TANIUM

Tools designed for security could be your biggest cybersecurity threat

Cybersecurity tool sprawl: Expensive, impossible to secure, poorly integrated, vulnerable to attack

Digital transformation has changed how businesses operate, making them more agile and responsive to the markets they serve. But this transformation has come at a cost — a rambling web of software tools and applications, cloud infrastructures, and decentralized application services. And this complexity presents a big challenge to cybersecurity teams.

In tandem with digital transformation initiatives has been the rise of the remote workforce, making traditional network perimeters a thing of the past. Many IT resources now operate outside the corporate firewall and are vulnerable to cyber threats of all kinds. The result? A much larger and more varied attack surface.

Many large enterprises use 40+ best-of-breed point solutions.

Unless the tools are sanctioned and inventoried, security teams are often unaware of their existence. And a security team cannot secure what it doesn't know exists."

Bradley Schaufenbuel
Paychex CISO

Tackling complexity and the security risks it presents

As complexity has taken hold, IT organizations have armed themselves with a litany of point solutions to tackle their most pressing security challenges. A Forrester survey[1] found that on average, organizations today use 20 or more tools from more than 10 vendors to secure and operate their environment. Many large enterprises may use upwards of 40 to 50 tools — all best-of-breed, point solutions. This is tool proliferation in the extreme.

A best-of-breed approach can work … if it delivers the results an organization is looking for. However, when organizations suffer from outage after outage and critical vulnerabilities and patches go unresolved for months, the merit of a best-of-breed approach comes into question.

Bradley Schaufenbuel, the CISO of Paychex, a provider of payroll services for small businesses, says "tool sprawl" has become a major concern for security teams. Every day, his own team finds new vulnerabilities from shadow IT tools in their estate. If that software is not regularly updated, the attack surface grows exponentially.

Many IT executives believe the sheer number of tools in their organization limits — not enhances — the effectiveness of Security and IT Operations teams. But, as we will discuss, a best-of-breed approach has been the logical default option for most IT teams.

The tyranny of best of breed

Twenty years ago, IT management solutions were primarily packaged as platforms. They provided integrated functionality, and their architectures for monitoring and acting on the environment worked under the relatively simpler requirements of that era. However, around 15 years ago, rapid changes in computing (advanced threats, increasing scale, IaaS, virtualization, remote work, cloud) created requirements that those platforms could not adequately deliver.

Enter the era of point solutions and best-of-breed approaches.

Enterprises were forced to start buying point solutions to address specific gaps in their tooling environment and emerging threats. Every nuanced need, every new desired feature, and every response to changes in the environment created new tool requirements, each with multiple vendor options.

But the best-of-breed approach has several drawbacks. Each tool provides different levels of visibility, based on how that tool scans and interrogates the environment. Tools are expensive to deploy, learn and upgrade. And they're often not extensible to accommodate changes over time, so they have short shelf lives.

> The very tools designed to secure your organization may present the greatest cybersecurity threat.

Security tools can breed insecurity

The great irony is that the very tools designed to secure the organization may well present the greatest cybersecurity threat, as the well-publicized SolarWinds attack in 2020 highlighted.[2]

Orion, SolarWinds' IT performance monitoring solution, allows IT departments to look at one screen and see its entire network. At the time of the attack, it was used by more than 30,000 public and private organizations, including local, state and federal agencies.[3] Hacking Orion was genius. Its privileged access and wide deployment made it a highly lucrative target.[4]

IT decision-makers know that the tools in their security portfolio lack integration. This, according to an IBM study,[5] adds cost and even more complexity, which which hinders your ability to detect and respond to breaches and other adverse events.

Moreover, problems with security-tool sprawl don't necessarily originate in IT. Instead, many security tools are one-time freeware installations by employees self-servicing their machines. But problems arise when licenses requiring corporations to pay for these tools kick in and block the program's use. Few users go the extra mile to actually remove them, creating additional potential cybersecurity vulnerabilities.

"Most security teams with dozens of tools will admit they don't really know how well they're working," comments Chris Hughes, cybersecurity consultant and university lecturer. "They're spending a lot on these tools but can't tell you if they're getting value out of them. And that's money they could have shifted to other resources, like bolstering their teams."

Cost-effective security: Certainty without complexity

In principle, companies invest in multiple tools because they have complementary capabilities, and the benefits they produce when combined are, in theory, greater than the sum of the parts. But Mark Settle, a former CIO for Okta and BMC Software, believes it often doesn't work out that way. "In practice, tools may have overlapping capabilities, be difficult to administer, and come with underlying security vulnerabilities," Settle notes.

So, how can IT operations and security teams tame tool sprawl, while reducing costs and protecting their organizations against the multitude of threats that circle them like hungry sharks?

A best-practice approach is to deploy a single, unified platform to handle multiple functions. This streamlines operations and improves security while also controlling the proliferation of shadow IT and rogue software solutions.

A unified platform can cut the cost of running, managing, and maintaining multiple security tools, while:

- Improving the ability to cost-effectively meet tightening global regulatory and compliance mandates.
- Addressing the pressure to make the right bets strategically when it comes to tooling and security practices.
- Deploying patches automatically with greater efficiency.
- Reducing the attack surface in the face of trends such as a growing remote workforce.
- Meeting the renewal demands of cyber-insurance carriers for improved mean-time-to-patch and mean-time-to-repair standards.
- Consolidating tools without compromising security.
- Simplifying the discovery, management, and protection of all assets within the IT estate.

Tool consolidation — the return of the platform approach

To address tool proliferation, IT leaders need to step back, set all aside tool preferences and biases for a moment and perform an objective tool audit. This involves:

1. Identifying the results and capabilities your organization needs to deliver regardless of tools and technology.
2. Assessing each tool individually and catalog the capabilities it provides.
3. Creating a visualization to see where overlaps and redundancies exist between tools. These overlaps are your opportunities for consolidation.

Such an audit will help inventory your current state and start the process of tool consolidation, the first step towards a platform approach.

With a unified security operations platform, CISOs, CIOs and CTOs can:

- Monitor software usage and eliminate solutions and licenses you don't need.
- Unify endpoint management and security onto a single console.
- Provide IT teams with instant, accurate, and actionable data to maximize efficiency and minimize risk.
- Proactively monitor system performance and resolve issues before they become incidents.
- Reduce mean-time-to-repair (MTTR) and the number of tickets to improve workplace productivity and reduce support costs.
- Improve IT decision-making around critical software and hardware refresh initiatives.

228% ROI

Forrester Consulting examined Tanium customer implementations and found an ROI of 228% over three years with a net present value (NPV) of $12.57M, benefits PV of $18.07M, and payback under six months.

A Forrester Consulting study commissioned by Tanium

Looking ahead

Remote work is here to stay. The need to effectively manage and secure all types of endpoints (in and out of the network) will only increase. So, it's clear that with a distributed workforce, IT teams will continue managing and protecting endpoints physically outside the corporate firewall. A converged platform that provides visibility, control and trustworthy data to IT teams will only grow more critical in a hybrid work environment.

A converged platform can deliver measurable results, such as

- Reclaimed assets, minimized point tools, and modernized IT.
- Increased team efficiency via accurate, timely data and tools to boost performance and improve decision-making.
- Greater visibility and control across teams to mitigate potential IT outages and their associated costs.

The acceleration of digital transformation and the rise of the remote workforce have contributed to a proliferation of security tools and applications for most companies. This tool sprawl, though once a logical way to fill gaps in capabilities, is now contributing to higher costs and creates additional security vulnerabilities. For companies looking to scale efficiently, it's time to move to a platform approach.

Learn how Tanium simplifies your IT tooling environment, enhances endpoint visibility and security, and helps you save time and money.

LEARN MORE

ENDNOTES

1. https://www.tanium.com/blog/why-best-of-breed-may-not-be-best/
2. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
3. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
4. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
5. https://pages.awscloud.com/rs/112-TZM-766/images/PTNR_idg-connected-security-whitepaper_Jun-2021.pdf

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

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