Sponsored by: **ForeScout**

Authors:
Robert Ayoub
Matthew Marden

December 2016

The Business Value of Pervasive Device and Network Visibility and Control with ForeScout

Business Value Highlights

392%
five-year ROI

13 months
to breakeven

$46,040
in benefits per year per 1,000 devices on networks

24%
more known devices

18%
more devices in compliance

50%
fewer network-related security breaches

13%
more efficient IT staff device and network security

EXECUTIVE SUMMARY

Many organizations feel like attackers have the upper hand. Statistics continue to pour in showing that successful breaches are still occurring with increased frequency even though security spending continues to increase. News headlines constantly report data that was leaked from organizations of all sizes, large and small, and in every vertical. It is evident that security must be improved, but how can an organization know that its security spend is addressing the core challenges and not simply adding one more security product to an already overworked staff?

IDC believes that one of the key attitudes for organizations to adopt is that of "already breached." This attitude focuses on visibility and detection, with strong remediation capabilities. Instead of perfectly protecting each and every vector, this attitude encourages constant vigilance and the ability to respond quickly, making the organization's security agile enough to meet the rapidly changing business and threat landscape. One solution that addresses this idea of pervasive device visibility and control is ForeScout's security solution.

IDC interviewed senior IT staff responsible for device and network security operations at seven organizations that have deployed ForeScout's security solution to understand the impact on their ability to control and secure their network environments. These interviews showed that ForeScout provides the visibility and control capabilities that these organizations need to effectively and efficiently reduce security risk inherent to the tens of thousands of devices using their networks on a daily basis. IDC calculates that as a result, these organizations will realize benefits worth an annual average of $46,040 per 1,000 devices on their networks ($1.97 million per organization) over five years and achieve a five-year ROI of 392% by:

- Saving time for IT staff managing device and network security through enhanced visibility, automation, and improved reliability
- Reducing the business and operational impact of network- and device-related security breaches
- Enabling auditing and compliance teams to work more effectively
- Supporting users and business operations with more efficient and effective network security measures

Situation Overview

The current IT landscape is much different than what it was 10 years ago. While the need to monitor the health of guest devices is still a key challenge, there are many other factors driving the need for visibility and access control today:

- **BYOD impacts networks.** The exponential growth of BYOD and the potential of IoT place unprecedented demands on both the wireless and the wired network. Administrators not only need to accommodate a greater amount of traffic but also need visibility into a range of devices that they have not had visibility into before. Employees must access the corporate network from almost anywhere without compromising network or application security.
- **IoT challenges are growing.** In addition to users bringing their own devices onto the network, the number and types of devices associated with each user have also increased. IoT devices ranging from sensors to videocameras are finding their way onto IT networks, causing significant challenges for security teams, which may not even know that these devices are on the network. Consistent policies must be applied regardless of the device. Most IoT devices don't run on traditional operating systems and therefore can't support software agents. Alternatively, new devices present new attack vectors that must be protected against.
- **Visibility and automation are key.** The complexity of today's network environment demands manageability that allows for quick and consistent deployment of policies. Organizations must have tools available that allow them to visualize the network and the devices on it. They must have tools that provide for consistent policy delivery and automated response to incidents as they occur.
- **Organizations must determine the security policy across all devices.** At the end of the day, organizations bear the ultimate responsibility for securing their networks and data. Organizations need to maintain consistency in how security is applied across the entire network infrastructure — wired or wireless and regardless of device type or user.

Forescout Network Security Solutions

ForeScout offers comprehensive network access control capabilities, allowing administrators visibility and control of both managed and unmanaged devices by constantly eyeing the access of the network. It continuously monitors activity of the network and the activity of known, company-owned devices as well as unknown devices such as personally owned and rogue endpoints. It allows administrators the ability to automate and enforce policy-based network access control, endpoint compliance, and mobile device security. ForeScout provides an extensive range of automated controls that preserve the user experience and keep business operations running to the maximum extent possible. ForeScout provides intelligence and functionality across three key areas, which are discussed in the sections that follow.

Visibility

ForeScout offers the ability to discover devices the instant they connect to the network, without requiring software agents or previous device knowledge. It profiles and classifies devices, users, applications, and operating systems while continuously monitoring managed/unmanaged devices including IoT, personally owned devices, and other endpoints.

Control

ForeScout can allow, deny, or limit network access based on device posture and security policies. By assessing and remediating malicious or high-risk endpoints, it mitigates the threat of data breaches and malware attacks that would otherwise put the organization at risk. In addition, by continuously monitoring devices on the network and controlling them in accordance with predefined security policies, ForeScout dramatically streamlines an organization's ability to demonstrate compliance with industry mandates and regulations.

Orchestration

ForeScout integrates with more than 70 network, security, mobility, and IT management products. This ability to share real-time security intelligence across systems and enforce a unified network security policy reduces vulnerability windows by automating systemwide threat response. This allows for a seamless workflow across existing security tools, thus saving time and automating many traditionally manual actions.

The Business Value of Forescout

Study Demographics

IDC interviewed seven organizations that have deployed ForeScout security solutions to understand the impact on their security and operations. These organizations were primarily large enterprises, ranging from several thousand employees to almost 100,000 employees, and represented the experiences of a number of industry verticals, as shown in Table 1. These organizations are using ForeScout to improve their security postures for networks with tens of thousands of devices accessing them on a daily basis, including a mix of company-owned, BYOD, and IoT devices. Growth to these device environments — particularly in terms of BYOD and agentless IoT devices — has proven especially challenging for organizations to handle, which was a major driver of their decision to add ForeScout to their security environments.

Business Value Analysis

Interviewed organizations have leveraged their use of ForeScout to reduce their exposure to risk even as they have made their network- and device-related security efforts more efficient. IDC projects that as a result, these ForeScout customers will realize benefits worth an average of $46,040 per 1,000 devices per year ($1.97 million per organization) over five years in the following areas (see Figure 1):

TABLE 1

Demographics of Interviewed Organizations

	Average	Median
Number of employees	31,100	20,000
Number of IT staff	1,623	1,000
Number of IT users	27,500	20,000
Number of offices /locations	788	100
Number of devices	42,843	32,500
Number of agentless devices	29,586	18,500
Countries	United States and United Kingdom	
Industries	Education, finance, government, healthcare, retail, software development, and technology manufacturing	

n = 7

Source: IDC, 2016

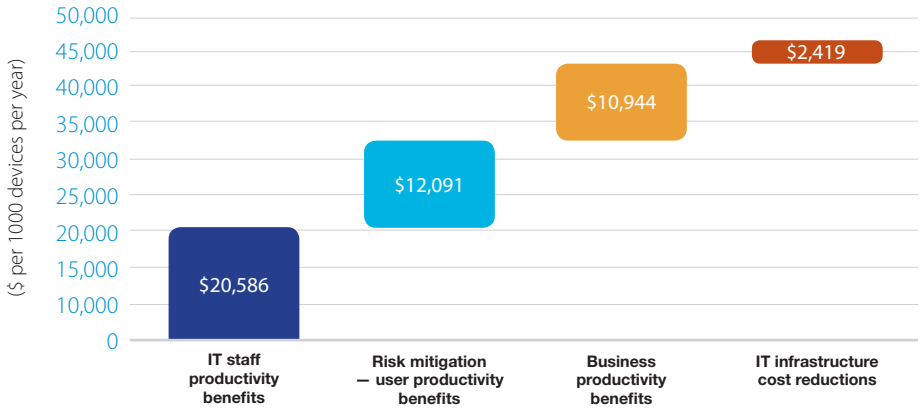
- **IT staff productivity benefits.** ForeScout provides the visibility, automation, and remediation capabilities that IT networking and device staff require to be more efficient in carrying out their responsibilities. As a result, organizations can manage and secure more devices, thereby improving their security postures without increasing IT staff count. IDC calculates that these organizations will achieve IT staff time savings worth an average of $20,586 per 1,000 devices per year ($882,000 per organization) over five years.
- **Risk mitigation — user productivity benefits.** ForeScout identifies and locates more devices, enabling organizations to bring them into compliance and apply security policy, which limits the frequency of security-related breaches and also enables faster remediation. IDC projects that as a result, interviewed organizations will capture $12,091 per 1,000 devices per year ($518,000 per organization) over five years in employee productivity and revenue, an amount previously lost to impactful breaches.
- **Business productivity benefits.** ForeScout provides a more secure business environment, which benefits LOB employees. IDC puts the value of higher employee productivity at an average of $10,944 per 1,000 devices per year ($468,900 per organization) over five years.
- **IT infrastructure cost reductions.** ForeScout enables interviewed organizations to retire certain other security solutions and limit the use of third parties supporting their security efforts. IDC calculates that these organizations will save an average of $2,419 per 1,000 devices per year ($103,600 per organization) over five years.

Improving Visibility

Interviewed organizations described achieving the requisite level of visibility into their network environments as among the most vexing issues they face in making their security efforts more efficient and effective. Stated succinctly, this means organizations were unable to efficiently locate and identify all devices accessing their networks, which left them susceptible to malware, viruses, and other security breaches. As a result, they were unable to provide the level of security demanded by their business operations, even if they were fortunate enough

FIGURE 1

Average Annual Benefits per 1,000 Devices



Average annual benefits per 1,000 devices: $46,040

Source: IDC, 2016

to not suffer significant security breaches that compromised customer data or other sensitive information.

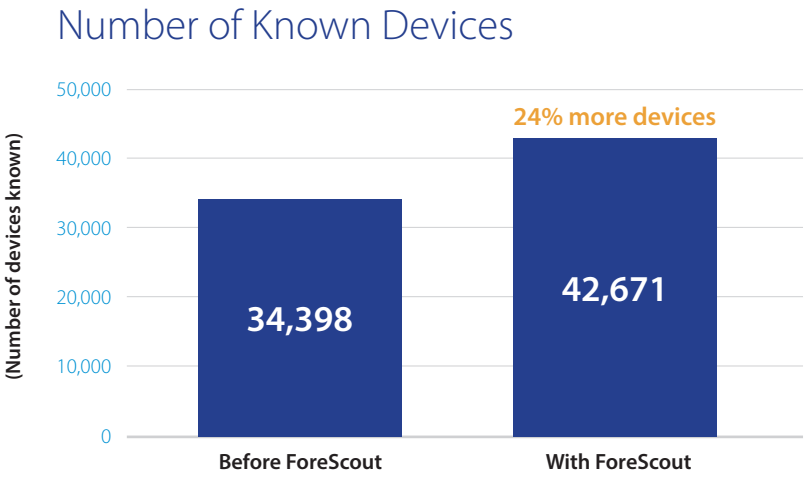
Interviewed organizations reported that the deployment of ForeScout has had a significant impact on their ability to gain a fuller purview into the devices accessing their network. As Figure 2 indicates, these ForeScout customers have increased the number of devices they know to be on their networks by an average of 24%. This means that they can now monitor, grant or deny access, secure, and respond to potential issues with these devices in a more proactive manner. One organization explained the profound impact ForeScout has had in this area: *"ForeScout has impacted the number of known devices by giving us visibility …. Before, we didn't really know how many devices were on our networks. I mean we had different methods of auditing things, but because we have a lot of people who are mobile, it makes it a very hard figure to keep an eye on. The number of known devices was much smaller — I'd say about one-third of now."*

"ForeScout has impacted the number of known devices by giving us visibility …. Before, we didn't really know how many devices were on our networks. I mean we had different methods of auditing things, but because we have a lot of people who are mobile, it makes it a very hard figure to keep an eye on. The number of known devices was much smaller — I'd say about one-third of now."

IT Staff Productivity Benefits

Like at many organizations, IT staff responsible for network and device management and security at interviewed organizations are challenged by expanding device environments and security threats. This makes the efficiencies they are achieving with ForeScout in remedying breaches, monitoring network environments, and automating security especially meaningful; ForeScout not only is helping them improve security but also is supporting the growing importance of the network to the operations and business. According to

FIGURE 2



Source: IDC, 2016

interviewed organizations, their IT staff teams are saving time with ForeScout in a number of areas where visibility and automation are impactful, including help desk (19%), device management (14%), security administration (13%), endpoint security (11%), network security (11%), and audit management (6%) (see Figure 3). Across these areas, the interviewed organizations are achieving an average of 13% efficiencies, saving 64 hours of staff time per year per 100 users supported.

An interviewed organization described how enhanced visibility with ForeScout enables it to more effectively and efficiently carry out the company's security policies: *"The most significant thing that ForeScout has done for us is that it's given us a holistic view of what's on our network in terms of managed, unmanaged, and BYOD devices. Previously, we had no good way of estimating what was out there. It's kind of like owning a huge ranch and not knowing what's going on, on different parts of your own property …. That's important because it allows us to size and target our security efforts appropriately."* Another organization explained how automation with ForeScout saves staff time on carrying out manual remedial steps: *"We have a team of 48 managing devices, spending 40% of their time on endpoint security. If we didn't have ForeScout, they'd be manually remediating stuff that's not encrypted, so they'd probably be spending at least another 10–20% of their time on it."*

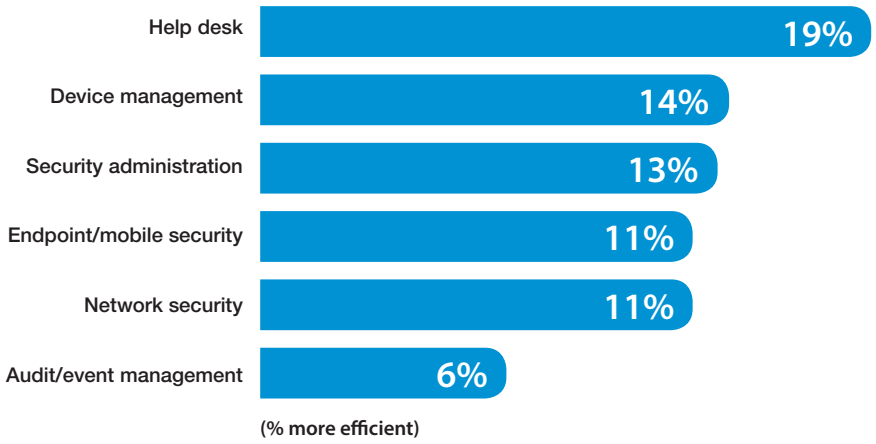
"We have a team of 48 managing devices, spending 40% of their time on endpoint security. If we didn't have ForeScout, they'd be manually remediating stuff that's not encrypted, so they'd probably be spending at least another 10–20% of their time on it."

Risk Mitigation — User Productivity Benefits

By identifying more devices on their networks, organizations can begin the process of minimizing risk associated with those devices. This often involves making sure that a device is in compliance with the organization's network security policies and taking proactive steps to ensure this where necessary. Figure 4 demonstrates the scale of the impact that ForeScout has had at these organizations; they have identified more than 8,200 additional devices per organization, or on average, 24% more devices than previously known, and ensured compliance of almost 5,500 more

FIGURE 3

IT Network and Device Security Staff Efficiencies



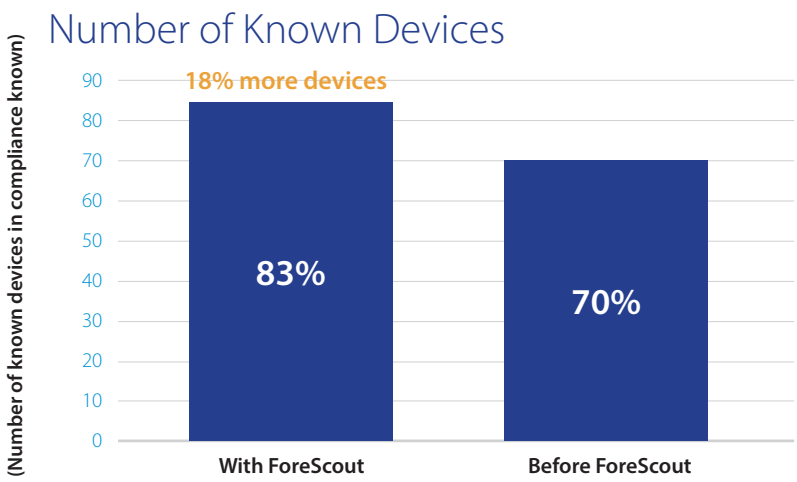
Source: IDC, 2016

devices per organization, or 18% more devices. This visibility enables organizations to ensure higher compliance rates up to full endpoint compliance per their needs, with more than half of the interviewed organizations leveraging ForeScout to achieve device compliance rates of 95%+. As a result, average device compliance rates have increased from 70% to 83% with ForeScout. As one interviewed organization explained: *"ForeScout has significantly helped device compliance because it has allowed visibility. We operate under a model of trust but verify; we trust that our staff managing endpoints are doing their jobs, but we now have an independent source of verification of compliance."*

"ForeScout has significantly helped device compliance because it has allowed visibility. We operate under a model of trust but verify; we trust that our staff managing endpoints are doing their jobs, but we now have an independent source of verification of compliance."

In addition to ensuring compliance, ForeScout makes it simpler for organizations to identify security threats and to take remedial actions as needed. In particular, its ability to evaluate any device's security posture and automatically take action to limit the likelihood of an impactful security event from happening limit organizational risk and make IT security teams more effective. One interviewed organization noted: *"With ForeScout, when there's a problem with a device, we can go proactively and tell whether the device is compromised. Before, the end users were the ones actually doing the detection and reporting. Now, we're doing the detection and reporting centrally, which means that MTTR has gone from a week or two for our field technicians*

FIGURE 4



Source: IDC, 2016

to 48 hours." Another organization described how visibility with ForeScout enables it to more effectively apply its security policies: *"Visibility improves our ability to implement security policies. In each area we have visibility, we take steps to standardize and then apply a policy …. That's the hard security and compliance. ForeScout is helping us mitigate our risk in ways that we otherwise could not."*

The net result for interviewed organizations is that ForeScout reduces the impact of network- and device-related security breaches to a significant degree, as demonstrated in Table 2. Probably of equal importance to these organizations, ForeScout provides an additional level of confidence that their most sensitive data will not be exposed through security breaches and that their business operations will not face disruptions from security exposure.

In addition to minimizing the operational risk associated with security breaches, ForeScout enables more efficient auditing and compliance efforts. These efficiencies can be traced in part to more limited paperwork associated with breaches as well as enhanced visibility about overall network and device environments. These teams are on average 26% more efficient with ForeScout, with one customer commenting: *"Quite a few people save time on our compliance team, because fewer breaches means a lot less work because there's less need to handle associated work like notifications. Probably about 10–12 people work on compliance, and they're saving at least one-third of their time with ForeScout."*

TABLE 2

Risk Mitigation

	Before ForeScout	With ForeScout	Difference	Benefit (%)
Network-related security breaches				
Number of impactful breaches per year	0.7	0.4	0.3	42
MTTR (hours)	15.2	10.0	5.2	34
Productive time lost per 1,000 devices per year (hours)	375	188	187	50
Device-related security breaches				
Number of impactful breaches per year	394	246	148	38
MTTR (hours)	11.3	6.0	5.3	47
Productive time lost per 1,000 devices per year (hours)	107	66	41	39
Auditing and compliance team efficiencies				
Time per 1,000 devices per year (hours)	381	282	99	26

Source: IDC, 2016

organizations have made obtaining guest network access much less time consuming, which means that less staff time is required to support this access. Also, this provides a better and more timely experience for network guests, which can be important for the partners, customers, contractors, and other users who require timely and secure network access when visiting these organizations.

ROI Analysis

Based on interviews with ForeScout customers, IDC used the following three-step method for conducting the ROI analysis:

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

TABLE 3

Business Operations Impact

	Per Organization	Per 1,000 Devices
User Productivity Impact		
Productivity gain from improved security	2%	2%
Number of impacted users	1,500	35
Additional productive time per year (hours)	16,389	383

Source: IDC, 2016

2. **Created a complete investment (five-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of deploying ForeScout and can include additional costs related to migrations, planning, consulting, configuration or maintenance, 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 organizations' use of ForeScout over a five-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.

Table 4 presents IDC's analysis of the total benefits and costs for interviewed organizations associated with their use of ForeScout. IDC calculates that these organizations will invest a discounted average of $32,381 per 1,000 devices ($1.39 million per organization) over five years and can expect to realize $159,292 per 1,000 devices in discounted benefits ($6.82 million per organization) in return. For these ForeScout customers, this would result in an ROI of 392%, with breakeven in their investment happening in 13 months on average.

Challenges and Opportunities

» **Need for policies and integration to be defined up front.** Like any other security solution, policies must be clearly defined and implemented at the time of deployment. ForeScout can ease the onboarding process, deploy policies consistently across the organization, and perform endpoint assessments, but those policies must be defined in advance. Control policies, however, can be phased in over time. Policies can be monitored over time prior to activating enforcement actions. ForeScout enforces policies but is not going to provide prevention or remediation for everything (such as malware outbreaks

TABLE 4

Five-Year ROI Analysis

	Per Organization	Per 1,000 Devices
Benefit (discounted)	$6.82 million	$159,292
Investment (discounted)	$1.39 million	$32,381
Net present value (NPV)	$5.45 million	$126,910
Return on investment (ROI)	392%	392%
Payback period	13 months	13 months
Discount rate	12%	12%

Source: IDC, 2016

and phishing attacks). Adding ForeScout may require integration with third-party security solutions to provide end-to-end protection. However, ForeScout has a very robust technology ecosystem to ensure compatibility and allow security workflow automation with most security equipment providers.

- **Potential impact on end users.** Any assessment of the endpoint has the potential to cause an impact to users. The quarantining of an infected device may affect the user experience and require manual intervention to resolve. Organizations must weigh a potentially negative user experience against protecting the enterprise network and determine the best way to handle exceptions.

- **Difficult to integrate results into security workflow.** While ForeScout's solution can increase the visibility of assets on the network, how the security team reacts to new devices, infected devices, and unpatched devices has to be determined. The wealth of information provided by ForeScout could be overwhelming for a security department that is not ready to ingest and react to that information.

Summary and Conclusion

"Behave as though you have been breached" is the new reality for security practitioners today. With the average attacker having access to a network for close to a year, it is clear that traditional approaches to security are flawed. The only way, however, to posture defenses in order to address breaches is to increase the visibility of all devices across the network and have a method in place for monitoring devices, scanning for vulnerabilities, and identifying and containing infections the minute they occur. These capabilities will require multivendor integration.

ForeScout's solution addresses key challenges around visibility, control, and automation, allowing security teams to not only better understand what devices are accessing resources but also respond to threats in a consistent manner. IDC's research with organizations using ForeScout network security solutions shows that they are gaining the visibility into their network environments that they need to increase security and become more efficient. These organizations that installed ForeScout reported significant savings in the time spent managing devices, ultimately leading to reduced costs per device and allowing the security team to realize efficiencies in their ability to respond to threats. As a result, they are better able to provide the level of security demanded by their business operations and minimize the security risk related to the tens of thousands of devices using their networks on a daily basis.

Appendix

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from current users of ForeScout as the foundation for the model. Based on interviews with seven organizations using ForeScout, IDC performed a three-step process to calculate the ROI and payback period:

- Measure the savings from reduced IT costs (staff, hardware, software, maintenance, and IT support) and increased user productivity over the term of the deployment compared with their previous infrastructure environments.
- Ascertain the investment made in deploying ForeScout network access control security solutions and the associated migration, training, and support costs.
- Project the costs and savings over a five-year period and calculate the ROI and payback for the deployed solution.

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. IDC assumes a fully-burdened salary of $100,000 per year for IT staff, and $70,000 for other employees, with an assumption of 1,880 hours worked per year.
- Downtime values are a product of the number of hours of downtime multiplied by the number of users affected.
- The impact of unplanned downtime is quantified in terms of impaired end-user productivity and lost revenue.

- Lost productivity is a product of downtime multiplied by burdened salary.
- The net present value of the five-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.

Because every hour of downtime does not equate to a lost hour of productivity or revenue generation, IDC attributes only a fraction of the result to savings. As part of our assessment, we asked each company what fraction of downtime hours to use in calculating productivity savings and the reduction in lost revenue. IDC then taxes the revenue at that rate.

Further, because IT solutions require 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