting access is a perpetual game of cat and mouse. Security measures that travel with the data can dramatically improve the integrity of the DX activity. Being critical for many BI initiatives, at the moment, data can no longer be inadvertently neutered by encryption, so prioritizing protection while retaining sufficient usability is the new paradigm of enterprise defense. This could change in the near future as homomorphic encryption and multiparty computation cryptography are becoming viable. Homomorphic encryption enables data scientists to operate on encrypted data, and some organizations are currently testing it.

- **Endpoints.** A dark internet will require presence at key termination points. Detecting the malicious has to happen at the termination points, where the data is unencrypted. In addition, endpoints are the source of most productive activity and also the most common first stop in an attack. Endpoints provide key telemetry data for analysis and detection.

The Implication of the Four New Control Points

The emergence of four new control points means that enterprises must now be concerned with both where and how security is applied. Extending on-premises security tools to a digitally transformed, location-agnostic constituency creates problems as backhauling security services from the "home office" suffocates the user experience with latency.

At AWS re:Invent 2019, AWS introduced two new features, Wavelength and Local Zones. AWS Local Zones are a new type of AWS infrastructure deployment that places compute, storage, database, and other select services closer to large populations, industry, and IT centers. AWS Local Zones are designed to enable enterprises to deliver applications that require single-

digit millisecond latency to end users. AWS Wavelength is a service that enables enterprises to deliver ultralow latency applications for 5G devices. As hyperscale cloud providers look to deliver digital service with latency measured in single-digit milliseconds, no tolerance exists for applying security with latency taxes measured in the hundreds of milliseconds.

Implementing on-premises security in the reality of a digitally transformed world with four new control points has implications on both the user experience and costs. Everyone appreciates the hard costs that are paid directly to a security vendor; those costs are transparent. The "soft costs" (which may be better termed as less transparent) are "the killers"; exposing these costs makes one realize that there is nothing "soft" about them.

Latency certainly kills the user experience, but increases in costs correlate with increases in latency. Essentially, one of the drivers of increased latency is "time on the wire." Transport and backhaul create cost because telcos do not provide those services for free. Often, such transport fees can be high but also have a significant yet silent impact as the cost is absorbed in another budget center. As transport costs due to backhauling security services come to light, the resulting epiphany can be quite dramatic.

Another soft cost of security is operation and maintenance. Security tools require a person to operate the tool, and unfortunately for enterprises, security professionals are in short supply and their time is very valuable. As a result, the expectation for security tools and usability has grown exponentially. Security tools need to be easier to configure. They also need to block malicious activity without creating alerts or requiring human interaction. Finally, security tools need to provide guided search to enable security professionals to perform at a higher level than they traditionally have been able to manage. Essentially, security tools must evolve to make security professionals both more efficient and more effective.

IBOSS CLOUD OVERVIEW

The initial iboss secure web gateway solution was engineered in 2004 to address the changes in internet traffic. At that time, companies struggled with snowballing internet speeds, growth of mobile devices, and the need to secure traffic on-premises and off-premises. The early solutions were noted for providing scalable advanced threat and malware protection without losing granularity. A single appliance was capable of monitoring 200,000 concurrent devices and 6 million TCP/IP connections while filtering in a mixed directory environment. In addition, iboss consolidated its management console for all services.

The advent of the cloud and its impacts were not lost on iboss. The company completely re-architected its solution in the cloud and for the cloud, leveraging a new containerized cloud

node architecture. By delivering security from the cloud, iboss secures users regardless of location. Because hyperscale cloud providers offer global points of presence, data backhaul, and the corresponding latency, is minimized. The cloud also eliminates the need for appliance installation, hardware configuration, software and hardware maintenance/patching and, of course, the up-front capital expense. In addition, capacity planning for organizations becomes easy as consumption is a function of the number of users. Internet speeds and growing data consumption are managed by the iboss solution as an inherent function of being a cloud-based SaaS offering.

The mantra of iboss cloud is that it "secures user internet access on any device, from any location, in the cloud." The key benefits of the solution touted by iboss are:

- Global cloud footprint
- Multicloud
- Designed for privacy, data sovereignty, and compliance
- Eliminates appliances
- Eliminates data backhaul
- Containerized cloud architecture

Security applied is congruent with the needs of a digitally transformed environment. Attributes of the iboss solution include:

- Able to cache and analyze files for malware and data loss prevention, including PDF, Outlook data files, and zip files
- Provides full visibility across the entire data stream to detect and block the evasive malware that causes data breaches
- Monitors across all protocols to ensure that applications such as TOR and Torrent aren't being used as conduits for evasive malware
- Dynamically detects highly evasive applications that circumvent and evade security
- Monitors across all traffic to detect anomalies, alert IT, and automatically contain data exfiltration before loss occurs

THE BUSINESS VALUE OF IBOSS CLOUD ENTERPRISE SECURITY SOLUTIONS

Study Demographics

IDC interviewed eight organizations about their use of iboss cloud. The interviews focused on understanding the impact of iboss cloud from both quantitative and qualitative perspectives in terms of security risk, operations, and costs. As shown in Table 1, study participants were relatively large organizations with significant employees and business operations to secure (7,576 employees and $7.14 billion in annual revenue on average). The scale of their operations is reflected in the average of more than 32,000 devices that access their enterprise networks on a typical day and the challenges that securing this level of device access entails. The organizations interviewed were headquartered in the United States (6), United Kingdom, and Spain and provided perspectives and experiences from the following industries: chemical manufacturing, customer experience management, education, government, healthcare, insurance, IT services provider, and utilities.

TABLE 1 Firmographics of Interviewed iboss Customers

	Average	Median
Number of employees	7,576	2,150
Number of IT staff	724	126
Number of business applications	333	75
Number of total devices on enterprise network per day	32,394	9,000
Revenue per year (billion)	$7.14	$1.45
Countries	United States (6), United Kingdom, and Spain	
Industry	Chemical manufacturing, customer experience management provider, education, government, healthcare, insurance, IT services provider, and utilities	

Source: IDC, 2019

Choice and Use of iboss cloud

Study participants reported deploying iboss cloud to address specific concerns related to providing secure internet access for their employees, customers, and partners. They realized that their existing security environments and solutions were not capable of providing needed levels of security and too often carried additional costs in terms of hardware, bandwidth, and solution subscriptions. Further, several interviewed organizations noted the importance of

having a security solution with turnkey integration for Microsoft applications. Interviewed iboss customers described these considerations:

- **Providing the right combination of security functionality and cost of operations:** *"We concluded that iboss cloud was light-years ahead of what we were using at the time in terms of security functionality. The price factor was also important. When it came to iboss versus the other solutions we considered, iboss was a lot more affordable."*
- **Improving visibility into network traffic:** *"We chose iboss cloud because it provided clear visibility of all the traffic going through our networks with a good reporting engine, granular detail, and a way of identifying all traffic — suspect or otherwise — per person, not per IP address."*
- **Delivering the ability to support Microsoft applications:** *"Our use of Microsoft services factored into our choice of iboss cloud in a couple of different ways. iboss has a turnkey Office 365 through a proxy approach, and Office 365 is difficult to make work with proxies, so having a turnkey solution is very important. We're also using the iboss agent to meet our security requirements for Office 365."*

Table 2 provides information about the interviewed organizations' use of iboss cloud. Because iboss cloud is a cloud-based security solution, study participants were able to deploy it on top of various other security solutions in a relatively brief amount of time (three months on average). These iboss customers are using it to secure devices for almost all employees accessing their networks with somewhat less than two devices supported by iboss per employee on average. Several interviewed organizations are using iboss to secure quite distributed operations, reflected in the use of iboss cloud at an average of 64 sites (including offices, factories, and other business locations) per interviewed organization.

TABLE 2 Interviewed Organizations' Use of iboss cloud

	Average	Median
Number of employees supported by iboss cloud	7,299	2,050
Average total number of employee devices supported by iboss cloud	13,209	3,000
Number of business applications	281	75
Number of sites/locations/offices	64	6

Source: IDC, 2019

Business Value and Quantified Benefits

Interviewed organizations reported leveraging iboss cloud to achieve important dual benefits: They have reduced security-related risk while establishing more performance- and cost-effective security environments. As a result, they spoke about substantial benefits in terms of both operational risk reduction that is more challenging to quantify and lower costs of operating their security environments. iboss customers commented on these benefits:

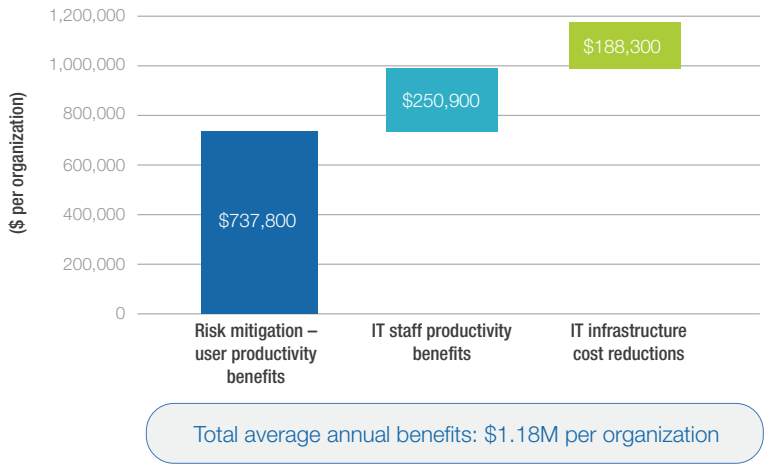
- **Having increased business confidence as a result of improved security:** *"The granularity that I have in the reporting with iboss cloud is far better than what I expected … We have more confidence in iboss and know that it will block threats. We've seen it perform and don't have to worry as much."*
- **Benefiting from moving to opex model:** *"We've consolidated security tools with iboss, and it does what we used to need six vendors to do … We're avoiding appliance purchases, which is included. One of the big advantages of moving to iboss cloud was moving from a capex-heavy cost model to doing all of it in opex — that's a huge benefit."*

Interviewed iboss cloud customers have leveraged improved and cost-effective security to capture significant value. Based on interviews with iboss customers, IDC projects that the customers will realize benefits worth an annual average of $1.18 million per organization ($89,100 per 1,000 devices) in the following areas (see Figure 1):

- **Risk mitigation and business productivity benefits.** Improved visibility and inspection of network traffic help minimize the risk of security breaches and other events, and more efficient routing of traffic enables improved application performance. IDC puts the value of improved user productivity due to improved application performance at an annual average of $737,800 per organization ($55,900 per 1,000 devices), while reduced operational risk is of crucial importance but typically more challenging for interviewed organizations to quantify because of its even more significant but more exceptional nature.
- **IT staff productivity benefits.** Network security teams handle network traffic and address security vulnerabilities more effectively, while help desk teams benefit from less frequent problems requiring remediation. IDC quantifies the value of efficiencies for these teams at an annual average of $250,900 per organization ($19,000 per 1,000 devices).
- **IT infrastructure cost reductions.** Use of a cloud-based security solution means that interviewed organizations avoid purchase and use of hardware appliances and reduce the extent to which they must backhaul network traffic to their headquarters. These hardware

and bandwidth efficiencies, combined with the lower cost of security solutions, enable cost savings worth an average of $188,300 per organization per year ($14,300 per 1,000 devices).

FIGURE 1 Average Annual Benefits per Organization



Source: IDC, 2019

Reduced Business and Operational Risks

Interviewed organizations must contend with the challenges associated with constant growth of network traffic and device numbers. Despite the use of various solutions and otherwise robust security environments, the organizations recognized that they did not have visibility into network traffic or the ability to inspect enough of it, leaving them vulnerable to impactful or even crippling security events.

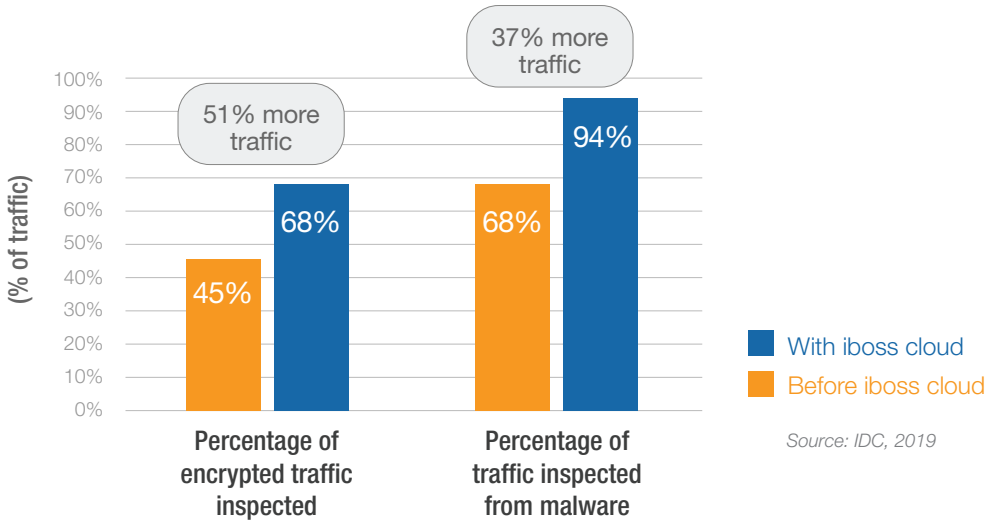
Interviewed organizations made the decision to deploy iboss cloud in large part because they concluded that it would provide critical visibility into network traffic, which they could leverage to better manage traffic and address potential security threats. In particular, iboss cloud has enabled them to inspect more network traffic through SSL decryption, thereby improving their understanding of network traffic and potential threats. As shown in Figure 2, interviewed organizations have made substantial and important strides in traffic inspection with iboss cloud, decrypting and inspecting 51% more traffic.

Study participants cited both iboss cloud's strong functionality in terms of SSL decryption and ability to allow for network inspection without significant adverse impact in terms of application performance that could otherwise undercut the rationale for inspection. One

interviewed iboss customer noted that it would have needed otherwise to double spending to offset potential performance impact: *"iboss cloud has enabled us to turn on inline SSL decryption because it was going to be about a 100% cost increase previously. This was because we could get only about half the performance on the hardware appliances. iboss has allowed us to do that in line without doubling spend."* Another organization reported similar considerations: *"With iboss cloud, we are able to actually use decryption, whereas we weren't using it with [our previous solution]. We weren't able to because it just would have brought everything down … We've reduced security risk with iboss cloud because we have far more mobile users that are coming through now, and we can inspect that traffic going both in and out."*

In addition to higher levels of network traffic inspection, study participants reported increasing the extent of protecting traffic from malware by an average of 37% with iboss cloud. These higher levels of traffic inspection and protection from malware represent significant and real gains in terms of hardening their security environments against impactful security events.

FIGURE 2 Security-Related KPIs



Source: IDC, 2019

For study participants, more robust internet security translates into improved risk profiles. While the value of reduced risk can be challenging to quantify — because risk-related losses are by their nature unique and unpredictable — study participants provided details about how they have lowered operational risk with iboss cloud by having better visibility into network traffic, identifying more potential security threats, and being able to proactively head off potential impactful events. One interviewed organization described the very significant impact on its ability to find and address vulnerabilities:

> *The risk of security breaches went down significantly with iboss cloud because we weren't seeing them, and now we are. When we first deployed iboss cloud, we had over 100,000 vulnerabilities, and we had close to 500 infected hosts. Today, we have about 6,000 vulnerabilities and we have about 12 infected hosts … With iboss cloud, we're identifying around 80% of potential breaches before they become impactful compared with 10% previously.*

Interviewed iboss cloud customers linked these types of improvement to lower risk associated with:

- **Impactful security breaches,** with study participants estimating a 38% reduction in risk on average with breaches that can hamper operations, create reputational harm, and require significant resources to remedy
- **Regulatory noncompliance,** with study participants attributing a 30% lower chance on average of incurring fines or penalties related to regulatory compliance regimes
- **Major revenue losses,** with study participants linking use of iboss cloud to a 17% lower chance on average of significant business interruptions

Study participants linked these types of security-related events to very significant costs, including the potential for reputational harm. While study participants could not put a specific value on having a reduced risk profile with iboss cloud, IDC's research with end-user organizations consistently shows that these events can carry costs in the tens of thousands, hundreds of thousands, or even millions of dollars or more in damage related to lower employee productivity, lost revenue, and fines and/or penalties.

Improved Application Performance

Study participants noted the ability to harden their security through traffic inspection regardless of a user's device and location without negatively affecting application performance. They also noted the ability to enable mobile and other users through more streamlined and frictionless security. Several organizations described challenges associated with the use of other security solutions and approaches, including virtual private networks (VPNs). As organizations' reliance on employees' ability to access applications from mobile devices increases, these approaches become more outdated and even costly in terms of limiting employee access to high-performing, robust business applications and services.

Study participants noted wide-ranging benefits for employees across their organization in terms of improved application performance as measured by latency with iboss cloud. They

linked these performance improvements to operational efficiencies in the form of higher user productivity as employees better leverage business applications to do their jobs.

One study participant linked its choice of iboss cloud back to enabling and securing mobile users: *"The main driver of moving to cloud security with iboss was the move to mobile devices for our field staff and mobile devices in general. We just implemented a system that is rolling out 700 mobile devices to our field staff."* Another cited time savings on a daily basis for employees because they no longer need to sign into VPNs: *"The biggest difference with iboss cloud is that remote users can use secure remote connections. Before, they had to sign into a VPN, so they are saving time by avoiding this sign-in step."* Overall, most employees at interviewed organizations benefit from application performance gains with iboss cloud, with IDC putting the average net time efficiency at 3.5 hours per user per year, a significant value driver across an average of 6,287 employees benefiting from iboss cloud (see Table 3).

TABLE 3 User Productivity Impact

	Per Organization	Per 1,000 Devices
Number of impacted users	6,287	476
Average gross productivity gain (impacted users)	1.2%	1.2%
Net productivity gain (FTEs)	11.6	0.9
Net productive hours gained per user per year	3.5	3.5
Total value of higher net productivity — IDC model*	$813,400	$61,600

Source: IDC, 2019

** IDC applies a 15% margin assumption in assessing the value of increased user productivity for purposes of the Business Value financial analysis.*

Security Team Efficiencies

Interviewed organizations rely on their security and other IT teams to deliver secure, high-quality IT services to their employees and customers. It is important that these teams be focused on taking all possible steps to harden their security environments rather than having time consumed by day-to-day activities.

Interviewed iboss cloud customers consistently described time savings for these teams by reducing time required for managing iboss cloud compared with previous solutions, making threat analysis and detection more seamless, and minimizing time spent on hardware. Interviewed iboss customers spoke about these benefits and noted the value in reallocating saved staff time to higher-level security activities and initiatives:

- **Reallocating staff time to manage broader security vulnerabilities:** *"We have a three-person team, and we're saving 50% of our time with iboss cloud and avoiding hiring … We're putting time savings into our vulnerability management program, which we've built in a way that complements iboss cloud."*
- **Avoiding hiring due to visibility that helps collect information**: *"Let's put it this way, without the visibility that iboss cloud provides, if we had to collect the additional information that iboss provides manually, it would take months to do it. This means that we're avoiding hiring people to do that work … We can use staff time savings for better expert analysis and do much more in deep site investigations."*
- **Saving time by minimizing hardware-related tasks:** *"Team time savings are around hardware maintenance and taking care of hardware upgrades, whereas we now have an evergreen cloud-based solution with iboss … Most of the freed-up staff time is spent on preemptive vulnerability management."*

Table 4 shows the impact on interviewed organizations' IT security teams from the use of iboss cloud. On average, they reported that these teams are 35% more efficient as a result of using iboss cloud, freeing up the equivalent of 2.4 staff members' time per organization even as they otherwise make significant strides in improving their security postures as described in this white paper.

TABLE 4 IT Security Team Impact

	Before iboss cloud	With iboss cloud	Difference	% Efficiency with iboss cloud
FTEs required to support equivalent SAP workloads per organization	6.8	4.4	2.4	35
Staff time per year in hours per 1,000 devices	973	632	341	35
Value of staff time required per organization per year	$683,400	$444,100	$239,400	35

Source: IDC, 2019

Security-Related IT Cost Savings

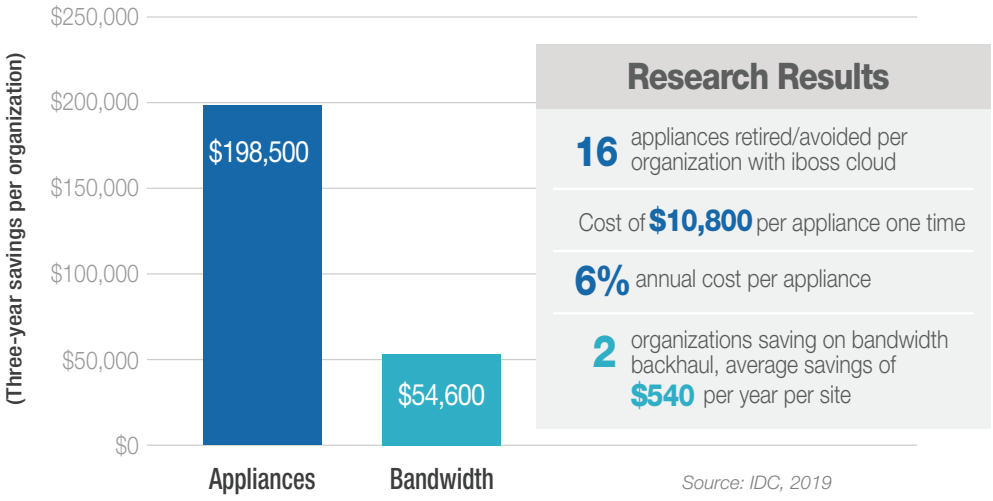
Study participants also described cost efficiencies from using a cloud-based security delivery model with iboss cloud in several key areas: hardware appliance, bandwidth, and solution costs. As a result, they can enhance their security in a cost-effective way, which helps them more readily extend and scale their iboss cloud environments to address business demand and new security threats.

Most interviewed iboss cloud customers cited their ability to deliver enhanced security without needing additional hardware as beneficial. They noted that they otherwise would have needed to deploy more hardware appliances, which would require not only up-front capital investment but also operational expenses to operate those appliances. In addition, several iboss cloud customers linked more efficient use of network bandwidth to the solution because they no longer must backhaul network traffic to their headquarters. This not only allows them to make more optimal use of bandwidth but also can result in lower latency levels and improved application performance, as described previously. Interviewed iboss cloud customers provided details about the cost-related benefits they are achieving:

- *"We've replaced 40 appliances with iboss at about $10,000 per appliance … We're also avoiding a little bit of backhaul bandwidth because we can connect locations without bringing it back to our headquarters first. We've avoided around $10,000 per month in additional spend on bandwidth."*
- *"If we were to purchase appliances in place of using iboss cloud, we'd probably spend $50,000–100,000 over a three-year life cycle … We are also avoiding backhauling with iboss. We are just not having to use backhauling as much. We're saving thousands of dollars a month."*

As shown in Figure 3, appliance-related savings for study participants include avoiding 16 appliances on average per organization with a three-year cost of $198,500 per organization. Additionally, interviewed iboss customers reported saving an average of $540 in bandwidth costs per site where traffic no longer must be backhauled, for a total savings of $54,600 per organization over three years.

FIGURE 3 Three-Year Appliance and Bandwidth Cost Savings



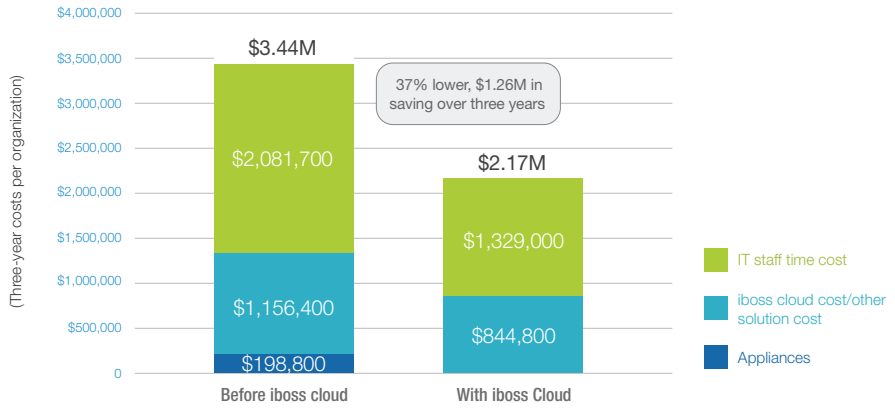
Source: IDC, 2019

IDC ANALYZE THE FUTURE

In addition, at a solution level, several study participants reported spending less on iboss cloud because it has enabled them to retire or consolidate other security solutions. One interviewed iboss customer commented: *"By canceling our subscription to our previous solution, we're saving money, but iboss is a much better product because our previous solution was only offering one feature that iboss has. iboss is much more complete, and you can control web filtering, do advanced malware, and have visibility on users."*

These cost-related benefits, in addition to the efficiencies for IT security–related teams, mean that study participants incur significantly lower total costs over three years with iboss cloud than previous or alternative approaches — 37% lower on average (see Figure 4).

FIGURE 4 Three-Year Cost of Operations



Source: IDC, 2019

ROI Summary

Table 5 presents IDC's analysis of the benefits and costs related to interviewed organizations' use of iboss cloud. IDC calculates that study participants will achieve total three-year discounted benefits in terms of higher user and IT staff productivity and cost savings worth $2.80 million ($211,800 per 1,000 devices). These benefits compare with total three-year discounted investment costs of $0.75 million ($56,500 per 1,000 devices). This would result in a three-year ROI of 275%, with breakeven occurring in an average of four months.

TABLE 5 Three-Year ROI Analysis

	Per Organization	Per 1,000 Devices
Benefit (discounted)	$2.80 million	$211,800
Investment (discounted)	$0.75 million	$56,500
Net present value (NPV)	$2.05 million	$155,400
ROI (NPV/investment)	275%	275%
Payback period	4 months	4 months
Discount factor	12%	12%

Source: IDC, 2019

CHALLENGES/OPPORTUNITIES

The most significant challenge with the iboss solution is that it requires a change in the way most enterprises think about security. IDC recommends that to tackle this challenge head-on, enterprises focus on the following benefits they can achieve via the iboss solution:

- Improve employee productivity levels by reducing latency and delivering more bandwidth, leading to improved application performance, especially for mobile users.
- Generate efficiencies for security teams by providing visibility and actionable detail into network traffic, allowing IT teams responsible for security to react more efficiently and effectively to threats.
- Lower security-related costs by avoiding the need for hardware appliances, reducing bandwidth consumption for backhauling network traffic, and retiring less cost-effective security solutions.

To change and thus realize such benefits, security, IT operations, purchasing, and other stakeholders may be required to come together and have a meaningful conversation. Comparing a price per user across multiple solutions makes it easy to select the lowest price solution; it just may not be the lowest total cost or most appropriate solution for the organization. Well-informed decisions take greater time and consideration.

CONCLUSION

Digital transformation has produced more than cosmetic effects on enterprise networks. DX has driven these networks to become highly heterogeneous, incorporating elements of mobile, Internet of Things, public/hybrid clouds, and SaaS applications with internal and remote access by employees and a burgeoning assortment of third parties from an equal assortment of devices, points of origination, and circumstances.

Enterprises thus need to rethink security at a time when ongoing digital transformation initiatives have helped businesses rapidly create new products and services. Inappropriate security not only provides a lack of protection for complex DX networks but also can be unintentionally or unknowingly expensive. The hard costs of security are easy to assess; those costs are transparent. The "soft costs" can be brutal. Latency certainly kills the user experience; the causal transport and backhaul of security traffic can create a cost epiphany. In addition, operation and maintenance of security tools create excessive effort for security professionals who are in short supply and see demand-driven salary increases. Today's security professionals must be empowered to perform at a higher level than they traditionally have been able to manage.

IDC's study demonstrates the strong value that organizations can achieve with iboss cloud by reducing business and operational risk as well as the costs of ensuring security. They noted having the ability to inspect significantly more network traffic, which allows them to better assess potential risk, and ultimately to reduce the risk associated with security breaches, regulatory compliance, and business operations. While the value of reduced risk can be challenging to quantify, these types of security incidents can carry substantial costs in tangible business losses and reputational damage. Meanwhile, iboss cloud has also helped interviewed organizations optimize their security costs by avoiding the need to purchase hardware appliances, reducing bandwidth requirements as network traffic no longer needs to be backhauled to headquarters, and making IT security teams more efficient and effective. Combined, these benefits translate to substantial value for interviewed iboss cloud customers, with IDC putting the value they will achieve at an average three-year ROI of 275%.

APPENDIX

Methodology

IDC's standard ROI methodology was utilized for this white paper. This methodology is based on gathering data from organizations currently using iboss cloud enterprise security solutions as the foundation for the model. Based on interviews with organizations using iboss cloud, IDC performed a three-step process to calculate the ROI and payback period:

1. Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of using iboss cloud. In this study, the benefits included staff time savings, user productivity benefits, and security-related cost reductions.

2. Created a complete investment (three-year total cost analysis) profile based on the interviews. Investments go beyond the initial and annual costs of using iboss cloud and can include additional costs related to migrations, planning, consulting, and staff or user training.

3. Calculated the ROI and payback period. IDC conducted a depreciated cash flow analysis of the benefits and investments for the interviewed organizations' use of iboss cloud over a three-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For purposes of this analysis, IDC has used assumptions of an average fully loaded salary of $100,000 for IT staff and an average fully loaded salary of $70,000 for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).

- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.

- Further, because use of iboss cloud requires a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC
ANALYZE THE FUTURE