Riscosity

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Financial Services And Software Supply Chain Attacks

A Whitepaper By Riscosity

The Weakest Link: Financial Services and Software Supply Chain Attacks

Riscosity Research
research@riscosity.com

[1] ***Abstract*—** According to the Verizon 2023 Data Breach Investigation Report (DBIR) [1], financial motives drive 94.6% of breaches. Moreover, breaches are only one factor in this sinister equation: ransomware is another major concern, and often these two go hand in hand. According to a recent Apple-commissioned report [2], ransomware attacks increased by nearly 70% in the first nine months of 2023 compared with the same time period last year. Overall, more ransomware attacks were reported from January to September 2023 than in all of 2022. Considering the obvious link between attackers' motives and the core asset of the Financial Services (FS) industry, the targeting of FS firms is expected. This paper looks at the FS industry through the lens of third-party risks, specifically on how the threat vector of software supply chain attacks are leveraged by threat actors. Readers of this paper will understand how dependent FS firms are on third parties, and consequently, how vulnerable they are to risks in the software supply chain. The goal of this paper is to equip the readers with the tools that allow them to measure and reduce such risks via third party data observability.

I. INTRODUCTION

This paper analyzes the third-party risk environment for Financial Services organizations, specifically within the software supply chain, in order to help educate industry professionals about the different possible business impacts and how to address them.

The computer is ubiquitous in the modern world, and no industry can consider itself impervious to it. The FS industry is no exception. While traditionally known for documenting facts and figures on paper, the industry has transitioned to electronic ledgers and online fund transfers. While digitization has resulted in improved efficiencies, it has exposed FS organizations – both legacy banks and new-age fintech firms – to cybersecurity threats.

This problem, specifically, third party data observability (TPDO) is compounded by the use of third-party products and services, over which the customer organization often has little control and oversight. Considering technology is not a financial capability, many FS organizations have adopted this new paradigm. However, this dependence on services outside the FS core ecosystem has resulted in a significant increase in risks that originate from those external parties.

Combining the elements of third-party dependencies and cybersecurity threats results in the specific attack vector of software supply chain attacks. This is the medium through which cybercriminals are increasingly targeting FS firms to exfiltrate sensitive information or encrypting it, to be rendered accessible only on the payment of ransom. Once considered a niche method, software supply chain attacks gained notoriety with the SolarWinds incident in 2020 and have continued to harm organizations big and small alike (three major incidents in just 2023 Q2 – 3CX, PyPI and MOVEit).

II. THE MAGNITUDE OF THE PROBLEM

In June 2023, the US Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC), issued final guidance [3] for banking organizations on managing risks in third party relationships.

The document recognizes the value of using third parties – "can offer banking organizations significant benefits, such as quicker and more efficient access to technologies, human capital, delivery channels, products, services, and markets". At the same time, it makes it clear where responsibility lies – "the use of third parties does not diminish or remove banking organizations' responsibilities to ensure that activities are performed in a safe and sound manner and in compliance with applicable laws and

[1]

regulations". To put it simply, if the third party makes a mistake in handling a bank's customers' data, the bank is still held liable.

Considering the above, recent events give FS organizations justifiable cause for concern. According to a 2023 report [4] by data science firm Cyentia Institute, based on analyzing data provided by risk-management firm SecurityScorecard, 98% of 230,000 organizations surveyed had at least one third party partner who had suffered a breach.

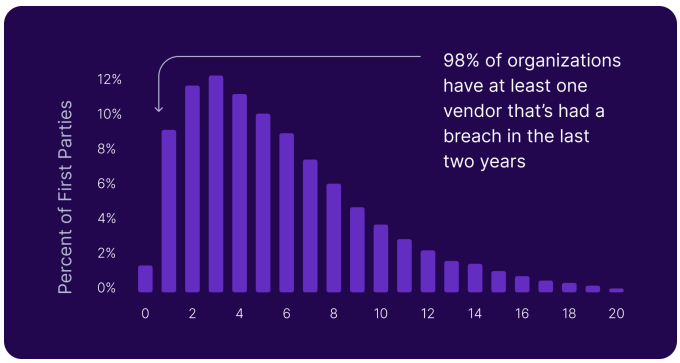

Figure 1: Third parties with a breach in last 2 years
(Source: [5])

Specifically for software supply chain risks, a report published in the aftermath of the SolarWinds attack clearly illustrates the magnitude of the problem. While the numbers may be skewed by the 18,000+ organizations affected during this specific attack, the broader point of this attack vector is evident.

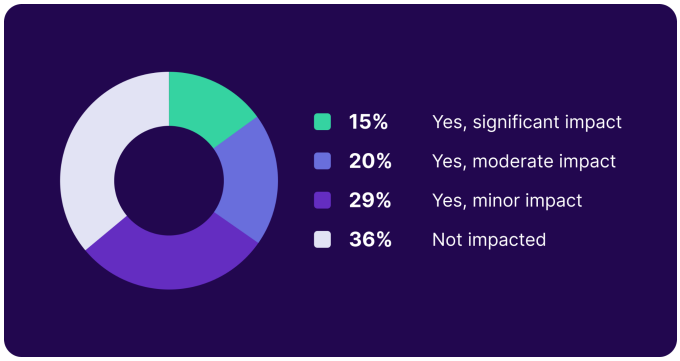

Figure 2: Affected by software supply chain attacks in last 12 months
(Source: [6])

A silver lining in the report is the respondents' acknowledgement of the validity of software supply chain risks and the desire to address them on priority. The important question to ask is, whether they have the right tools for the job.

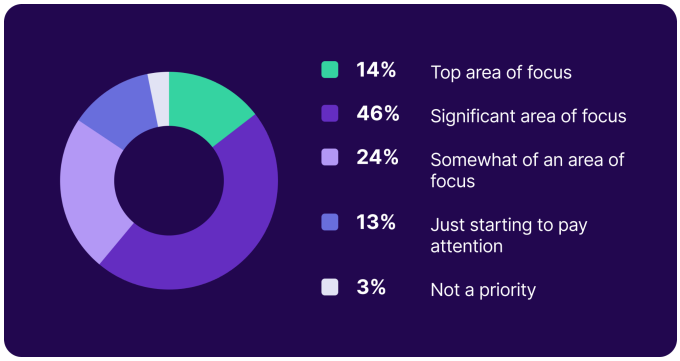

Figure 3: Focusing on software supply chain security
(Source: [6])

While SolarWinds was a watershed moment in software supply chain security, it was not an isolated incident. Software supply chain attacks, and as a result TPDO challenges, have been increasing every year for the last few years. In fact, a lot of this increase can be attributed to the growing use of open-source software (OSS). In 2022, there was a 742% year-over-year increase in OSS supply chain attacks, aimed at exploiting any weaknesses in upstream open-source ecosystems, such as JavaScript, Java, .NET, and Python [7]. In 2021, the figure was 650%, and 430% the year before. As is evident, this is a problem that is persistent and growing.

Last year, Gartner identified digital supply chain risk as one of seven top security trends [8]. Gartner predicted that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

The increase in software supply chain attacks is driven not only by its success, but its success relative to its cost. Unlike a targeted attack on a specific organization that requires time-consuming reconnaissance and expensive exploit build in the hope that such an attack is successful, a software supply chain attack depends on the popularity of the underlying software for its success. By targeting a vendor or supplier, attackers can gain access to many potential victims, as well as valuable information about their targets. This is akin to a burglar targeting a lock manufacturer and installing a weakness in the product such that any future users

are left exposed to a weakness that only the burglar knows about and can potentially exploit.

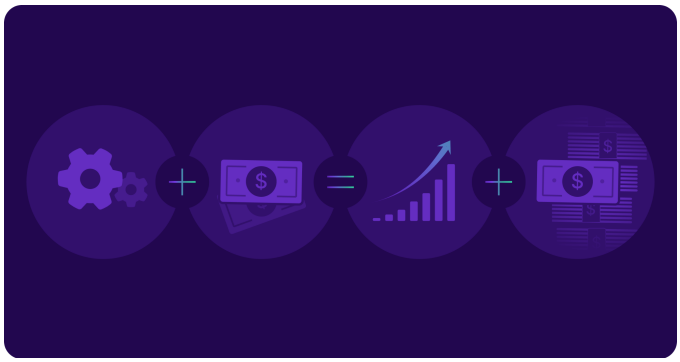

Figure 4: The Economics of Software Supply Chain Attacks
(Source: Self-made)

If the three parameters used to evaluate an attacker – motivation, opportunity, and capability – are considered, two are found to be higher than the third for FS software supply chain risks. With respect to "motivation", or what an attacker seeks to achieve, this is extremely high considering these entities typically deal with high-value information (personally identifiable information, financial information). As the 2023 Verizon Data Breach Investigation Report (DBIR) reveals, financial motives drive 94.6% of breaches [9]. The very nature of software supply chain attacks renders the "opportunity" argument moot; due to the popularity of the software, opportunities for a successful attack are plenty. Finally, on the subject of "capability", while there is a barrier to entry versus leveraging a simpler attack vector like phishing, as long as the economics make sense, these attacks will continue.

III. THE MECHANISM OF SOFTWARE SUPPLY CHAIN ATTACKS

The Cybersecurity and Infrastructure Security Agency (CISA) of the United States Department of Homeland Security (DHS) defines a software supply chain attack as "when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers" [10]. However, there are different ways by how such attacks are executed, as evidenced in the following events:

- **Hijacked Update: SolarWinds**
  This attack took advantage of the fact that most software products receive regular updates from providers. The SolarWinds Orion platform is widely used to monitor IT infrastructure. In 2020, attackers managed to inject malicious code into genuine software that was then distributed to SolarWinds customers as an update. The same mechanism was employed in the more recent 3CX hack of 2023.

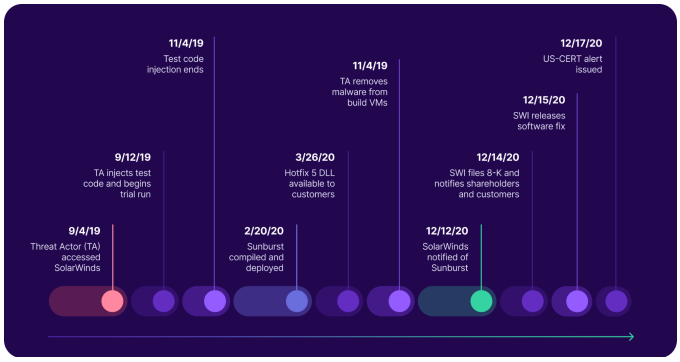

Figure 5: SolarWinds Attack Timeline
(Source: [11])

- **Undermined Codesigning: Mimecast**
  Codesigning is used to validate the identity of the code's author and the integrity of the code. By undermining the process, attackers can impersonate providers and distribute malware as genuine updates. In the 2021 Mimecast incident, attackers compromised the security certificate that authenticated the Mimecast service on Microsoft 365 Exchange Web Services.

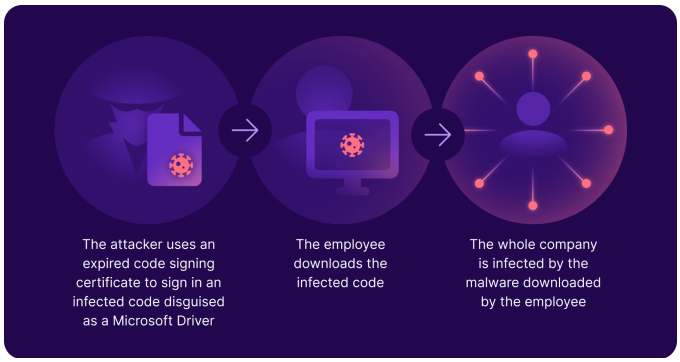

Figure 6: Code Signing Attack
(Source: [12])

- **Compromised Open-Source Software: PyPI**
  PyPI or the Python Package Index is the official software repository for the popular

programming language Python and has over 700,000 users working across 450,000 projects. Such a large user base made it an attractive target for attackers to implant malicious packages that may then end up being used by developers, thereby rendering their own code vulnerable. In 2023, several researchers found many such packages, impersonating real libraries, in PyPI. This is a clear example of a TPDO risk - injected malware in PyPI packages that lead to the silent exfiltration of company data.

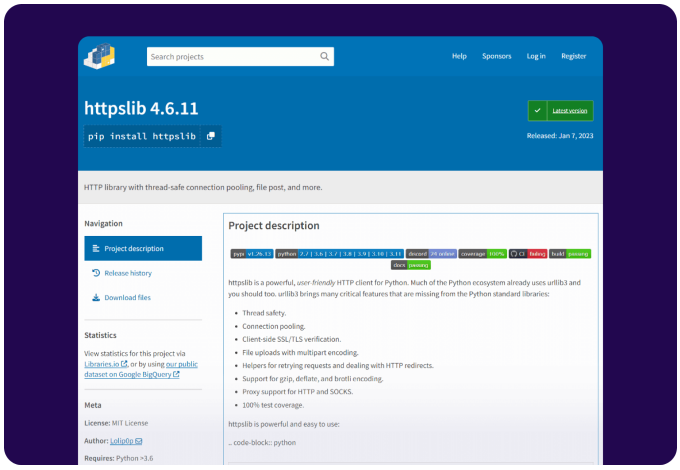

Figure 7: Malicious PyPI Package
(Source: [13])

IV. THE IMPACT OF AN INSECURE SOFTWARE SUPPLY CHAIN

For a FS firm, an insecure software supply chain can have manifold adverse impacts. These can be broadly categorized as:

A. Regulatory

The FS industry is perhaps regulated more than any other industry in the United States. Such regulations include Gramm-Leach-Bliley Act (GLBA), SEC Cybersecurity Rule, CFPB, FINRA, and Sarbanes-Oxley (SOX). Some of them have specific third-party risk management requirements that may be violated by an insecure software supply chain.

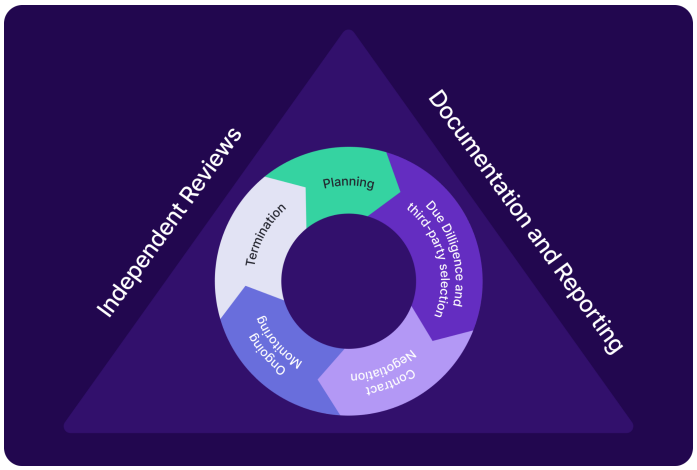

Figure 8: Stages of the Risk Management Life Cycle
(Source: [14])

B. Financial

In addition to the above, FS firms are also liable for privacy violations of customer data. While federal privacy regulation akin to EU GDPR does not exist in the US yet, FS firms with customers in the twelve states that have passed privacy legislation – California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia – can receive significant monetary penalties if an insecure software supply chain leads to a breach of personal data.

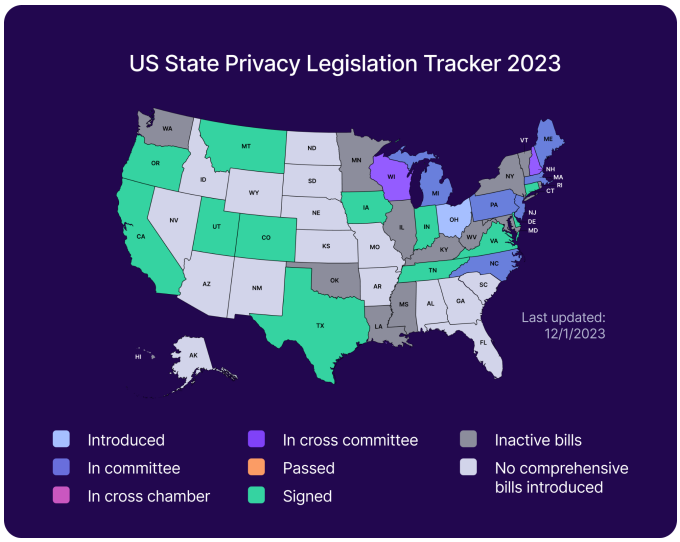

Figure 9: US State Privacy Legislation
(Source: [15])

C. Legal

FS firms can be sued by their end clients for falling victim to a software supply chain attack in case their personal information is stolen, or funds are restricted. Also, not ensuring a secure software supply chain may be against the terms of the contracts they sign with their partners or cyber insurance providers.

D. Reputational

FS firms are possibly more dependent on their reputations than organizations in any other industry. Trust is a very important asset for any organization that handles people's money. Any software supply chain attack at a FS firm that results in a data breach or unavailable services can adversely affect its reputation and threaten its business viability.

Figure 10: Cost of Bad Reputation
(Source: [16])

V. THE SOLUTION

The problem of software supply chain attacks is not something a customer organization can easily solve. This is because they have limited control over what the provider does. However, with the following controls, FS firms can significantly reduce the risk:

- **Pre-deployment diligence**
  FS firms looking to purchase and deploy a third-party software product or service should perform their due diligence. The provider should be able to provide evidence of the following:
  - Observation of Secure Software Development Life Cycle (SSDLC) practices such as developer training, static and dynamic testing, separation of test and production environments, etc.
  - Performance of independent external security audits
  - Existence of a software bill of materials (SBOM) that articulates the components and other attributes of the software product

- **Secure deployment**
  Once diligence has been performed and the software provider selected, the customer FS firm should require the following for deployment:
  - The software should be granted the least privileged access that is required to function properly
  - Software integrity checking via common code authentication mechanisms must be supported
  - Software updates and patches should be deployed in a test environment first before being rolled out to Production
  - All transactions should be logged in immutable form

- **Post-deployment monitoring**
  The FS firm's responsibility does not end with deployment but continues with monitoring the software in action. However, this is often the weakest link in the software supply chain.
  - Conducting regular audits of provider's security program.
  - Obtaining full observability into third party data flows, essentially sunsetting the entire TPDO risk spectrum.

VI. CONCLUSION

Software supply chain attacks are increasingly year over year. Even with the relatively higher level of effort required to execute such an attack, the potential return on investment, especially with FS firms, makes this an attractive attack vector for bad actors. Even with limited control over software providers' security processes, there are several

controls customer organizations should look to implement. In general, while FS firms are diligent before and during deploying third party software, such rigor is absent post deployment. Even if contract terms allow FS firms to audit providers' security programs, they usually lack visibility into how providers handle their data.

A platform like Riscosity can empower a FS firm to achieve full third-party data observability (TPDO) where all data flows to and from their environment can be scrutinized in detail and potential security concerns (transit to high-risk countries, high volume, etc.) can be flagged, or even blocked. Not only is Riscosity the most advanced solution in the market available to address this pressing need, but it is also integrated seamlessly on existing technology stacks. Customers start seeing value immediately after a 20-minute deployment, with risks further minimized via a weeklong Proof of Concept (PoC).

ACKNOWLEDGEMENT

The authors would like to acknowledge the guidance provided by Riscosity's advisors.

- **Anand Singh: CISO, Alkami Technology Inc. (NYSE: ALKT)**
- **Rich Watson: Proprietor, Intrepid Cybersecurity**
- **Prasad Ramakrishnan: CIO, Freshworks (NYSE: FRSH)**

Finally, the authors would like to credit Riscosity's FS clients for their feedback that provided key insights into their environments, business needs and technology risks. These insights contributed towards this paper and building a better platform responsive to FS use cases.

REFERENCES

[1] Verizon (2023). *2023 Data Breach Investigations Report.* [Online]. Available: https://www.verizon.com/about/news/2023-data-breach-investigations-report. [Accessed: 1-Jul 2023].

[2] Apple, Prof. Stuart E. Madnick (2023). *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase.* [Online]. https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf. [Accessed: 7-Dec 2023].

[3] FDIC, FRB, OCC. (2023). *Final interagency guidance.* [Online]. Available: https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf. [Accessed: 3-Jul 2023].

[4] Security Scorecard. (2023). *Close Encounters of the Third- (and Fourth) Party Kind.* [Online]. Available: https://securityscorecard.com/blog/close-encounters-of-the-third-and-fourth-party-kind-blog/. [Accessed: 3-Jul 2023].

[5] Dark Reading. (2023). *Nearly All Firms Have Ties with Breached Third Parties.* [Online]. Available: https://www.darkreading.com/cloud/nearly-all-firms-have-ties-breached-third-parties. [Accessed: 3-July].

[6] Anchore. (2022). *Survey of Large Enterprises Shows 64 Percent Affected by a Software Supply Chain Attack in the Last Year.* [Online]. Available: https://www.prnewswire.com/news-releases/survey-of-large-enterprises-shows-64-percent-affected-by-a-software-supply-chain-attack-in-the-last-year-301314327.html. [Accessed: 10-July].

[7] Statista. (2023). *Year-over-year (YoY) increase in open source software (OSS) supply chain attacks worldwide from 2020 to 2022.* [Online]. Available: https://www.statista.com/statistics/1268934/worldwide-open-source-supply-chain-attacks/. [Accessed: 10-July].

[8] Gartner. (2022). *Gartner Identifies Top Security and Risk Management Trends for 2022.* [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022. [Accessed: 16-July].

[9] Verizon. (2023). *Data Breach Investigations Report.* [Online]. Available: https://www.verizon.com/business/resources/infographics/2023-dbir-infographic.pdf. [Accessed: 11-July].

[10] CISA. (2021). *Defending Against Software Supply Chain Attacks.* [Online]. Available: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf. [Accessed: 11-July].

[11] Krebs On Security. (2021). SolarWinds: What Hit Us Could Hit Others. [Online]. Available: https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/. [Accessed: 11-July].

[12] Code Signing Store. (2021). *Code Signing Certificate Expired? Here's What This Means for Your Business.* [Online]. Available: https://codesigningstore.com/what-happens-when-code-signing-certificate-expires. [Accessed: 17-July].

[13] Fortinet. (2023). *Supply Chain Attack Using Identical PyPI Packages, "colorslib", "httpslib", and "libhttps".* [Online]. Available: https://www.fortinet.com/blog/threat-research/supply-chain-attack-using-identical-pypi-packages-colorslib-httpslib-libhttps. [Accessed: 16-July].

[14] Federal Register (2023). Interagency Guidance on Third-Party Relationships: Risk Management. [Online]. Available: https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management. [Accessed: 2-Nov].

[15] International Association of Privacy Professionals, Andrew Folk (2023). *US State Privacy Legislation Tracker.* [Online]. Available:

https://iapp.org/resources/article/us-state-privacy-legislation-tracker/. [Accessed: 7-Dec].
[16] SEO For Growth (2023). *How a Bad Reputation Can Cost You Money*. [Online]. Available: https://seoforgrowth.com/how-a-bad-reputation-can-cost-you-money/. [Accessed: 2-Nov].

ABOUT RISCOSITY

Our mission is to secure data in transit.

We've built Riscosity to solve a critical business problem – there's no easy way for companies to protect all sensitive data-in-transit. More than ever, companies today rely on multiple 3rd party services. Individually securing outbound data transfers is an onerous, often manual process, that is error prone. Riscosity offers an automated, comprehensive solution that seamlessly integrates with a customer's tech stack. Our goal is simple – we want teams to never worry about sending the wrong data to the wrong endpoint, ever again.

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Highly Automated, UserFriendly and scalable solutions. Our robust solutions include Comprehensive Email Security with Anti-Phishing Protection and Training, Automated Patching and Endpoint Management, Asset Risk Visibility and Management with Policy Enforcement (ARM), Secure Agentless Multi-Browsing with ZTNA, Third-Party Data Flow Security solutions to assess and mitigate all known and shadow assets and an Online Gamified Simulation Platform for Cyber Security Training.

.

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Highly Automated, UserFriendly and scalable solutions. Our robust solutions include Comprehensive Email Security with Anti-Phishing Protection and Training, Automated Patching and Endpoint Management, Asset Risk Visibility and Management with Policy Enforcement (ARM),Secure Agentless Multi-Browsing with ZTNA, Third-Party Data Flow Security solutions to assess and mitigate all known and shadow assets and an Online Gamified Simulation Platform for Cyber Security Training.