TANIUM

Supply chain security is tough: So what should good look like?

Organizations are struggling to manage supply chains end to end. The best practice for security should start with visibility into all of your IT assets.

Cybersecurity breaches keep piling up. And with each new incident, security officers and CEOs breathe a sigh of relief that they weren't the victim. But who can say they won't fall prey to the next major supply chain attack? Because there will be a next time.

Whether we're talking about third-party software, hardware, or service providers, organizations still rely too much on blind trust and spreadsheets, manually assembled from a disjointed array of reports and cyberdata.

As an industry, we need to develop a better way of doing things — one that combines rich, quantitative data with reputable third-party attestations and assessments.

The challenge deepens, of course, when it comes to managing supply chains end to end. Can you vouch for the security practices of your third parties' third parties? How many degrees of separation can you track?

Global organizations have struggled with this challenge for years, and there are no simple answers. What we can say is that best practice supply chain security should always start with visibility — into your IT assets and those of your partners.

Only with this kind of back-to-basics approach can you begin to answer those fundamental questions to help calculate risk exposure: Who are your suppliers? What's their security maturity? What data can they access? And how do they use it?

The problem with supply chains

The complexity of modern supply chains can very soon make risk management efforts spiral out of control. Many larger companies are exposed on multiple fronts. Many digital businesses use SaaS products, global data processors, hardware provided by third parties, outsourced software developers, and consultancy services. These third parties use their own third parties.

It doesn't help that, for decades, many organizations used manual processes and audits based on overly simplistic questions to help them calculate supplier risk (for example, Do you have a patch management program?).

This approach may elicit binary responses or highly subjective answers that you can't validate through any form of third-party attestation.

Take the fallout of the SolarWinds incident. Some organizations asked their suppliers: "Did you have the affected versions of SolarWinds Orion in your environment?"

But the "yes/no" response this elicited isn't enough information to determine important risk calculations.

If the supplier in question had weak asset and application management processes in place, they might not even know the answer with any certainty. And what good is an assurance that's based on partial or incomplete data?

Mature organizations ask more open-ended questions of its suppliers (for example, How does your company approach threat modeling? Describe your approach to patch management.). In answering these more holistic questions, you can obtain a much wider assurance of supplier security.

In addition, some organizations have tried to move beyond the manual spreadsheet-based approach with technical solutions that try to calculate the security posture of suppliers more rigorously.

But many services will succeed only in providing an incomplete, "outside-in" view of suppliers based on a limited set of criteria and subjective scoring. They aren't holistic enough to be much help. This failure is just the tip of the iceberg.

Key challenges with supply chain security

Security and risk teams engaged too late

Supply chain governance commonly happens too late in the onboarding process to leave enough time to mitigate or remove any risk that it discovers. The security and risk team can come under tremendous pressure from the business to give its blessing to the new deal. Keen not to be seen as the "department of no," chief information security officers (CISOs) may feel like they have no choice but to do so.

Recertification doesn't happen

As important as rigorous due diligence prior to onboarding is, periodic reappraisal of the relationship is also critical.

For example, you might use a SaaS provider whose service was originally deployed to just a small number of developers using only test data. That app may now be used by hundreds of employees and processing critical business information.

Periodic recertification is vital to dynamically manage risk as it evolves. Unfortunately, supply chain security is "set and forget" for many organizations.

End-to-end visibility and assurance

Third-party risk management is one thing, but the further upstream or downstream you go, the harder it gets. What about your suppliers' suppliers? And their suppliers? The challenge here is that there's no consistent, industry-wide best practice for managing end-to-end supplier risk.

Even if you ask your suppliers to provide detailed data based on threat models and risk analysis, their processes to validate their own partners could be lightweight, cursory inspections. When each component of the supply chain is different, it becomes incredibly challenging to qualify aggregate risk end to end.

What happens next?

All organizations struggle with these challenges to a certain extent — even those with relatively mature cybersecurity programs. That's why all organizations need to go back to basics and answer fundamental questions about who their suppliers are, what their security maturity is, and how they use your data, if at all.

This struggle boils down to visibility: understanding what IT assets you own, what's running on them, and what third-party dependencies there are.

It's simple to say but not always simple to do. **Tanium research** found that 94 percent of global IT executives and managers have discovered endpoints within their IT environment that they were previously unaware of.

You must extend this same visibility to your suppliers. They must be able to provide a comprehensive, accurate inventory of their IT assets to understand the status of endpoints and what software versions are installed. And they must be able to patch promptly to mitigate risk dynamically.

This inventory should be part of a holistic effort to calculate the overall maturity of your suppliers' security posture — taking in not just partial point-in-time patch and vulnerability telemetry, but also a supplier's approach to threat modeling, secure software development, security architecture and much more.

It isn't just about, Do you run a particular version of software? You need to consider the processes used to develop people and technology in a company.

Focusing on prescriptive questions like, *Were you running the malicious SolarWinds Orion update?* provides an ostensible assurance at a point in time, but won't help when the next global cyberattack happens. Effective supply chain security demands a far more expansive approach. You need to know:

- Mean time to deploy a critical patch
- Percentage of endpoints that don't conform to a CIS Benchmark Hardening Standard
- Percentage of endpoints missing the company's endpoint security tooling (AV, patch/vulnerability management agents)

Once you have this quantitative data in hand, combine it with third-party attestation and evaluations to gain a 360-degree view of risk in each supplier. You might want to use international standards to help here, like **ISO 27001.**

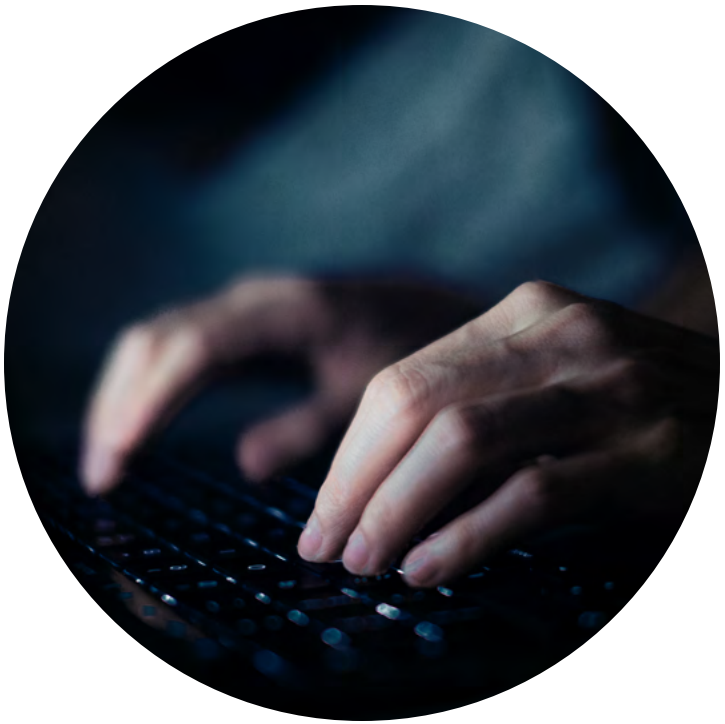
Build supply chain protection into your organizational processes.

As a next step, you should define a minimum set of requirements and embed them into contracts. Doing so will help build a more consistent, data-driven alternative to that arbitrary, spreadsheet-based approach to assurance, which too many of us depend on.

Here are some other ways to build up your supply chain protection:

- Involve security and risk teams as early on in the new supplier due diligence process as possible. Base requirements on the sensitivity of the provided service.
- Perform periodic security certifications and align these efforts to the criticality of the provided services.
- Carry out comprehensive threat modeling and risk analysis to better understand who your main adversaries are, where they may strike, and how. Doing so will help inform your supply chain security strategy.
- Ensure your suppliers have a clear process for breach notification in the event of a worst-case scenario.
- Understand suppliers' approaches to the security software development lifecycle (SDLC): How are their developers trained and certified in application security? What are their processes for static and dynamic analysis?
- Define incident response playbooks, so you know what good looks like if the worst happens.

This isn't an exhaustive list, and you'll notice that it doesn't address the challenge of end-to-end supply chain assurance. Certainly, this is a topic we, as an industry, need to think about more carefully.



Assess your organization's risk posture

Request a five-day, no-cost risk assessment to get a comprehensive view of risk posture across your organization.

Get risk assessment →

Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete and up-to-date endpoint data — giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.