servicenow

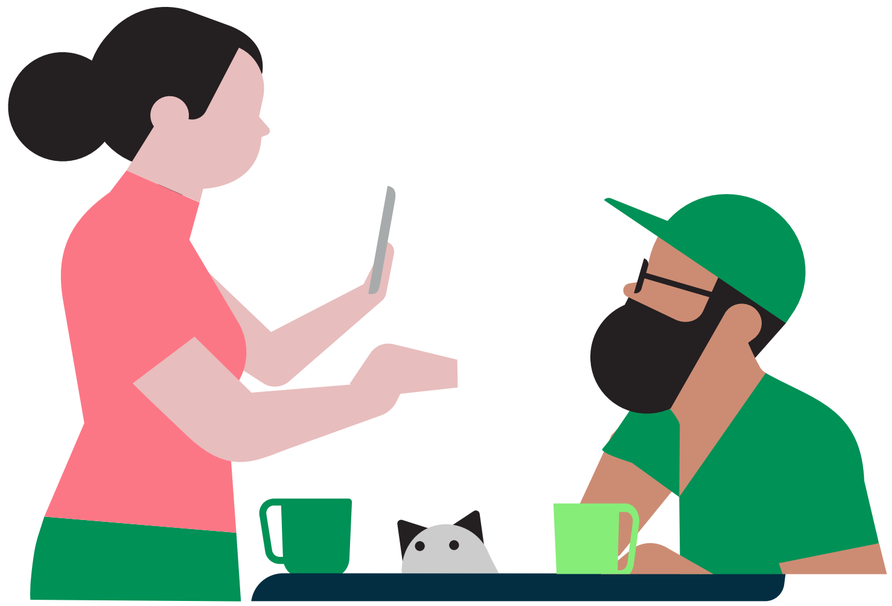
Same cyberthreat, different story

How security, risk, and technology asset management teams collaborate to easily manage vulnerabilities—within a workday

servicenow

Chapter 1

The bad old days



It is such a beautiful day in Half Moon Bay, California that I've decided to start work on my back patio to enjoy the fresh air and sunshine. I'm a senior IT security analyst for an enterprise software company in Santa Clara, but I can use all the tools of my trade remotely. That's cool because I've got the flexibility to work from home whenever I want. It is a routine day so far–mostly P2 tasks–and I've just finished off my second cup of coffee. The French doors open, and my lovely wife appears.

A moment I can't miss

"Hiya Trev!" Aimee says, a little bit too enthusiastically for 8:17 a.m. "Remember, we need to be ready to leave by about 6 tonight. Courtney's thing starts at 7 and we should try to be in our seats by 6:45. Capeesh?"

"Absolutely!" I reply. "No way I will miss seeing her on stage again."

Our daughter Courtney is a theater major at our local community college. She'd scored the lead role in the spring musical. Three years ago, she was also starring in a high school production, and I'd missed the only chance I had to see her–it was heartbreaking for me.

"The night of her performance, my team and I at my previous employer dealt with a P1 cyberattack that came in through unpatched software during the day. Addressing the breach was mostly a manual, chaotic process."

servicenow

The past haunts me

The night of her performance, my team and I at my previous employer dealt with a P1 cyberattack that came in through unpatched software during the day. Addressing the breach was mostly a manual, chaotic process. Our recovery and remediation activities extended well past 10 p.m.—and long after my daughter had performed.

My former organization, a prominent financial services company, was already hamstrung with a disconnected inventory of hybrid IT assets from at least 15 sources across multiple departments as well as a host of disparate tools to track those assets. It took about 90 staff hours just to generate an asset inventory. And it often took weeks of manual activities to identify and prioritize security vulnerabilities, patching needs, and compliance issues, then remediate them.

And like too many organizations, the company failed to detect, track, or restrict shadow IT (often 40% of IT spending[1]) or prevent unsanctioned software. In fact, like 60% of organizations, they didn't even include shadow IT in threat assessments, even though it accounts for 20% of all cyberattacks—with SaaS representing 45% of all incidents.[2]

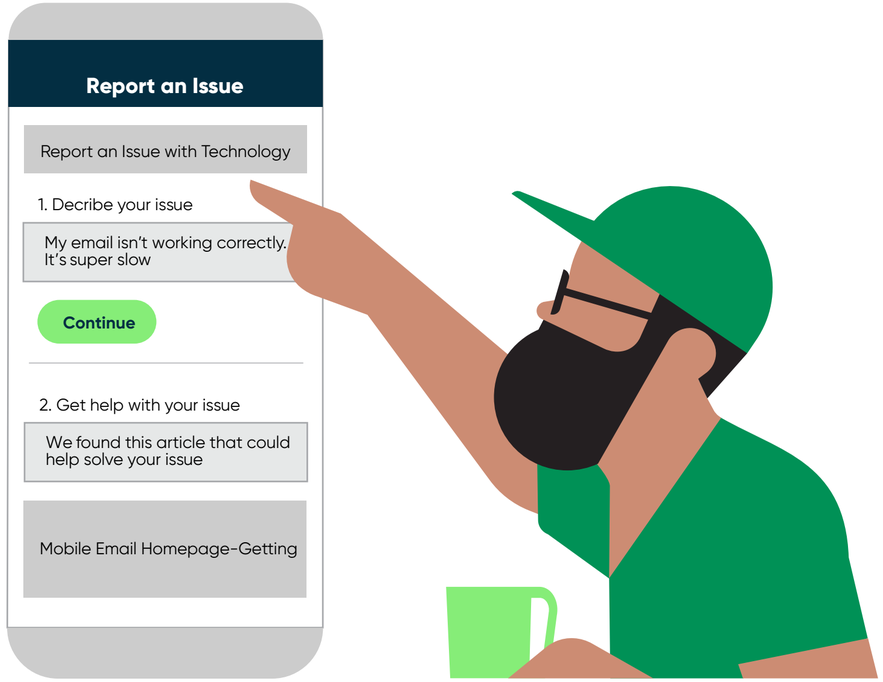
Bad processes exposed

Sure enough, a cyberbreach occurred because of a vulnerability in prohibited software that an employee had managed to download a week prior to the incident. The breach exposed the personal data for more than 280,000 customers. After that first night, it took 73 days of manual effort to fully address the breach—at a cost to the company of $3.2M in labor expenses, lost revenue, and a damaged reputation. But for me, the biggest loss was missing that great moment in my daughter's life—the chance to see her excel at something she loves. Plus, I wasn't the only one who missed family time—the whole team did! That was when I—and other employees—made the decision to start looking for a better job.

"Sure enough, a cyberbreach occurred because of a vulnerability in prohibited software that an employee had managed to download a week prior to the incident"

Chapter 2

I've got issues



With just hours to go before my daughter is to be on stage singing her heart out, my peaceful morning is interrupted by an alert on my smartphone. With a glance, I see that the risk team has assigned me to address two security incidents based on vulnerability issues. The tool the risk team uses for risk monitoring has already determined that the issues are a high priority because they could impact a significant percentage of our company.

- **Incident one** involves additional processes detected in productivity software running on a server in the datacenter. Those processes are impeding timely, enterprise-wide, reliable email communication—a critical business service. We're already seeing users reporting this issue company-wide. It's a zero-day vulnerability.
- **Incident two** concerns a new exploit that's just surfaced in the wild via a common engineering software that isn't regularly patched. Another company that uses the software experienced a security breach through it, and our CISO, Alison, has raised an alarm. She wants to know if our company also uses the software and wants to ensure that there aren't any older version of it currently residing on networked devices—and any devices that might attach to the network after the initial patching occurs.

I have my work cut out for me.

" The tool the risk team uses for risk monitoring has already determined that the issues are a high priority because they could impact a significant percentage of our company. "

servicenow

Chapter 3

The sweet comfort of automation

Time is of the essence, but I honestly don't have a sense of dread like I did a few years ago when my former employer was hammered by that security breach.

My current company uses modern tools on a single platform to manage security, risk, IT asset management (ITAM), and several other IT workflows. During my tenure here, all the teams in security operations, risk, ITAM, IT operations management (ITOM), and other business-critical services continually work together to get a comprehensive understanding of issues. By using automated workflows to resolve issues, we react faster—and we avoid crazy firefighting when we hear about a potential breach.

How does it all work?

I visualize a presentation slide in my head:

IT Workflows on a single platform with automation

How to use automation to resolve issues:
1. A healthy CMDB provides visibility of the entire IT estate.
2. Combination of agentless and agent-based discovery finds software anywhere.
3. Discovered software and purchasing data are combined and updated as assets.
4. An AI-driven risk assessment tool continually monitors for changes.
5. A security operations tool collects and prioritizes vulnerability data based on impact.
6. Patches are applied and software asset data is updated.
7. Risk scores are updated in real time as risk levels change.
8. Risk analysts can see changes and remediations on their dashboard.
9. The platform captures every action for an audit trail.

" **By using automated workflows to resolve issues, we react faster—and we avoid crazy firefighting when we hear about a potential breach.** "

Time to collaborate

Because of automation, orchestration, and integration between security, technology assets, risk, and IT workflows, I have the visibility I need to quickly start collaborating with my counterparts on other teams to stop these vulnerabilities from morphing into serious security breaches. And, we won't have to take up time snapping screenshots, filling out spreadsheets, and running reports to be ready for auditors.

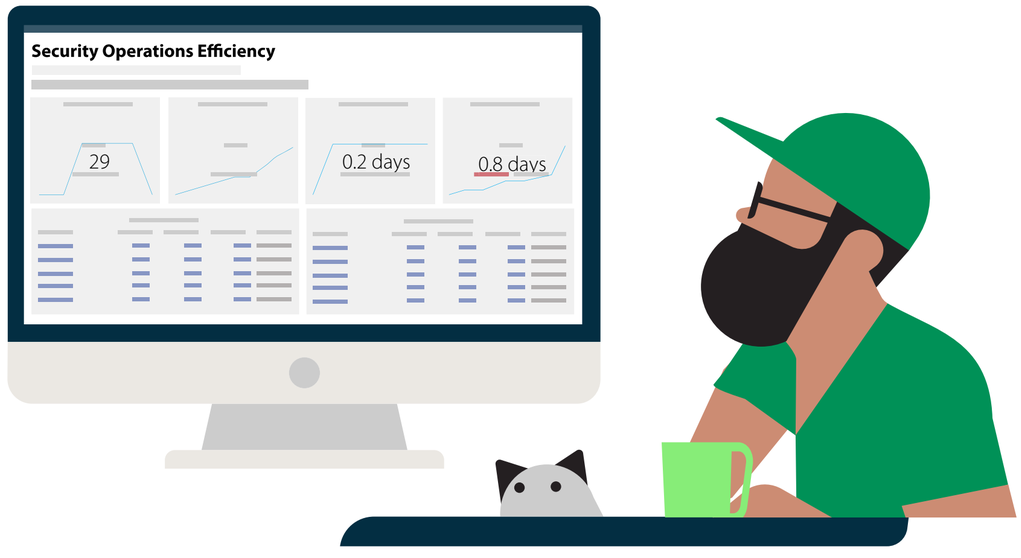
Lunchtime security conversation

I know the way my company maintains cooperation among departments to manage risk reporting is not yet the industry norm, but I'm grateful it's how we do things here. I recall a conversation I had with Jonathan, my colleague on the risk team, over lunch a few days ago.

"You know that 84% of teams don't collaborate consistently on risk reporting?[3]" He'd asked me, shaking his head. "I just read that in a Gartner report."[3]

I nodded in agreement, then replied: "That's too bad because orchestration is absolutely key to stopping cyberattacks. Our CISO mentioned in an all-hands last week that the cost of global cybercrime is growing every year and is expected to reach $10.5 trillion a year by 2025."[4]

With serious money on the line, vigilance and robust security processes are key. I'm thinking now would be a good time to log into our security operations tool to get more details about the vulnerability issues, find out when they were identified, and see if there are remediations available.



> **"Orchestration is absolutely key to stopping cyberattacks. The cost of global cybercrime is growing every year and is expected to reach $10.5 trillion a year by 2025."[4]**

Chapter 4

The power of easily accessible data

As I open our security operations tool, I think of the famous quote from IT visionary Tim O'Reilly, "Who has the data has the power." My job is so much easier now that so many manual tasks are automated, and I know I'm working with accurate, real-time data.

My quick investigation

I immediately see that the risk team has identified an unpatched vulnerability on the productivity software, where the firewall had detected and flagged connections to an unknown IP address. The issue is automatically assigned to me. I see also that a lot more employees have now raised the issue that email communication supported by this software is unacceptably slow. Clearly there is something going on. AI would have also offered remediation if we had run into this problem in the past. It's possible this vulnerability has left us exposed to a bad actor.

To get information about the second vulnerability issue involving engineering software, I leverage a dashboard with software asset information to view inventory data supplied by the ITOM team. I discover that our company does indeed use the software. I confirm an update is required to avoid a security breach.

"Clearly there is something going on. AI would have also offered remediation if we had run into this problem in the past. It's possible this vulnerability has left us exposed to a bad actor."

Armed with data, we proceed with confidence

Data is readily available from the IT asset management (ITAM) tool that runs on the same platform as tools we use for risk management and security operations. The ITAM tool can easily determine where the productivity software with the vulnerability is running in the data center. It can also identify what machines are running which versions the engineering software that needs patching.

Since the ITAM tool can pinpoint and trigger patching tools that remediate scheduled patching needs, shadow IT, restricted software, and end-of-life software, I know I don't have to be concerned today about other software installations that present risks. This is a great illustration of why an integrated ITAM tool makes sense for enterprises because about 70% of ITAM initiatives are driven primarily by information security and risk management needs.[5]

> **"An integrated ITAM tool makes sense for enterprises because about 70% of ITAM initiatives are driven primarily by information security and risk management needs."[5]**

servicenow

Chapter 5

Microsoft Teams work makes the dream work

It's a no-brainer that the zero-day, productivity software vulnerability qualifies as a crisis event, so I promote it accordingly in the security operations tool with a few mouse clicks. Major security incidents get prioritized over more routine ones, so that there is a faster resolution process. In Teams, I ping Ron, the director of security operations and my boss. I bring him up to speed.

"Thanks for staying on top of these issues!" Ron tells me in our Teams chat. "Alison was already anxious about the patch for the engineering software, and I know she's also concerned about the fix we need to make in the data center."

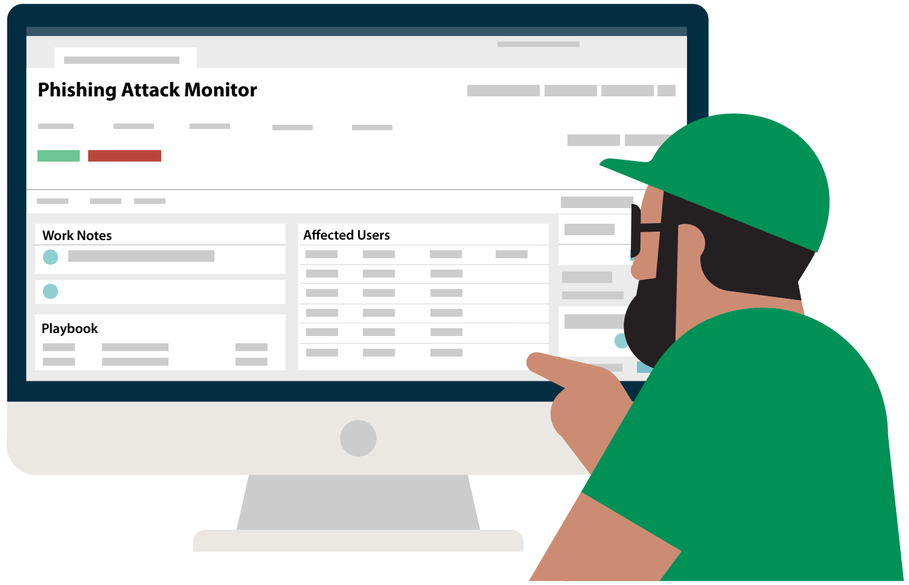
Taking the commandor's chair

Ron designates me as the incident commander for these issues. This enables me to use our virtual command center to activate the Microsoft Teams conference call feature. In the Teams application, I can engage everyone working on the issues from risk management, IT, security, and other groups. What's really cool is that we can all view the communication tasks within Teams during the call.

> **"It's a no-brainer that the zero-day, productivity software vulnerability qualifies as a crisis even. Major security incidents get prioritized over more routine ones, so that there is a faster resolution process"**

Chapter 6

Bad actors turn in a poor performance



After the call, I use a feature in the security operations tool to quickly identify how the issue appeared in the productivity software. I see that a malicious actor sent a phishing e-mail, and when a user clicked on a link in the email, it downloaded malware to gain access to customer records through the software. It's an old trick but the bad guys are getting smarter about making those emails look legitimate.

Playing defense, then offense

We discover a security bypass vulnerability—from a coding error—exists in the productivity software, which fails to enforce security settings configured on a system. But because of tight integration that the security operations tool facilitates between SOAR and the MITRE ATT&CK framework, the attempt to access customer records was thwarted–for now. I think to myself: "Nice try, weasels, but you probably weren't expecting this level of defense, were you?"

Since the security operations and ITAM tools are integrated, it takes just minutes for Edna, my colleague on the ITAM team, to proactively identify which servers in the data center are hosting the productivity software. Their locations and necessary corrective measures are documented for me in the security operations tool. Then the tool notifies Owen, my security teammate who's managing the servers, so he can take action. It's a good time for me to grab some lunch–leftover pizza that's delicious even when it's cold.

"Since the security operations and ITAM tools are integrated, it takes just minutes for Edna, my colleague on the ITAM team, to use automated workflows to proactively identify which servers in the data center are hosting the productivity software."

Chapter 7

Patching things up

After lunch, I see that Owen used another feature in the security operations tool to search for and implement a solution to purge the malware, then patch the productivity software on multiple servers. The capability to quickly remediate threats is our superpower that thwarts future threats. A data point pops into my head that I read recently in a Gartner report—that 79% of the companies that experienced a security breach indicated that it could have been avoided with a patch or a configuration change.[6] "Other companies could prevent so many hassles if they had the tools we have," I think to myself.

Creating an audit trail is easy on the same platform

For the engineering software vulnerability, I know Edna and the rest of the ITAM team are using the ITAM tool to identify all the software installations throughout the enterprise by searching on product name, the vulnerable versions, and the software publisher. Sure enough, Edna conveys this information within the security operations tool. In a quick Teams chat, I collaborate with everyone again. I note that the changes have occurred to the software asset data in the ITAM software workspace and know that the risk tool will pick these changes up too, because it's leveraging the same data. This makes it easier to track the software lifecycle and follow an audit trail if needed.

"Our tools for ITAM, security operations, ITOM, and risk management—which thankfully run on the same platform—will automatically detect, track, and trigger patching actions for devices that connect to the network."

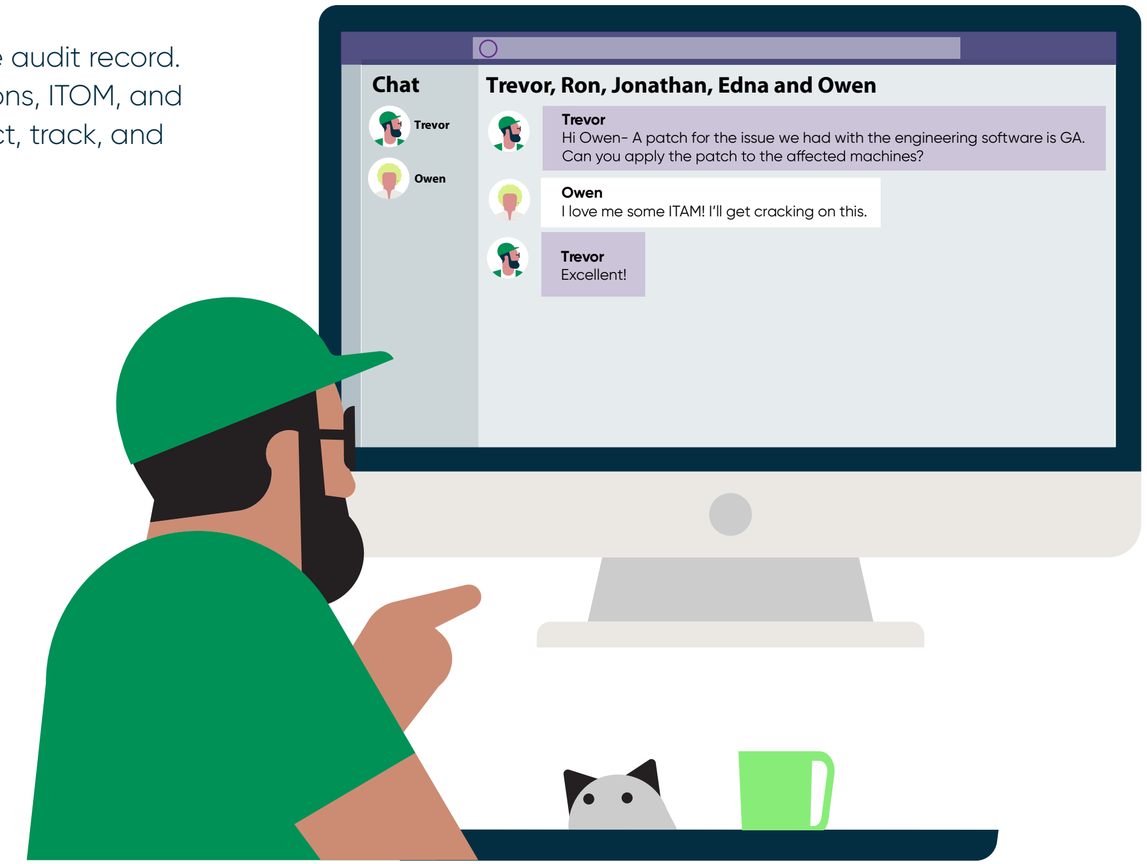
Automatically applying a patch

I also discover through data delivered in the security operations tool that a patch for the engineering software issue was recently released for general availability through the vendor, but never distributed. Within the Teams chat, I communicate this information to Owen, who will execute the patching effort, using data generated by the ITAM tool on how many machines are affected and which ones haven't been updated. "I love me some ITAM!" Owen says in the chat. "I'll get cracking on this."

Owen works with Edna on the ITAM team to take the information identifying all the instances in the asset fleet and moves quickly to automatically apply the patch. He then loads the patch into our patching tool using orchestration directly from the security operations tool. It's amazing how much time we save with this stuff!

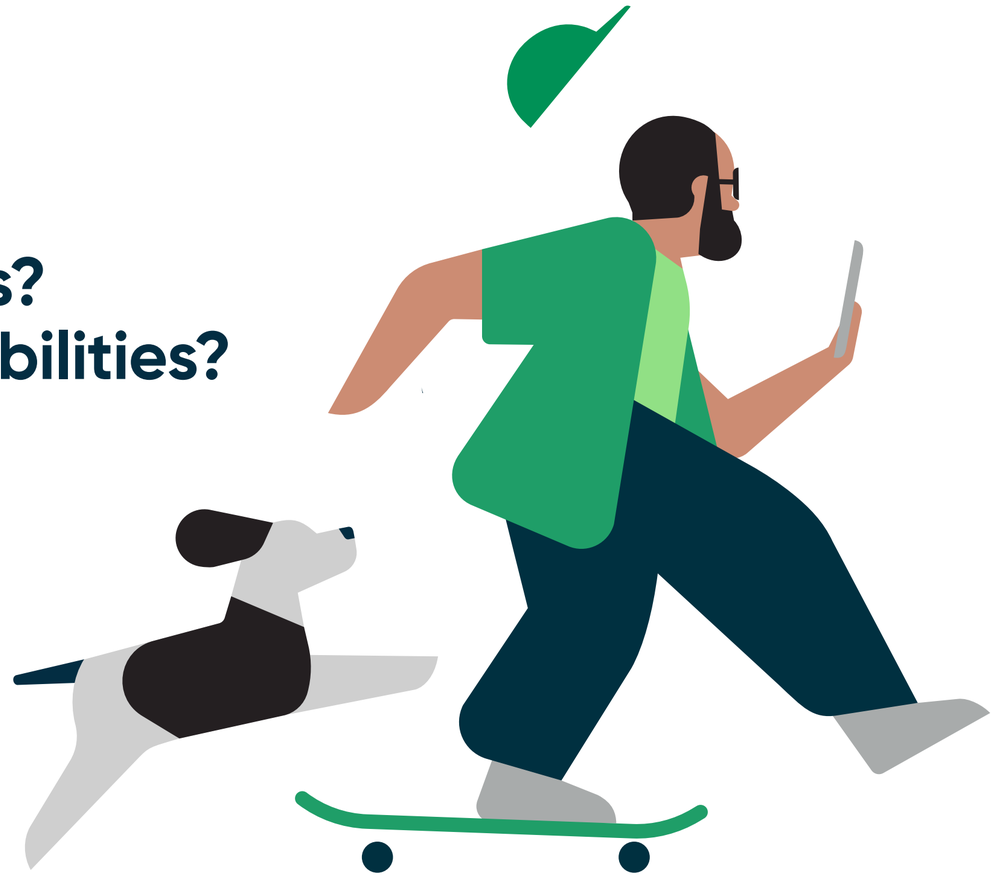
Patches update more than software

These actions are also reflected in the security operations tool and the risk tool for the audit record. If this issue arises later in the engineering software, our tools for ITAM, security operations, ITOM, and risk management—which thankfully run on the same platform—will automatically detect, track, and trigger patching actions for devices that connect to the network.



Chapter 8

Vulnerabilities? What vulnerabilities?



I take a late afternoon break to walk my dog Dinker on the Coastal Trail along the ocean. I stop for a few minutes at a bench and log into the mobile version of our security operations tool with my phone. With a quick look at the security operations dashboard, I see that the solution for the productivity software and the patch for engineering software have both been applied.

Still on my phone, I shoot off a message about the status in our Teams chat and note that the information also is accurately reflected in the incident records shared by the security operations and risk tools. Automation rocks!

The final step to automatically close the issue is for the risk team to run another control test within the risk tool. If everything works as expected, the test will no longer identify the risk because the vulnerability will no longer appear in the security operations vulnerability scan data.

"When there's an inevitable regulatory audit, my company has the data and evidence to prove we managed the issues properly."

Time to relax

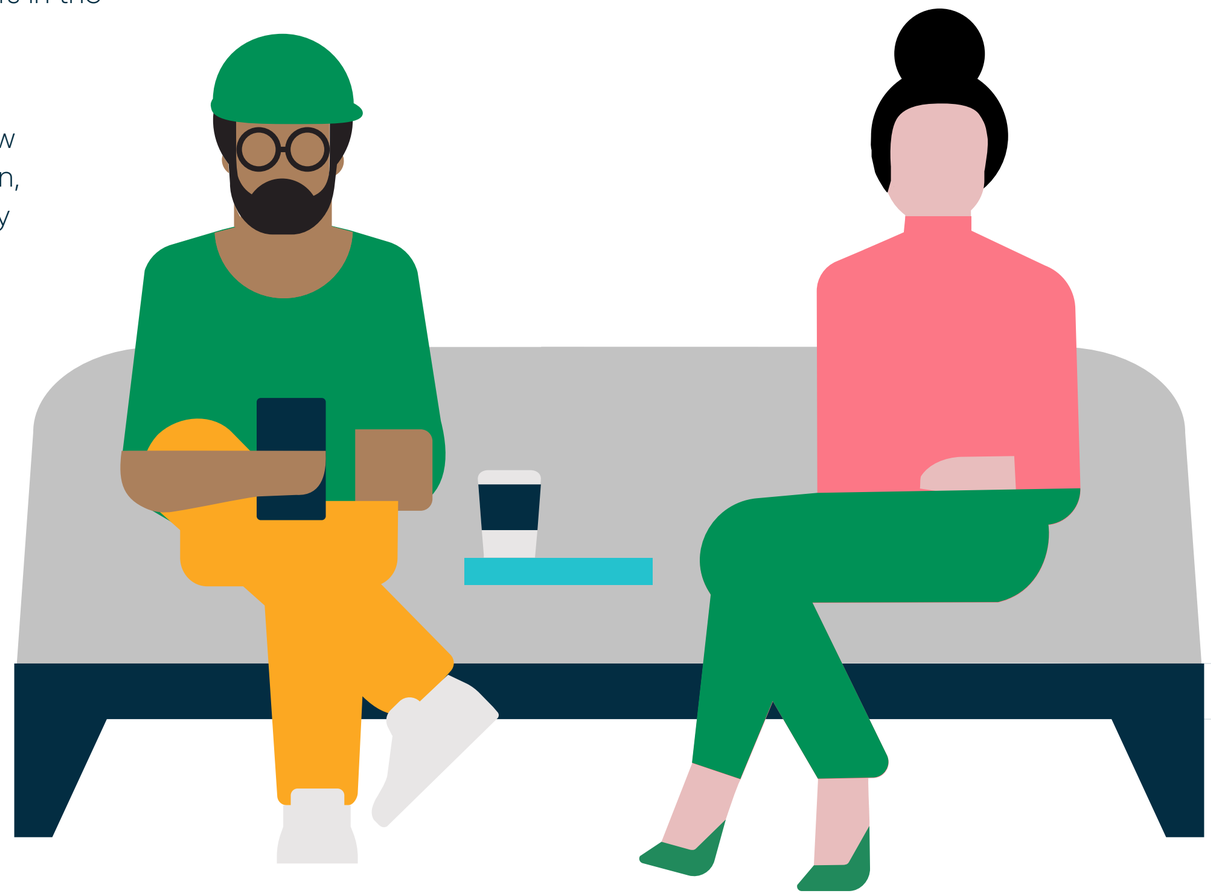
By the time I get back to the house and log back into the security operations tool on my laptop, I confirm that the vulnerabilities no longer appear. I know this means the risk tool has detected a lower risk level; there are two fewer risks reflected in the risk dashboard—and the issues are automatically closed.

But now it's time for me and my wife Aimee to head to the college theater to see our daughter perform, so I log off and close my laptop. I'm ready to turn my attention away from bad actors in the cyberworld to good actors (like my daughter) in the real world.

Grateful for the right tools and the best teams

After I settle in my seat in the theater, I send an email to my boss Ron to let him know that the engineering software is no longer a threat to the company. Our CISO, Alison, will be happy when she gets the news. As the lights go down, I know I can truly enjoy the performance. I'm grateful again that I have the right tools, workflows, and collaborative colleagues so I can do my job, and our collective teams can keep our company secure. And, I have the peace of mind that when there's an inevitable regulatory audit, my company has the data and evidence to prove we managed the issues properly.

On with the show!



Chapter 9

ServiceNow workflows for the win

The next morning, I'm still basking in the glow of my daughter's performance last evening. She was amazing on stage, as we expected she would be! I try to focus as the security team gets on Zoom for a post-mortem call.

Ron thanks us for our efforts and reminds us that orchestration and automation among ITAM, IT operations, risk management, and security helps us stay one step ahead of the latest threats and drives continuous improvement. "I mean, when you pair human action with AI and automation, you can cover all the angles, no matter where the team members are located," says Ron.

Ron gives a shout out to the tools we use from ServiceNow. I second that motion, but with a nod to our ServiceNow solution! No other vendor can provide a single platform solution and shared data model, to support cross-functional, automated workflows and to reduce manual processes. Point solutions only provide a subset of capabilities without much integration, automation and insights. With ITAM, IT operations, security, and risk management on one platform, we get the visibility, cyberthreat remediation, and governance we need to reduce the risk to our organization. In addition to increased productivity, our teams are empowered to work efficiently, meaning we can have personal lives and never miss great moments with family and friends.

Take a bow, ServiceNow.

"Orchestration among ITAM, IT operations, risk management, and security helps us stay one step ahead of the latest threats and drives continuous improvement."

servicenow

Technology-based workflows are better together with ServiceNow

When you empower your risk, security, and ITAM teams to collaborate with AI-driven automation, you'll take vulnerability management to new heights, and drive unprecedented efficiency in your IT organization.

Learn More:

Solution brief: **Integrate your security and asset workflows to remediate threats faster**
Solution brief: **Asset management and IRM: The more you know, the lower the risk**
Solution brief: **Power your resilience business with risk informed decisions**
Ebook: **6 steps to a stronger security posture**

Sources:

1. How much is Shadow IT costing you?, Jamf.com
2. Ibid
3. The Top Enterprise Risk Management Priorities for 2021, Gartner
4. Cyberwarfare in the C-Suite, Cybersecurity Ventures, Nov. 2020
5. IT Asset Management: Current State and Near-Term Outlook, EMA
6. Market Snapshot/Secure Operations Automation, Voke

SN-Risk_Security_ITAM Ebook-052022