The Case For End-To-End Solutions For Mid Market Firms
Better Security Improves Every Part Of The Business

In a digital business, processes are rarely, if ever, confined to the infrastructure of the company. Customers and employees engage across numerous digital channels and dozens of third-party relationships critical to operations. IT leaders must rapidly evolve to protect their firms’ brands, strengthen their reputations, and build customer trust. To do so, security and productivity should go hand-in-hand, and that means a well-defined policy framework, metrics that demonstrate business value, and a business-aligned strategy that ties all this together.

Key Findings

Security drives profits. Security touches every part of the business, but a breach can cost firms hundreds of millions of dollars, making it a compelling business case.

Security should be a pillar of business differentiation. Companies that take a proactive approach to improving their security for their employees and their customers will create more marketable and better services.

Building a high-performing security organization depends on partners. Leveraging the expertise of partners reinforces a robust security infrastructure — especially those that can provide end-to-end security solutions.
In the digital age, firms must protect data from theft, misuse, and abuse because data is the lifeblood of a digital business. The biggest source of competitive differentiation comes from how organizations use data and act on insights to create value for their customers while also increasing operational agility to serve customers and form digital ecosystems that have, at the bare minimum, the potential to drive entirely new revenue streams.

It’s no surprise then that IT and business decision makers are concerned about the loss of customer data (58%). In fact, attackers can compromise any party that has access to the organizations’ data, which is why malware or ransomware (58%) also top the list of security concerns. Other security concerns include loss of employee data (53%), compromised IP (52%), and security holes in applications (51%).
Security Initiatives Focus On Data, Devices, And Infrastructure

Cybercriminals and attackers can breach the security defenses of even the largest enterprises with relatively mature security programs and practices, and incentive to do so ranges from financial gain to ideological protest to nation state-backed mandate. In fact, only 8% of respondents said they have never had a security breach. During a breach, organizations stand to lose valuable intellectual property and personal data of customers, partners, and employees.

Taking the level of concern into consideration, over the next 12 months, business and IT leaders are seeking to shore up their security defenses by improving data security (85%), device security (82%), and infrastructure capabilities like increasing security monitoring (82%).

The top IT infrastructure priority is to improve the security infrastructure of the organization (83%).

Which of the following initiatives are likely to be your firm’s top IT security priorities over the next 12 months?

- Improving data security: 85%
- Improving IT and device security (including mobile): 82%
- Improving the security of customer-facing services and applications: 82%
- Improving security monitoring capabilities: 82%
- Improving application security capabilities and services: 78%
- Leveraging cloud-based or managed security services: 78%
- Improving advanced threat intelligence capabilities: 77%
- Rolling out effective security training and awareness for employees across the organization: 77%
- Enhancing business continuity/disaster recovery capabilities: 77%
- Achieving and/or maintaining regulatory compliance: 77%

Overview

Situation

Challenge

Opportunity

Conclusion
Walking The Tightrope Between Security And Employee Productivity

Organizations are walking a tightrope in safely securing employees from external and internal threats while enabling them to be productive in the workplace. Too many authentication processes stifle employees from being efficient in their work, and IT decision makers (ITDMs) inhibit employees with poor background IT processes (59%). The inability to easily and securely share data (49%) further complicates this issue.

To compound the dilemma, not only do organizations agree they have ongoing issues with their restrictive ecosystem of applications (48%), but they’re also ill-suited for employee needs (46%). This all stems from inflexible IT processes (44%). Additionally, data center consolidation challenges include inadequate technology resiliency (30%), lack of in-house skills to successfully plan a move and legacy apps, and underlying infrastructure (26%).
The Case For Balancing EX And Security Controls

Organizations realize the importance of training and expertise for IT and security teams to understand what a security incident is and how to respond accordingly. Why? The threat landscape is always evolving, which is why 65% of respondents identified this as the top security challenge they face as an organization. Security is not a plug-and-play type function. It requires constant adjustment, innovation, and strategic focus to be tacitly successful.

Even though everyone recognizes the importance of the human element to security, employees tend to act unwisely and (un) knowingly invite threat actors into the business network. More than half (58%) of firms identify employee behavior as a security challenge. Business and IT leaders also recognize the importance — and challenge — of training staff and employees in compliance and relevant tools to use for their jobs (57%).

Which of the following are IT security challenges for your organization?

- Changing/evolving nature of IT threats (internal and external) (65%)
- Complexity of our IT environment (60%)
- Employee behavior (58%)
- Training staff/end users in compliance and tools (58%)
- Difficulty recruiting and hiring new staff (57%)
- Balancing employee experience and usability with security controls (57%)

Base: 887 Business and IT decision makers who are involved in decision making for laptops, computers and other devices

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2019
The Need For A Strengthened Security Infrastructure

According to Forrester’s research, most large enterprises still have a legacy infrastructure in place, which was never intended to connect with other systems¹. It’s no surprise that budgets for every type of security will increase over the next 12 months — including cybersecurity issues (52%), network security (48%), mobile security, (43%) and endpoint security (42%).

Technology that applies protections either directly to the data itself, the application that stores/provides access to data such as data loss prevention or database security are in high demand today.

However, operating with little or no internal support and lacking even minimal security controls can mean organizations often don’t have the expertise to completely understand.

How do you anticipate your security budget changing, for each of the following items, over the next 12 months?

<table>
<thead>
<tr>
<th>Item</th>
<th>Increase</th>
<th>Stay about the same</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security</td>
<td>52%</td>
<td>43%</td>
</tr>
<tr>
<td>Cloud security (IaaS, PaaS, SaaS)</td>
<td>49%</td>
<td>44%</td>
</tr>
<tr>
<td>Network security</td>
<td>48%</td>
<td>47%</td>
</tr>
<tr>
<td>Mobile security</td>
<td>43%</td>
<td>49%</td>
</tr>
<tr>
<td>Endpoint security</td>
<td>42%</td>
<td>51%</td>
</tr>
<tr>
<td>Security operations</td>
<td>42%</td>
<td>53%</td>
</tr>
<tr>
<td>Security analytics</td>
<td>40%</td>
<td>52%</td>
</tr>
<tr>
<td>IoT security</td>
<td>38%</td>
<td>54%</td>
</tr>
<tr>
<td>Risk and compliance</td>
<td>38%</td>
<td>56%</td>
</tr>
<tr>
<td>Application security</td>
<td>37%</td>
<td>56%</td>
</tr>
<tr>
<td>Security automation and orchestration technologies</td>
<td>32%</td>
<td>60%</td>
</tr>
</tbody>
</table>

Base: 887 Business and IT decision makers who are involved in decision making for laptops, computers and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2019
Champion Security And Productivity By Offering The Right Tools

Organizations must understand employee needs and how they get work done to mitigate security risks, improve collaboration, and boost employee experience (EX). Survey respondents looking to improve EX and productivity rank the ability to provide better devices (67%) and applications (67%) high on their agendas. Interestingly, organizations that enable employee workstyles from different locations are also enabling usability via less intrusive security controls (55%).

This is not to say that ITDMs have to relax their attitude toward security, but they must refine inflexible IT processes to better improve overall EX.

In fact, it’s interesting to note that while employees face various login challenges, IT prefers to work on enablers rather than solving the challenges. To succeed, IT must do both.

What would you like to do to help improve the employee experience and productivity? Select up to 5 in order

- Provide better devices for employees: 67%
- Provide better applications for employees: 67%
- Implement a faster device refresh cycle: 65%
- Improve help desk services: 59%
- Learn about approaches and successes from peers at other organizations: 55%
- Provide less intrusive security controls: 55%
- Provide single sign-on to applications: 53%
- Map employee journeys and personas: 41%
- Support BYOD and more variety of devices: 39%

Base: 887 Business and IT decision makers who are involved in decision making for laptops, computers and other devices

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2019
Trusted Partners Must Have Full-Scale, Easy-To-Manage, Integrated Security From End To End

Organizations that focus on security within their own organizations have a narrow lens to look through, which is why it’s important to increase their peripheral vision by leveraging outside help.

For a robust security infrastructure, organizations require partners that can provide security assurance (78%). Every organization has a different security composition from dedicated teams to entire departments to even a single entity running the show. Hence, it’s important for partners to provide tailor-based solutions according to the business type (76%). Other factors organizations look for in a partner include device expertise (74%) and a breadth of products and services (70%).

How important are each of the following as you consider partners to help your organization with your infrastructure needs?

- Security capabilities/assurance: 78%
- Ability to tailor based on business needs: 76%
- Industry expertise: 75%
- Device expertise: 74%
- Breadth of products and services: 70%

Overview

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY DELL | JULY 2019

Base: 887 Business and IT decision makers who are involved in decision making for laptops, computers and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2019
Conclusion

Organizations must consider the following:

- Understand how employees get work done, in order to provide the appropriate (and secure) tools to support productivity. Otherwise, people will find another way that may be less secure or go around security policies to do their jobs.

- Take a data-centric approach to data security. Bring controls closer to the data itself and protect the data wherever the business needs it to go. Enable secure collaboration, and secure remote work.

- Ensure that employees understand the value of data that they use to do their jobs and the value of that data to the business. This data awareness an important component of security and privacy awareness, so people know how to appropriately handle and use sensitive data as a part of their jobs.

Project Director:
Tarun Avasthy, Market Impact Consultant

Contributing Research:
Forrester’s Infrastructure and Operations research group
Methodology

This Opportunity Snapshot was commissioned by Dell. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of business and technology leaders. The custom survey began in February 2019 and was completed in April 2019.

Demographics

<table>
<thead>
<tr>
<th>REGION</th>
<th>POSITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA: 30%</td>
<td>C-Level: 13%</td>
</tr>
<tr>
<td>EU: 29%</td>
<td>VP: 19%</td>
</tr>
<tr>
<td>APAC: 31%</td>
<td>Director: 41%</td>
</tr>
<tr>
<td></td>
<td>Manager: 27%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIZE OF ORGANIZATION</th>
<th>RESPONSIBILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 to 499 employees: 68%</td>
<td>Final decision maker: 35%</td>
</tr>
<tr>
<td>500 to 999 employees: 32%</td>
<td>Part of a decision-making team: 37%</td>
</tr>
<tr>
<td></td>
<td>Department decision maker: 28%</td>
</tr>
</tbody>
</table>

ENDNOTES

1 https://www.forrester.com/report/Benchmark+Your+Cybersecurity+And+Privacy+Maturity+2019/-/E-RES144597