Remote Access and Security
Challenges & Opportunities
Remote Access Is Important and Growing

But How Secure Is It?
If more than 40% of breaches come from authorized users accessing unauthorized systems, why assume access can be trusted?

Q. To the best of your knowledge what percentage of major incidents or breaches were due to the following?

- From unknown origin
- Unauthorized entity gaining access
- Authorized contractor or vendor gaining unauthorized access
- Authorized employee gaining unauthorized access

N=304 Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
The need for remote access is growing.

Remote Access Employees & 3rd Parties **Tomorrow**

- Decrease and Don’t Know: 6%
- Stay flat/no change: 19%
- Increase 1% to 10%: 15%
- Increase 11% to 20%: 25%
- Increase 21% to 40%: 24%
- Increase more than 40%: 12%

Q. By what percent do you believe that the number of your organization employees and contractors who access applications remotely will increase or decrease in the next 12-24 months?

N=304  Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017

76% expect to increase remote access over next two years.
Security and simplifying user experience (UX) are top of mind for third-party vendors or contractors.

Q. Please rate the importance of the following when providing remote access to your third-party vendors or contractors.

Scale: 1 - Not very important  5 - Very important

N=304  Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
81% of respondents feel remote access is important for employees or staff productivity. Remote access security is top of mind for 83%.

Important Factors for Providing the Remote Access to Employees

- Enable working off-site: 70%
- Improve staff productivity: 81%
- Provide secure access: 83%
- Reduce operational costs: 78%
- Improve customer service with 3rd party vendors: 67%

N=304 Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
Budgets for remote access average 21% of IT spend. However, respondents who’ve experienced the most incidents from unauthorized entities gaining access only spend an average of 16%.
But Remote Access
Is Complex and Difficult
50%+ report they use more than 10 network and application components to add a new external user group to an organization.

Q. How many network and application components (HW and SW) are involved in adding a new external user group in your organization?
83% rated providing access to third-parties (e.g., contractors or supply chain partners) difficult to extremely difficult.

N=304     Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
From a technology standpoint...

VPN and Cloud tools are favored most by IT and Line of Business

VPN is the overwhelming choice favored

86%  20%  17%  48%  18%

VPN tools  ADC tools  WAF tools  Public cloud application directory tool  Others

N=304  Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017

However...
VPN is also linked to companies that have the **highest number of major incidents** from authorized and unauthorized employees, contractors and vendors gaining access.

### Percentage of Major Incidents on Different Tools to Provide Remote Access

<table>
<thead>
<tr>
<th>Tool Type</th>
<th>Most from Authorized Employee Gaining Unauthorized Access</th>
<th>Most from Authorized Contractor or Vendor Gaining Unauthorized Access</th>
<th>Most from Unauthorized Entity Gaining Access</th>
<th>Most from Unknown Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN tools</td>
<td>50%</td>
<td>4%</td>
<td>20%</td>
<td>0%</td>
</tr>
<tr>
<td>ADC tools</td>
<td>17%</td>
<td>5%</td>
<td>18%</td>
<td>0%</td>
</tr>
<tr>
<td>WAF tools</td>
<td>15%</td>
<td>4%</td>
<td>4%</td>
<td>0%</td>
</tr>
<tr>
<td>Public Cloud Application</td>
<td>16%</td>
<td>5%</td>
<td>20%</td>
<td>14%</td>
</tr>
<tr>
<td>Directory tools</td>
<td>39%</td>
<td>54%</td>
<td>50%</td>
<td>55%</td>
</tr>
<tr>
<td>Others</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

*Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017, N=304*
Security Is the Largest Concern with Remote Access
Security breaches rank highest in challenges faced with remote access.

**Challenging Factors When Providing the Remote Access**

- **Security breaches**: 56%
- **Compliance issues**: 44%
- **Complexity of architecture/integration issues**: 41%
- **Poor user experience**: 29%
- **Dedication of resources**: 29%

*Question: RANK 1&2 - Please rank the following in terms of how much of a challenge they are when providing remote access.*

*N = 304  Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017*
Over 50% of respondents agree that all aspects of securing remote access are difficult.

- Securing distributed apps is a problem: 59%
- Securing remote app access is a problem: 75%
- Company is vulnerable via unauth remote access: 57%
- Concerns about ability to secure/control 3rd party access: 59%
- Remote application access is extremely complex: 63%
- Contractor/3rd party access continuously monitored for threat: 68%
- Vendor/3rd party remote access are monitored for PCI DSS: 66%
- Malicious activity from 3rd party/contractors in found timely fashion: 69%
- Malicious activity can be thwarted in a timely fashion to avoid breach: 73%
- My organization has a formal program to access third-party risk: 68%
- IT monitors remote user activity and reports on which applications are accessed, by whom, for how long etc.: 64%

N = 304  Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
57% feel their company is vulnerable to an unauthorized remote access breach.

Q. My company is vulnerable to an attack through unauthorized remote access. Please indicate your level of agreement with each statement.
9.5% estimate frequency of major incidents or breaches their organization experiences is more than 10x a year

46% estimate frequency of major incidents or breaches their organization experiences is a few times a year

N = 304  Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
Most companies estimate major incidents or breaches have happened across all types of remote access (from employees, from third-party vendors and/or from unknown sources).

Q. To the best of your knowledge what percentage of major incidents or breaches were due to the following? (Responses, excluding “Don’t Know/Not Applicable”)

- None (0%)
- Some (1-50%)
- Most (51-500%)

N=304 Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
Most companies report that breaches happen a few times annually.

Q. Which of the following best estimates the frequency of major incidents or breaches your entire organization experiences?

- 10% More than ten times per year
- 46% A few times per year
- 22% Once every few years
- 18% Almost never
- 4% Don’t know

N = 304 Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
© IDC Visit us at IDC.com and follow us on Twitter: @IDC
Who's Got Secure Access?
Many organizations are confident they will avoid breaches by being proactive, **but...**

I am confident that all malicious activity (insider or through an external source) associated with remote access of 3rd party vendors and contractors is discovered in a timely fashion.

![Bar chart showing percentages of strongly agreed responses](chart.png)

- **Total:** 20%
- **Most from unauthorized employee gaining unauthorized access:** 31%
- **Most from unauthorized contractor or vendor gaining unauthorized access:** 0%
- **Most from unauthorized entity gaining access:** 10%
- **Most from unknown origin:** 18%
- **Don't know the distribution of source of breaches:** 21%
- **All others:** 21%

*Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017*

**None of the organizations** who had experienced most incidents from an authorized contractor or vendor gaining unauthorized access believed that they could **discover it quickly**.
Poor remote access security is costly.

Amount of Losses or Expectation of Losses due to Unauthorized Access to Remote Applications

- **Average**: $6.5M
- **500-999 employees**: $3.7M
- **1000-4,999 employees**: $7.3M
- **5000+ employees**: $7.5M
- **1 to 49 3rd party vendors**: $4.2M
- **50 to 99 3rd party vendors**: $6.3M
- **100+ 3rd party vendors**: $8.2M

N=304  
Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017

Average expected loss is $6.5M with greater loss expected by larger companies ($7.5M) and those with more third-party vendors ($8.2M).
Organizations who believe most strongly that malicious activity can be thwarted once discovered experienced the greatest financial loss due to unauthorized access to remote applications.

Q. Which of the following best estimates the financial amount your entire organization loses or expects to lose on average due to unauthorized access to remote applications?
IT is more pessimistic than LOBs about security losses.

IT respondents estimate losses to be 74% higher than LOB estimates ($7.5M vs. $4.3M)

Source: Remote & Secure Access User Requirements Survey, IDC, April, 2017
What’s Needed?

Businesses must **pivot from** the common security mantra of “trust but verify” to “verify and never trust” in the new threat landscape. Traditional access solutions grant users full access to the network once they “verify” through user credentials, but is that the most secure approach? Solutions like VPNs put a hole through your firewall, enabling anyone inside of your perimeter to potentially move laterally across your network.

It’s time for a radically new approach to application access that is simple to use and more secure. Learn more » [www.akamai.com/eaa](http://www.akamai.com/eaa)