

The State of Employee Trust

Zero Trust is only for data,
not employees

Volume 1

Table of contents

03 **Foreword**

04 **Key takeaways**

05 **Results and analysis**

05 High levels of trust are rare

06 Trust changes over time

07 Trust extended to employees returns
high value

08 **Conclusion and recommended actions**

09 **About Cerby**

10 **Methodology**

Foreword

In January 2022, the White House issued a memorandum setting forth the Federal Zero Trust architecture strategy, igniting worldwide implementation efforts for governments and businesses alike. And for a good reason: when appropriately implemented, a Zero Trust strategy reduces the cost of security breaches by 43%¹. However, an interesting contrast exists for those in security and IT: Zero Trust is quite popular, but can the same principles of trust that succeed in securing data, applications, assets, and services (DAAS) apply as well to employees? The simple answer is no.

Our research sought to discover the most practical ways employers can gain employee trust moving into 2023, and the results surprised us. **If empowered to choose the applications they use for work, 39% of employees said they would be willing to take a 20% pay cut.** This finding sheds light on what many employers fail to realize: *applications are intimately tied to how people get their work done and their job satisfaction level.*



If you remember one thing after reading this report, let it be this: when it comes to your data, assets, applications, and services, aim for Zero Trust. But when it comes to your employees, high levels of human trust should be the goal. To quote famed investor Warren Buffett, “Trust is like the air we breathe: when it is present, nobody really notices. But when it’s absent, everybody notices.”

Matthew Chiodi
Chief Trust Officer

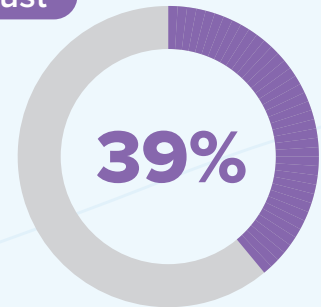
¹“Cost of a Data Breach Report,” IBM Security, 2021, <https://www.ibm.com/downloads/cas/OJDVQGRY>

Key takeaways

Employee freedom to choose applications builds human trust

39% of employees said they would take a 20% pay cut for the ability to choose the applications they need to accomplish their goals at work.

Most employees associate autonomy in choosing the tools, technologies, software, and applications they need to get their work done with elevated levels of job performance, job satisfaction, and happiness. In fact, decision-making rights over which applications to use contribute more to increased performance at work than financial rewards and positive feedback from superiors.

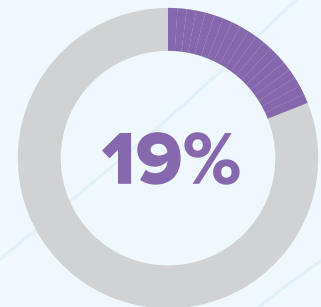


Would take a 20% cut in pay for the ability to choose their applications

Zero Trust policies are only for applications and data

19% of employees immediately ignore application “blocks” and still use the applications they want, according to our previous research, *State of Employee Choice*.

Organizations should seek to balance high trust in employees and Zero Trust principles for data, applications, assets, and services (DAAS). Attempting to rely on security tools that block and prevent employees from using anything but IT-sanctioned applications continues to fail as employees ignore the rules or find workarounds to imposed policies. This calls for a new enrollment-based approach to security that balances trust-positive initiatives, like employee application choice, with cybersecurity and compliance requirements.

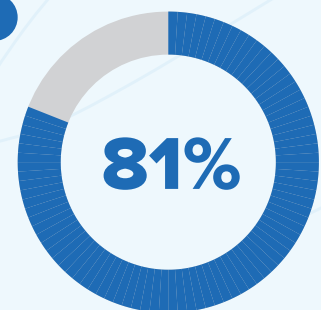


Still use "blocked" applications

High employee trust yields better outcomes for everyone

81% of employees felt increased energy, happiness, productivity, and contribution when employers demonstrated trust.

Every organization should aspire to a high trust relationship with employees because the most sought-after outcomes in organizational life flow from high levels of employee trust. Higher quality products, improved innovation, and increased growth and profitability are vital outcomes when companies demonstrate high trust towards employees.



Felt increased energy when trusted by employers

Results and analysis

High levels of trust are rare

A 2021 study by Atlas Technology Solutions² studied HR complaints, employee monitoring, and Google search trends and discovered an increasing need for more trust between employees and employers. While most leaders believe that a lack of trust threatens their organization's growth, most have done little to increase trust, mainly because they are unsure where to start. Perks to garner employee satisfaction are limited to foosball tables, sleep pods, tai chi classes, and gourmet foods. These can boost workplace satisfaction in the short term, but they don't enhance trust, nor have they had a lasting effect on long-term retention or performance. The workplace has become increasingly complex since the pandemic, with many offices striving to nurture employee satisfaction in ever-changing in-office, hybrid, and remote scenarios.

Research by Rebecca Johannsen and Paul J. Zak at Claremont Graduate University³ shows that an employee-centric culture of trust generates a meaningful difference in businesses: higher productivity, a more energized work environment, better collaboration amongst colleagues, higher engagement, better products, innovativeness, and increased profitability. Employees stay with their employers longer than people working at low-trust companies. Trusted employees suffer less chronic stress and are more positive and happier with their lives, leading to more robust performance.

But the question remains: Where to start? **The first thing to remember about human nature is that extremely high levels of trust are rare.** Our research found that only 14% of employees and managers state they have extremely high trust for other people. 20% trusted their current employer to treat them fairly and 23% said that their employer trusts them. **When only 23% of employees feel a high level of trust, it's indicative of corporate cultures where burnout is the norm and employees feel stifled.** See Figure 1.

Figure 1. Extremely High Levels of Trust: Three Perspectives
Percentage of respondents



² "HR Complaints and Monitoring," Atlas Technology Solutions, 2021, <https://www.atlashxm.com/resources>

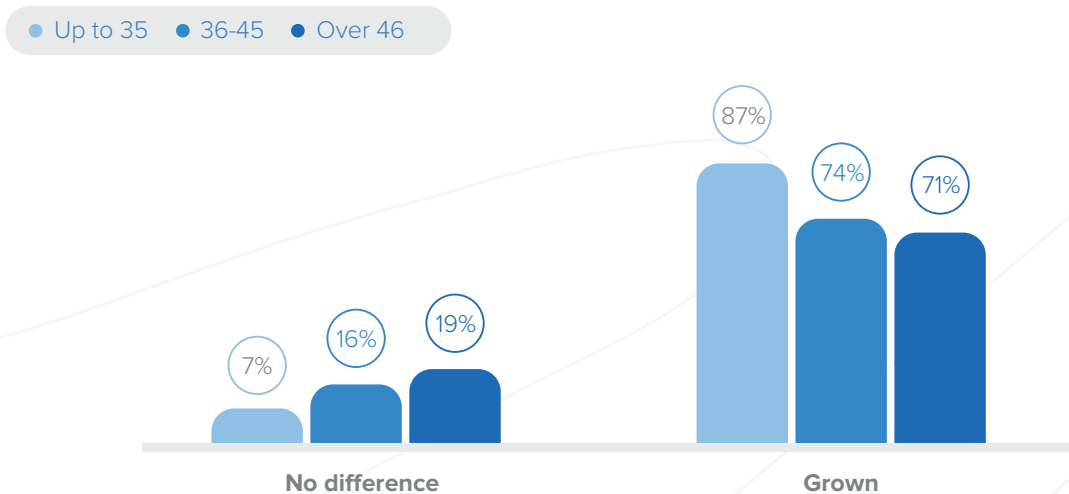
³ "The Neuroscience of Organizational Trust and Business Performance," Rebecca Johannsen & Paul J. Zak, 2021, <https://philpapers.org/rec/JOHTNO-15>

Trust changes over time

Trust is not static. Most of those we spoke with said trust in their employer had grown compared to jobs held earlier in their careers. The most significant growth in trust is among employees and managers aged up to 35 years (87% said their trust had grown, and only 6% said it had diminished). See Figure 2.

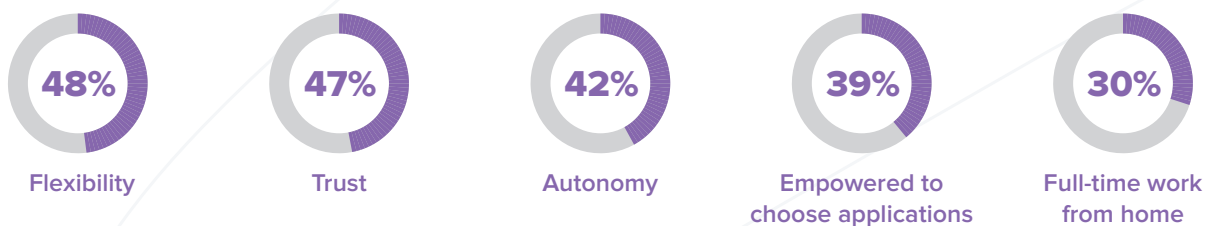
In the more seasoned age brackets, fewer of those we spoke with said their trust had grown. This indicates a greater range of work experiences, roles at good and bad employers, and harsh economic cycles when employers often take drastic actions. **The longer employees work, the more jaded they become.** Your seasoned employees will require more effort to convince them they are trusted. Why is this so important to accomplish for all employees? **Employees rank trust and other factors as more important than financial compensation.**

Figure 2. How trust in employers changes over a career
Percentage of respondents



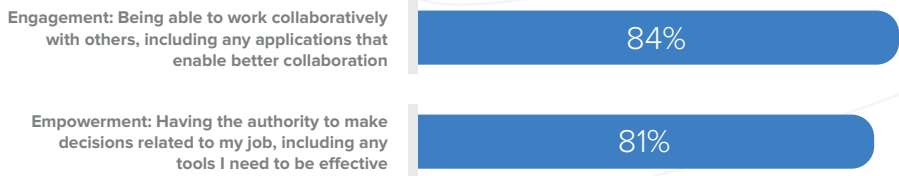
Specifically, **47% of employees and managers say they would take a 20% pay cut in return for higher trust from their employer.** The three other characteristics most valued by employees were flexibility (48%), autonomy (42%), and being empowered to choose the applications needed to work effectively (39%). This last statistic might be shocking for leaders. **Could allowing employees the freedom to choose the applications they use for work significantly impact trust?**

Figure 3. What employees would exchange for a 20% cut in pay
Percentage of respondents



Our research shows that employers need to significantly improve two closely related factors: engagement and empowerment. These factors deliver the hat trick of high job satisfaction, high happiness, and low stress. See Figure 4.

Figure 4. Importance of factors for job satisfaction, happiness, and low stress
Percentage of respondents indicating “high importance” or “extremely important”



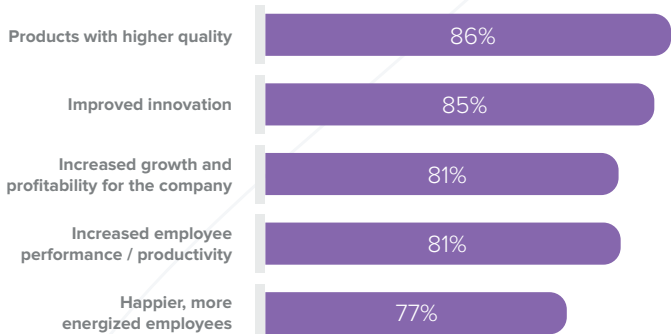
Notice the tight correlation between engagement and empowerment. Employees want to collaborate with others and be able to choose the applications they use for work.

Trust extended to employees returns high value

What do organizations get when they demonstrate trust toward employees? The returns are visible in a flow of highly valued outcomes for the organization, its customers, and its employees. As shown in Figure 5, outcomes include:

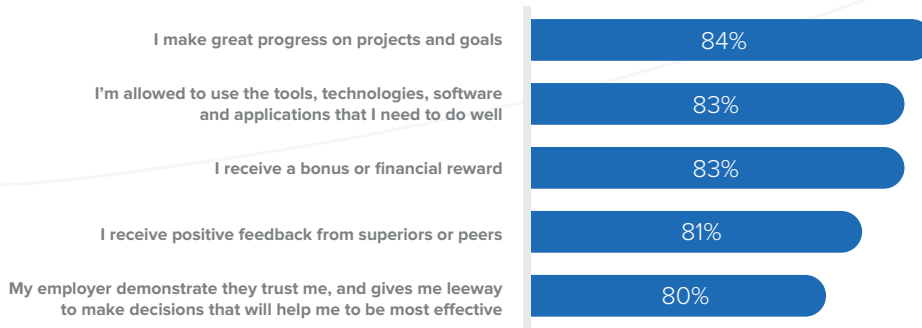
- Improved market standing for the organization due to higher quality products and improved innovation, which flows through to increased growth and profitability. Increased employee performance and productivity also drive growth and profitability.
- Customers gain access to higher quality products and improved innovation in products and services. Customers engage with happier, more energized employees.
- Employees achieve increased energy, happiness, productivity, and contribution when employers demonstrate trust.

Figure 5. Impact of trust demonstrated towards employees
Percentage of respondents indicating “high impact” or “extreme impact”



Productivity, growth, employment longevity, and engagement are also considered critical to high performance at work. Making progress on projects and goals—the productivity and growth factors—has the highest impact on performance. Closely, the second event that enables high performance is the freedom to use the applications that employees believe they need (which is one part of the engagement factor above). **Employees rank the freedom to choose applications at work higher than receiving a bonus or financial reward.** It is also ranked higher than receiving positive feedback from superiors or peers. See Figure 6.

Figure 6. Impact of events on increasing performance at work
Percentage of respondents indicating “high impact” or “extreme impact”



Conclusion and recommended actions

The research is clear for leaders who want to build high-performance organizations for shareholders and employees: **Zero Trust is only for applications and data, not employees.** Organizational leaders must take tangible steps to build trust daily if they want the highest quality products, continuous improvement, and innovation.

What does this look like, practically speaking? Douglas Conant, the former CEO of Campbell Soup Company, provides three steps⁴: declaring intent, demonstrating respect, and delivering results.

Declaring intent is an action leaders can take where they verbalize the why behind their actions. It must be genuine and benefit both the leader and the employees. A great example is when security and IT teams roll out new tools. They often do it without the required two-sided explanation: yes, it will help the company be more secure, but what’s in it for the employee? How will it help them be more productive?

Demonstrating respect is something IT and security leaders can do to empathize with the challenges employees regularly face when it comes to security controls. In previous research on the [State of Employee Choice](#), we found that over half of employees wanted their IT and security departments to “get out of the way” when selecting and using applications for work. When combined with the 61% of employees who said they’d experienced a preferred application being blocked, it’s no wonder 60% of employees said the blocks negatively affected how they felt about their company. Demonstrating respect and growing trust will require security and IT teams to revisit many security tools used in most enterprises. Typically, an overreliance exists on enforcement-based controls that take heavy-handed approaches, for example, blocking, banning, and denying employee use of certain preferred applications. This approach

⁴“The Connection Between Employee Trust and Financial Performance,” Stephen M. R. Covey and Douglas R. Conant, 2016, <https://hbr.org/2016/07/the-connection-between-employee-trust-and-financial-performance>

erodes employee trust. On the other hand, enrollment-based controls take a different approach and incentivize employees to make security-conscious decisions because the tools help the employees be more productive. Enrollment-based controls have something in it for both the employee and employer. Application blocks and bans interfere with employee autonomy and undermine trust—which can negatively affect job satisfaction and performance. *Ironically, this approach will likely lead to a Zero Trust relationship with employees that couldn't be further from what employers need heading into a possible economic downturn.* More companies are recognizing this and are taking a business-led IT approach, giving business units the freedom to choose their preferred applications while keeping security and privacy in check.

Finally, **delivering results** requires leaders to consistently and confidently make good on their words. In terms of building trust with employees, this means backing up words with substance. “Delivering results in a way that builds trust is more than just accomplishing tasks—it’s doing the right thing, in the right way, for the right reasons, in the way that you said you would.”⁴ This step is best accomplished by setting specific goals and consistently doing the things you declared.

Security and IT teams might set a goal to reduce risk from applications that don’t support enterprise-grade security features like single sign-on (SSO). These applications often fall into the categories of shadow IT and/or “unmanageable applications,” and many employees use them without approval or IT and security governance. Outright bans of these applications don’t work, so delivering results might look like deploying a solution that harmonizes employee application choice and employer priorities such as security and compliance.

In short, the right solution to shadow IT and unmanageable applications works with end users, not against them. This approach increases employee trust and supercharges productivity while automating and ensuring security.

Ready to empower your employees and build trust?

Cerby makes it easy to build trust with employees by empowering them to choose the applications they need to get their work done. Cerby balances employer priorities such as security and compliance by automating error-prone manual processes, like 2FA enrollment, and connecting non-SAML/SCIM supporting applications to corporate identity providers like Okta and Azure Active Directory. To get started with Cerby, visit us at cerby.com and request a demo.

About Cerby

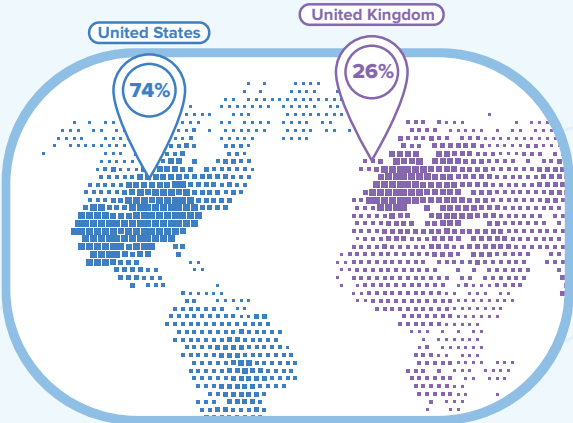
Cerby delivers the world’s first user-driven security platform for unmanageable applications by automating manual processes, uncovering security issues, and empowering users to implement Zero Trust principles. Our proprietary technology uses robotic process automation to understand applications in a business context and automatically enforces security best practices before vulnerabilities and misconfigurations become breaches. Cerby is a must-have for technology executives and their teams to protect the brand, stay secure, and increase productivity.

Since Cerby released its platform in 2022, it has helped clients like Fox, News Corp, L'Oréal, and Dentsu fix common application liabilities efficiently while facilitating collaboration. Our last investment round was led by Ridge Ventures, with participation from Founders Fund, Okta Ventures, Salesforce Ventures, A.Capital, Bowery Capital, AV8, Vela Partners, Carnrite Ventures, and Incubate Fund. Visit us at cerby.com and follow us @CerbyHQ on Twitter.

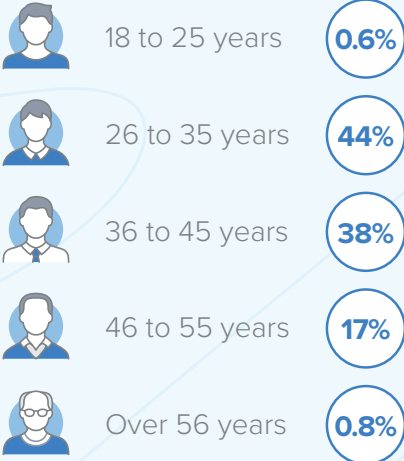
Methodology

Cerby conducted this study in partnership with Osterman Research in late 2022. Over 500 employees and managers in the United States and the United Kingdom were interviewed on trust, empowerment, autonomy, using preferred applications at work, and cybersecurity practices.

Geography



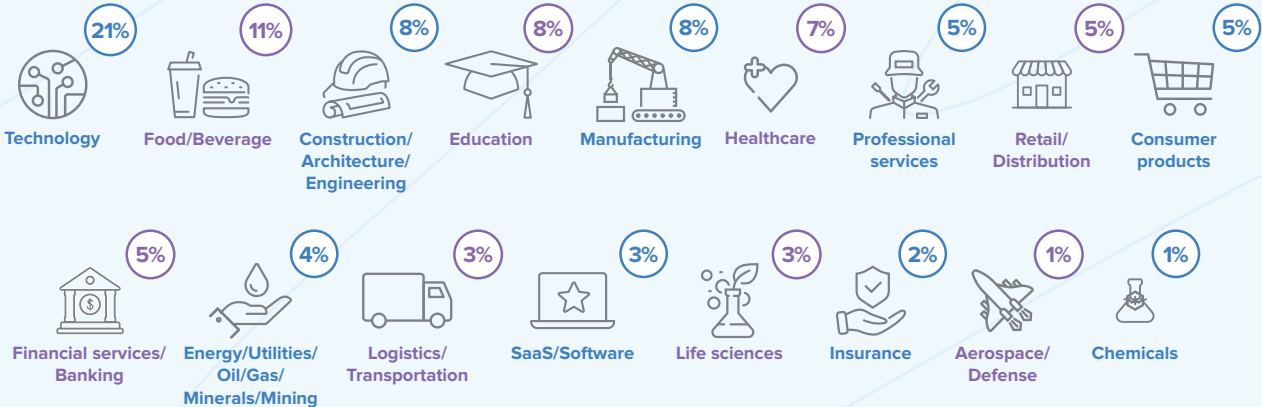
Age



Annual Revenue



Industry





Visit us at [Cerby.com](https://cerby.com) and follow us [@CerbyHQ](https://twitter.com/CerbyHQ) on Twitter.

