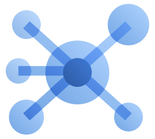
Acronis

Assessing and mitigating **software vendor supply-chain** cybersecurity risk

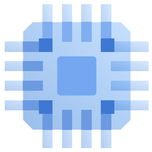
2021

Table of contents

Executive summary



The SolarWinds attack brought the risk of potentially catastrophic supply-chain attacks into sharp focus for enterprises, government institutions, and service providers alike.



The breach was notable for its subtlety and sophistication**:** it was effectively an advanced persistent threat (APT) attack staged by a state actor against a software vendor for the purposes of conducting surveillance on the vendor's many customers in government and private enterprise.

Managed service providers (MSPs) in particular should focus on this risk, as a successful attack that extends to the MSP's clients could represent an existential threat to those businesses. Few companies will want to do business with an MSP that, rather than protecting its clients, provided a conduit for data theft, tampering or destruction.

In a business which by its nature depends on a complex supply and delivery chain, an **MSP's cybersecurity posture** can be dramatically weakened by vulnerabilities among its suppliers, partners, and clients. A chain is only as strong as its weakest link.

MSPs seeking to reduce their software supply-chain risk should focus first on critical areas of cybersecurity risk associated with their tech vendors and service providers, including:

1. **Security** of access controls
2. **Quality** of their secure software development and distribution practices.

Historic scope of the SolarWinds breach

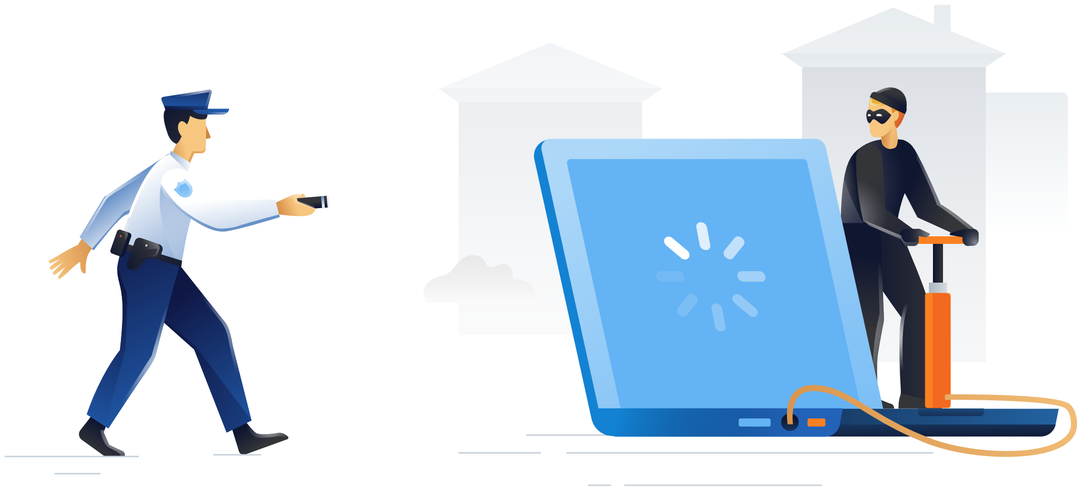
The SolarWinds supply chain incident that was detected in early December 2020 has emerged as one of the most sophisticated and successful cyberattacks on Western government institutions and businesses in recent history. In it, a well-organized, well-funded, highly skilled group purportedly affiliated with Russia's Foreign Intelligence Service successfully penetrated thousands of large global enterprises and multiple U.S. federal government agencies, including the Departments of Homeland Security, State, Treasury and Commerce. While 80% of victims are believed to be U.S.-based, the attack also compromised targets in Canada, Mexico, the U.K., Spain, Belgium, Israel and the U.A.E.

The SolarWinds breach is the latest extant example of a so-called software supply-chain attack, in which an adversary compromises a trusted source of software, firmware or hardware, embedding surveillance tools and other malicious code in it. The initial target can be a vendor's private repository or app store, or a public code-sharing repository like GitHub. A potential breach is enabled whenever a user installs the compromised software update, firmware update, or hardware. In the case of the SolarWinds breach, attackers penetrated the tech vendor's private repository for Orion, a network management and performance monitoring tool popular with enterprises, public institutions, and service providers. Such tools are a popular target for attackers because by their nature they can easily provide access to an entire business, its partners and its customers.

The attack also qualifies as an advanced persistent threat (APT), characterized by a sophisticated, multi-stage effort most often undertaken by nation-states that have the deep pockets, patience and skills required to mount them. APTs are by their nature designed to evade detection over the long term, thus are difficult to defend against and then to root out completely once they have been discovered.

Anatomy of the attack

The attack followed the classic multi-stage tactics of APTs: initial compromise, communication to an external command and control server to download additional malware, surveillance of the tech environment to identify vulnerabilities, escalation of privileges, lateral movement within and beyond the network to infiltrate other accessible targets, and then execution of the ultimate attack, in this case the theft of valuable data. Extraordinary, ingenious methods were used at every step of the attack to evade secure software development guardrails and cybersecurity countermeasures.



Beginning in the autumn of 2019, the attackers began implanting a malicious backdoor into legitimate Orion code, using a highly sophisticated process to ensure that any compromised Orion software builds did not fail and thus alert the developers to an intrusion. The compromised software now contained a backdoor that could communicate via HTTP to external third-party servers. This gave it the ability to retrieve and execute commands to transfer files to external services, execute malicious as well as legitimate processes, profile the system, reboot machines, and disable system services like forensic and anti-virus countermeasures. Its network traffic masqueraded as a normal Orion protocol, and it stored its reconnaissance in ordinary plugin configuration files, allowing it to blend in with everyday SolarWinds activity.

Once the trojanized update was installed by an Orion customer, a malicious DLL was loaded by a SolarWinds installation process that saw it as legitimate, as it was signed with the proper digital certificate. After a dormant period of up to two weeks, this malware began connecting with external command and control servers, all renamed to look like legitimate servers in the victim's environment, and using virtual private servers to present IP addresses from the victim's country.

Traffic to the malicious control servers mimicked normal SolarWinds API communications to evade detection. After gaining initial access, the attackers continued to disguise their operations while they moved laterally across the organization, frequently using legitimate credentials to gain remote access into a victim's environment. They routinely replaced legitimate utilities and scheduled tasks with their own malicious counterparts, ran them, then restored the originals, removing their tools and backdoors once remote access had been achieved.

This approach enabled the use of a memory-only dropper running as a service to read a fake .jpg file, decode its embedded malicious payload, and manually load it directly into memory, thus evading antivirus scans. This payload did the real damage, identifying useful files throughout the organization and quietly uploading them to the attackers' external servers.

The resulting theft of sensitive business and government data, including knowledge of IT infrastructure and operations, appears to be the main goal of the attack. While the success of this operation is a big blow to the affected businesses and government agencies, it is conceivable that its effects could have been much worse. For example, in addition to data theft, attackers might also have mounted a ransomware attack that encrypted the target's data, leaving victims struggling to recover now-inaccessible data and resume normal operations.

The existential threat of supply-chain attacks to service providers

For any service provider, a **SolarWinds-style software supply-chain attack** has to be viewed as an existential threat to the business: breaking SLAs, violating contracts, and gravely harming the company's reputation, client confidence, and public valuation. If an MSP cannot be trusted to vet its own suppliers to prevent such an attack, why should any business trust it with sensitive business applications and data?

No company, no matter how sophisticated and deep its security regimen, **should get overconfident**. Profit-driven cybercriminals are less fearsome: they will move onto a new target if their current one doesn't quickly yield results. By contrast, state actors bring unlimited resources, patience, and hacking expertise to their attacks. Few private businesses could repel an attack with the scale, sophistication, and persistence of the SolarWinds APT, especially in light of the fact that the typical MSP has as many as 25 tech vendors, 25 clients, and 2000 endpoints as potential attack surfaces.

Nevertheless, there are steps that MSPs can and must take to minimize the risks of software supply-chain attacks, as well as measures to limit the extent of the damage if an attack succeeds. Many large enterprises and service providers turn to industry frameworks from international standards bodies like ISO/IEC and NIST for help in conducting security assessments of suppliers, customers, and themselves. **However, these often require dedicated staff** experienced at working with such frameworks to be very effective, and most are oriented toward large enterprises rather than the multi-tenant, multi-client environment in which MSPs operate. Regardless, they can provide a useful starting point to understand full-fledged security assessment processes and methodologies. See the ADDITIONAL RESOURCES section below for where to find documentation on these frameworks.

To help get started down the path of security assessment in the interest of mitigating software supply-chain attack risk, consider using the following abridged set of questions for key risk areas:

ACCESS TO APPLICATIONS

Who and how access is granted to sensitive data, how access is documented and what measures are taken to ensure that the infrastructure the data is hosted on is managed and tested for security.

SECURE SOFTWARE DEVELOPMENT

Measures used throughout the software development process, from design through release to customers, to mitigate risks of tampering (malicious code insertion) and other security threats mounted by external or insider actors.

Vendor security assessment for software supply-chain risk requires more than just getting documentation. It requires challenging their assertions and demanding proof of key claims. This can include audit trails, proof of training and certification, data center compliance certificates, and even on-site facilities audits.

Application access security

Access control to sensitive applications and data is a critical component of software supply-chain security. **A few key questions to ask** of suppliers, including multi-tenant service providers, on this score:

1. **Do you restrict, log, and monitor access** to your security management systems (e.g., firewalls, vulnerability scanners, network sniffers, APIs, etc.)?

2. **Do you monitor and log privileged access** (e.g., administrator level) to security management systems? Have you implement privileged user management to ensure time-limited, least-privileged access to critical systems?

3

Do you have policies, procedures, and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?

4

What are your procedures and technical measures for data access segmentation in multi-tenant environments?

5

What Authentication, Authorization and Accountability (AAA) systems do you have in place? What systems do or do not require multi-factor authentication? Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?

6

What controls do you have in place to prevent unauthorized access to your own applications and object source code? What analogous controls do you have in place for tenant applications?

7

Do you require a periodic authorization and validation of the entitlements for all system users and admins?

8

Do you support use of, or integration with, existing customer-based Single Sign-On (SSO) solutions to your service? Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?

9

Do you have an identity management system (enabling classification of data per tenant) in place to enable both role-based and context-based entitlement to data?

10

Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?

11

Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement? Do you allow tenants/customers to define password and account lockout policies for their accounts?

12

Do you support forced password changes upon first logon?

13

Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?

14

Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc.) appropriately restricted and monitored?

Secure software development

The SolarWinds attack demonstrated that once an attacker has compromised a secure code repository, many traditional security mechanisms you might have in place can be defeated, as such countermeasures assume that a certain OS, application, driver or network element is legitimate and therefore will not act maliciously unless compromised by external, more readily detectable attacks.

Thus, you must vet your key software vendors to ensure that they have implemented a secure software development program as well as mechanisms to defend the product and customer data from modification and other attacks.

KEY QUESTIONS TO ASK YOUR SOFTWARE VENDOR:

1. **Do you train your software architects and engineers** as well as IT operations and cybersecurity staff in security awareness and relevant standards for secure code architecture, development, and protection against tampering?

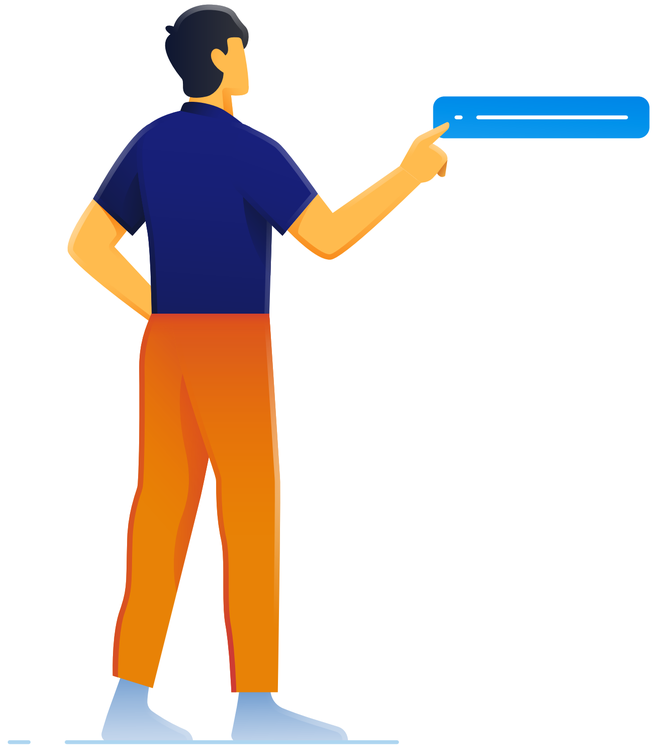
2. **Do you have a multi-level process** in place to analyze and review code for vulnerabilities at every stage of development, with reviews conducted independently by internal development teams, sandbox testers, and external auditors?

3. **Have you implemented a decomposed code development process** that enables scrutiny of individual software components by random reviewers prior to commitment to the next stage of the development process and subsequent integration?

4. **Do you securely transmit code modules** to subsequent development phases, use digital signing of secured binaries prior to a final sandbox review of security and privacy features prior to distribution to external auditors, partners and customers?

5. **How do you protect encrypted customer data** against access, modification or copying by your own employees?

6. **Do you employ an independent security team**, separate from internal IT operations and cybersecurity staffs, to conduct internal security awareness training, audits of security infrastructure and processes, and enforcement of security policies?



7. **What cybersecurity and physical security standards** do you enforce for your data centers? Do you conduct routine audits by independent third-party auditors of high reputation, external penetration testing of network security measures, internal network segmentation, and intrusion detection scanning?

8. **Do you encrypt customer data** in transit and at rest in your data storage infrastructure, and conduct stringent erasure and/or destruction of decommissioned storage media?

9. **Do you implement strict confidentiality, business ethics, and code of conduct policies** for your employees, including background checks where appropriate, non-disclosure agreements, and principals of segregation of duties, need to know, and least privilege to protect against malicious or inadvertently dangerous acts by insiders?

10. **What access controls, multi-factor authentication and activity logging** do you implement to ensure only appropriate access to sensitive systems?

11. **Do you have a bug bounty program** to encourage and reward the disclosure of potential security vulnerabilities in your products?

12. **Do you use hardware-backed storage** for private binary encryption keys to ensure that customer keys cannot be exported or leaked?

Summary

The SolarWinds breach provides a useful reminder that modern adversaries, both cybercriminals and hostile state-actors, continue to innovate and evolve in sophistication, guile, and persistence. They are using the same advanced tools in the development of their attacks – heuristics, machine learning, artificial intelligence, increased integration and automation – as legitimate tech vendors and service providers are using to defend their businesses and customers. It is a battle in which attackers generally have first-mover advantage: it is easier to attack than it is to detect, contain, terminate, and recover from an attack.

Implementing a full-bore ISO/IEC or NIST security framework is often beyond the needs and resources of many MSPs, but the philosophy behind them can still useful. They provide a proven vocabulary and methodology for managing cybersecurity risk. By starting with these basic questions, you can start down the path of systematically identifying and mitigating your software supply-chain security risk. A framework-based mindset can help you to identify areas where existing processes can be strengthened and new processes implemented, as well as prioritize your security requirements and set appropriate expectations with your suppliers and partners.

Acronis offers security consulting and auditing services to help you get started.

For more information, see acronis.com/services

Acronis Cyber Protection Solutions certifications and tests

PLEASE NOTE this document is for educational purposes only. It is not legal advice, and you should not treat it as legal advice. The document is provided as-is without representation or warranty of any kind.
You should contact an attorney to obtain advice with respect to any particular issue or problem. No defense is impervious to cyberattack and no measures will completely prevent a committed attacker from breaching your defenses.

Additional resources

Many businesses rely on industry frameworks from international standards bodies for guidance on conducting security self-assessments as well as assessments of suppliers and partners. While not all of them are optimized for multi-tenant, multi-client MSP environments, these tools provide a useful starting point. Here are some of the most popular and widely-adopted security frameworks and assessment methodologies:

NIST 800-171 – A popular general framework for assessing internal security policies, procedures and personnel:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

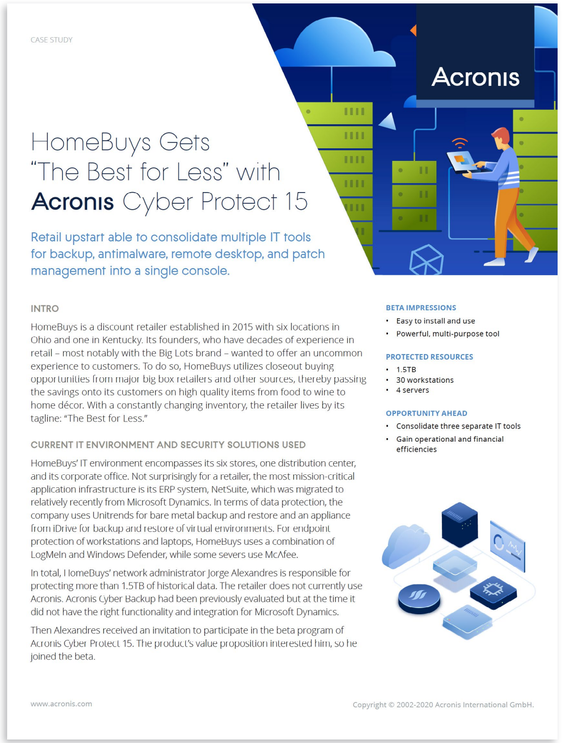
Vendor Security Alliance – A detailed vendor security assessment questionnaire:
https://www.vendorsecurityalliance.org/downloadQuestionaire

Center for Internet Security (CIS) Risk Assessment Method (RAM) – A good high-level internal security assessment framework:
https://www.cisecurity.org/cybersecurity-tools/

Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) – Tools for assessing security controls in IaaS, PaaS, and SaaS services:
https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/

ISO/IEC 27001 – A broadly-adopted set of international standards for internal security management:
https://www.iso.org/isoiec-27001-information-security.html

Additional insights from Acronis



CASE STUDY

HomeBuys Gets "The Best for Less" with Acronis Cyber Protect 15

Retail upstart able to consolidate multiple IT tools for backup, antimalware, remote desktop, and patch management into a single console.

INTRO

HomeBuys is a discount retailer established in 2015 with six locations in Ohio and one in Kentucky. Its founders, who have decades of experience in retail – most notably with the Big Lots brand – wanted to offer an uncommon experience to customers. To do so, HomeBuys utilizes closeout buying opportunities from major big box retailers and other sources, thereby passing the savings onto its customers on high quality items from food to wine to home décor. With a constantly changing inventory, the retailer lives by its tagline: "The Best for Less."

CURRENT IT ENVIRONMENT AND SECURITY SOLUTIONS USED

HomeBuys' IT environment encompasses its six stores, one distribution center, and its corporate office. Not surprisingly for a retailer, the most mission-critical application infrastructure is its ERP system, NetSuite, which was migrated to relatively recently from Microsoft Dynamics. In terms of data protection, the company uses Unitrends for bare metal backup and restore and an appliance from iDrive for backup and restore of virtual environments. For endpoint protection of workstations and laptops, HomeBuys uses a combination of LogMeIn and Windows Defender, while some severs use McAfee.

In total, I HomeBuys' network administrator Jorge Alexandres is responsible for protecting more than 1.5TB of historical data. The retailer does not currently use Acronis. Acronis Cyber Backup had been previously evaluated but at the time it did not have the right functionality and integration for Microsoft Dynamics.

Then Alexandres received an invitation to participate in the beta program of Acronis Cyber Protect 15. The product's value proposition interested him, so he joined the beta.

BETA IMPRESSIONS

- Easy to install and use
- Powerful, multi-purpose tool

PROTECTED RESOURCES

- 1.5TB
- 30 workstations
- 4 servers

OPPORTUNITY AHEAD

- Consolidate three separate IT tools
- Gain operational and financial efficiencies

www.acronis.com

Copyright © 2002-2020 Acronis International GmbH.

Acronis Blog: Provides the latest updates and insights from the world's cyber protection leader.

Acronis YouTube Channel: Delivers frequent videos of use cases, demos, cyberthreat analysis, and company news.

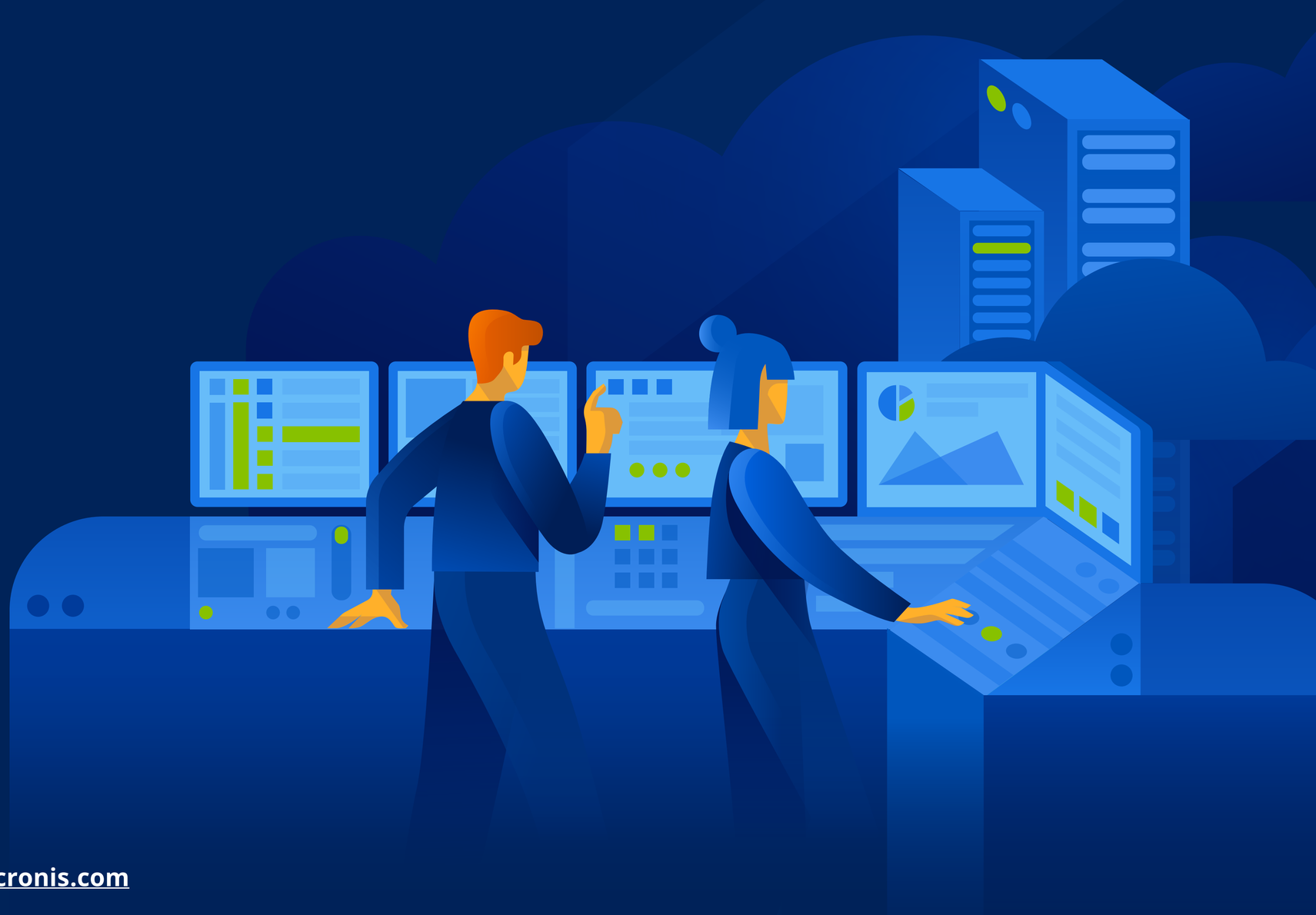
Acronis Resource Center: The go-to hub for cyber protection white papers, e-books, in-depth articles, tutorials, infographics, etc.

Acronis Events: Ongoing series of events, webinars, interviews, etc., including details on joining.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions. With award-winning AI-based antimalware and blockchain-based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on-premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,500 employees in 33 locations in 18 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages.



Acronis

Learn more at **www.acronis.com**