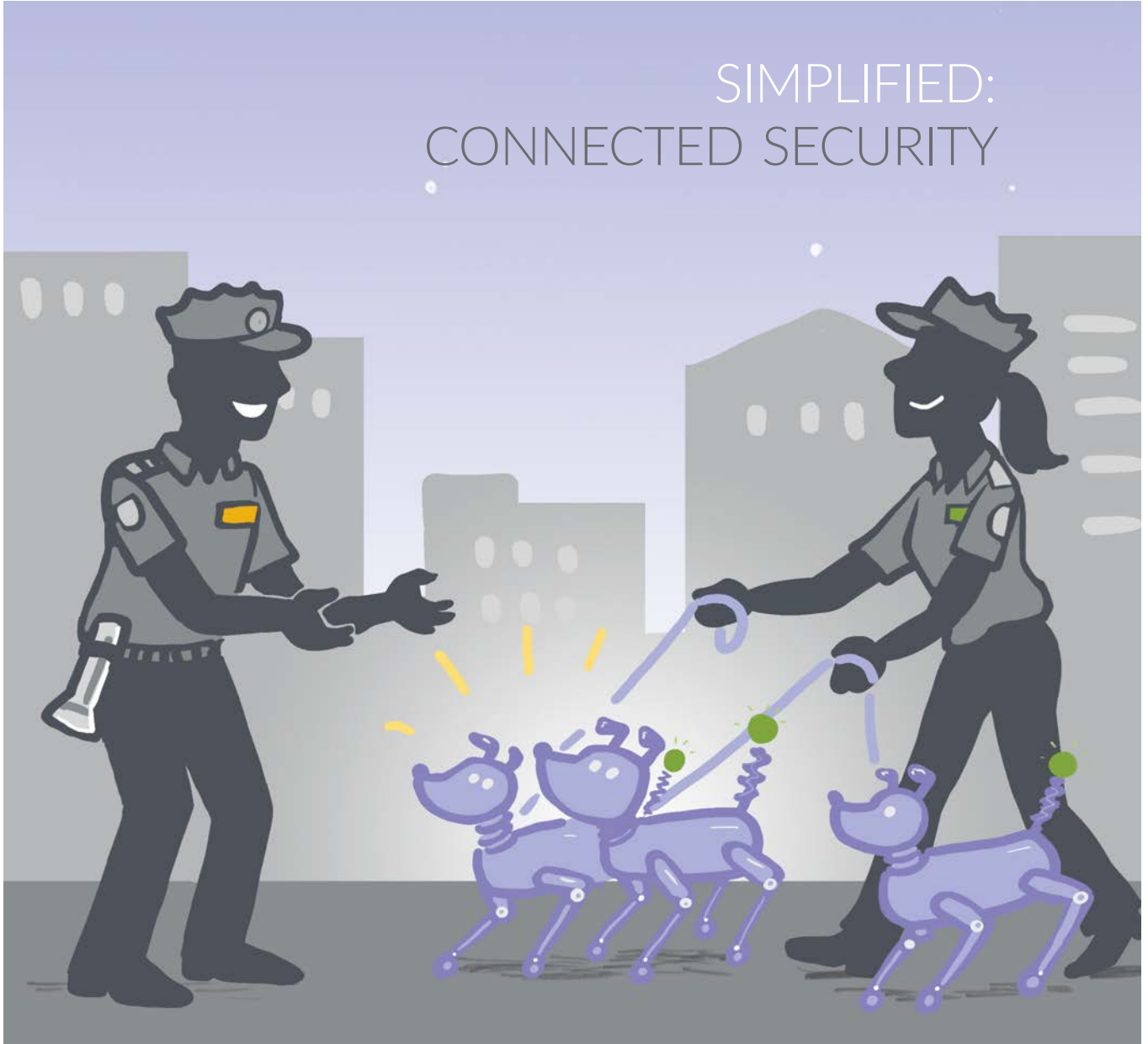


SIMPLIFIED: CONNECTED SECURITY





SIMPLIFIED:
CONNECTED SECURITY

When it comes to security,
everyone has noticed that threats
are getting more sophisticated...



...and more frequent.



So security solutions are getting more sophisticated and capable, but also more difficult to manage...



...and the security solutions landscape has become crowded.



There is a solution for every threat,
but each solution has a cost.



Tools need to be organized and managed,
issues need to be explored and resolved...

...and this takes money and time.



For years, the focus in security circles has been finding every single threat. And so long as budgets can support the growth in tools, this strategy can continue.



But as budgets become constrained the emphasis shifts from merely finding the threats to more efficiently managing security operations.



Security operations require three things. First, you have to be able to see what is happening.





To see clearly, you need depth — more information from systems and devices, and breadth — information from every point in the infrastructure, no matter the device type or who made it.

Second, you have to know what to do based on what you see.



Some alerts are false alarms...
while others identify real threats.

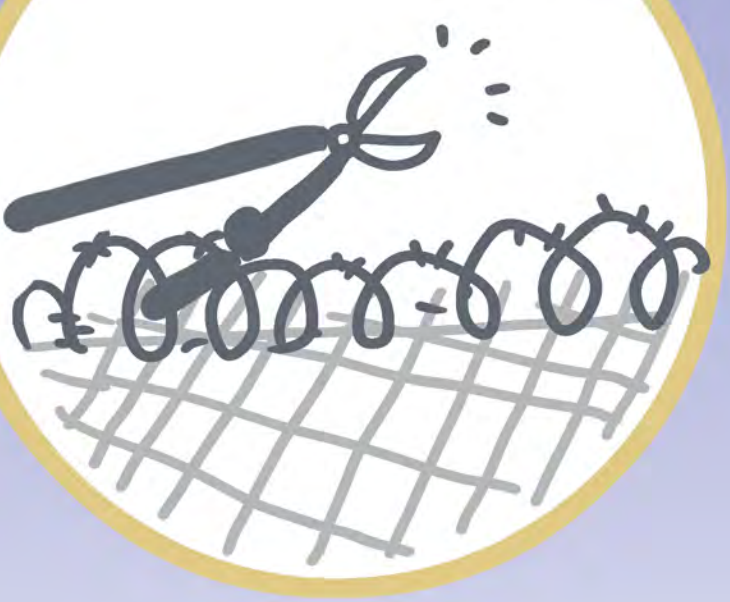


You need to know
which ones to act on,
and what to do
about them.



Not every problem needs
the same solution.





So you need to use the right solution
in the right place.



Sometimes you might want to protect against a specific threat. Other times you might quarantine a host or application.



The key is matching the response to the threat.



And third, once you know what to do, you have to actually do it.






But as operating environments
become more diverse...

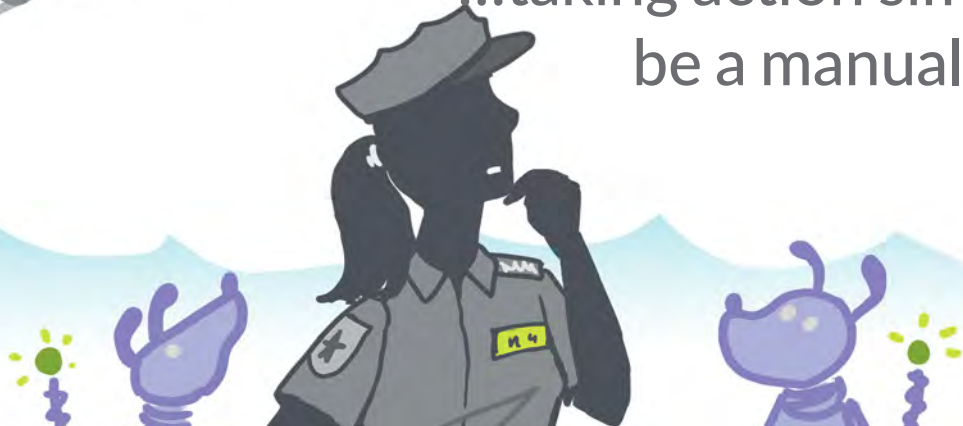
...and companies
embrace mobile and
multicloud...

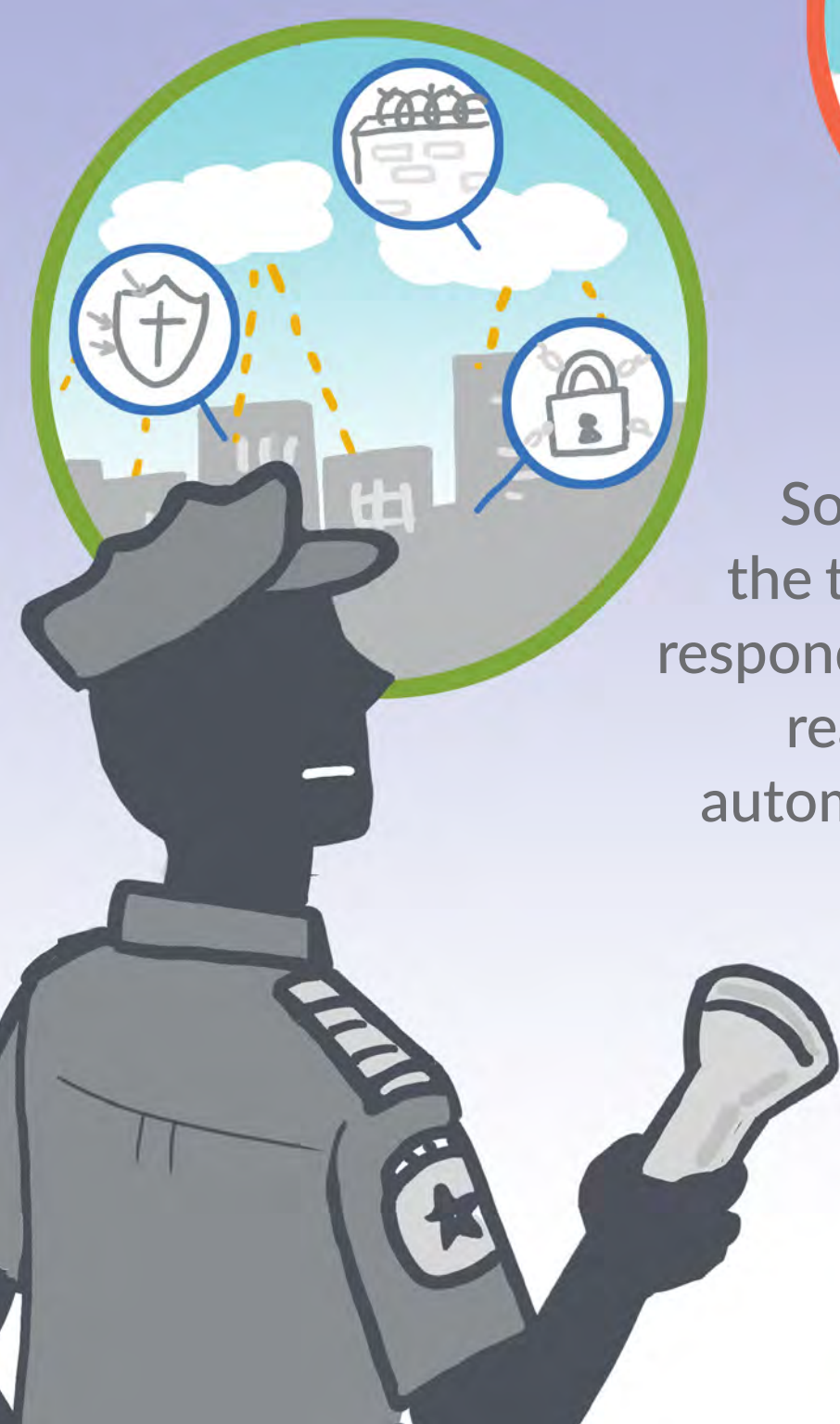


...as well as IoT
and edge computing...



...taking action simply cannot
be a manual operation.





So how do you see the threats you must respond to, identify the real problems, and automatically provide protection?





If your infrastructure is a loose collection of isolated elements, or requires too much management, you can't.





This is why modern security requires that all of these things be connected...





...with multiple points of enforcement throughout the network.

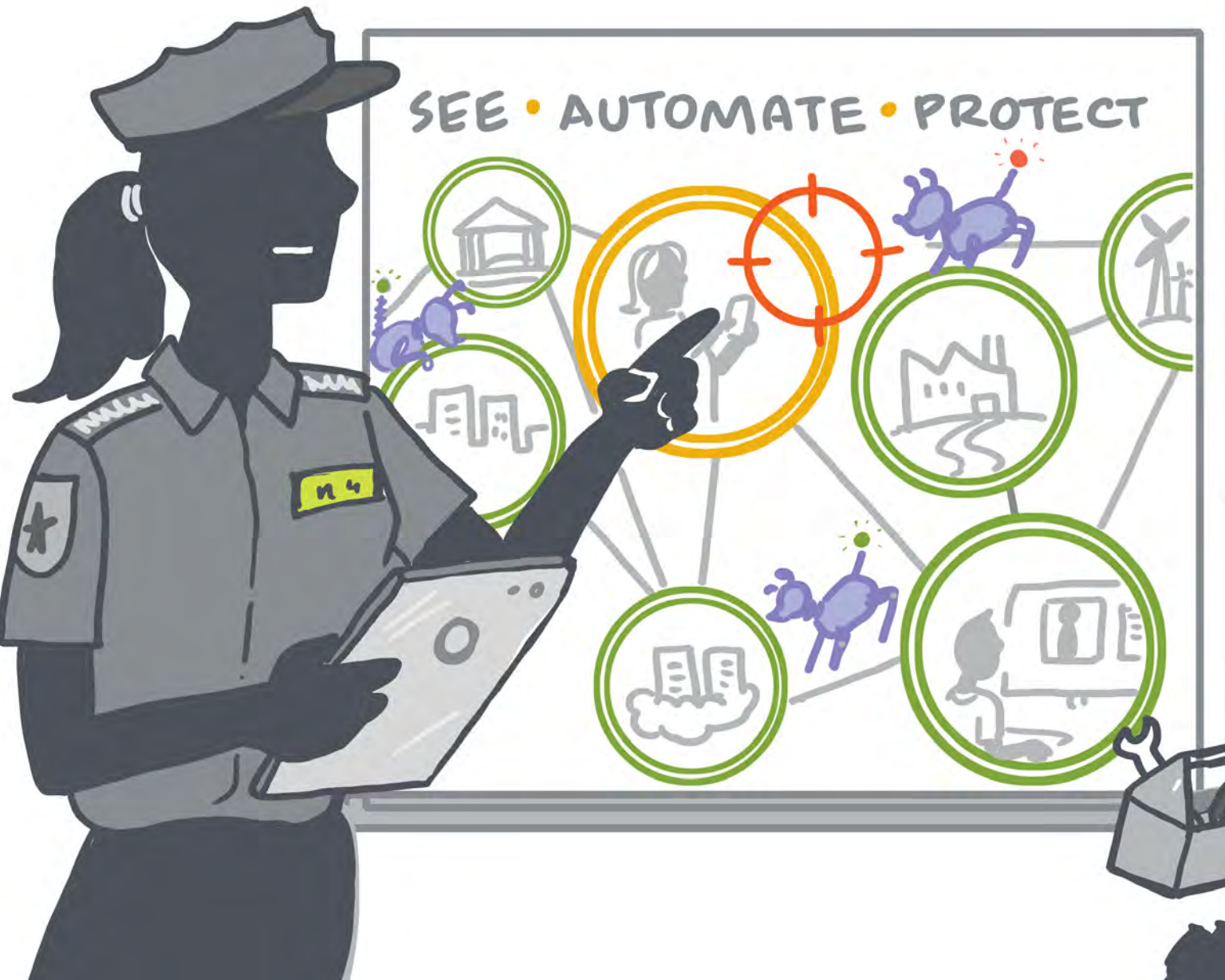


So that information from anywhere
can be used to identify
all kinds of threats.





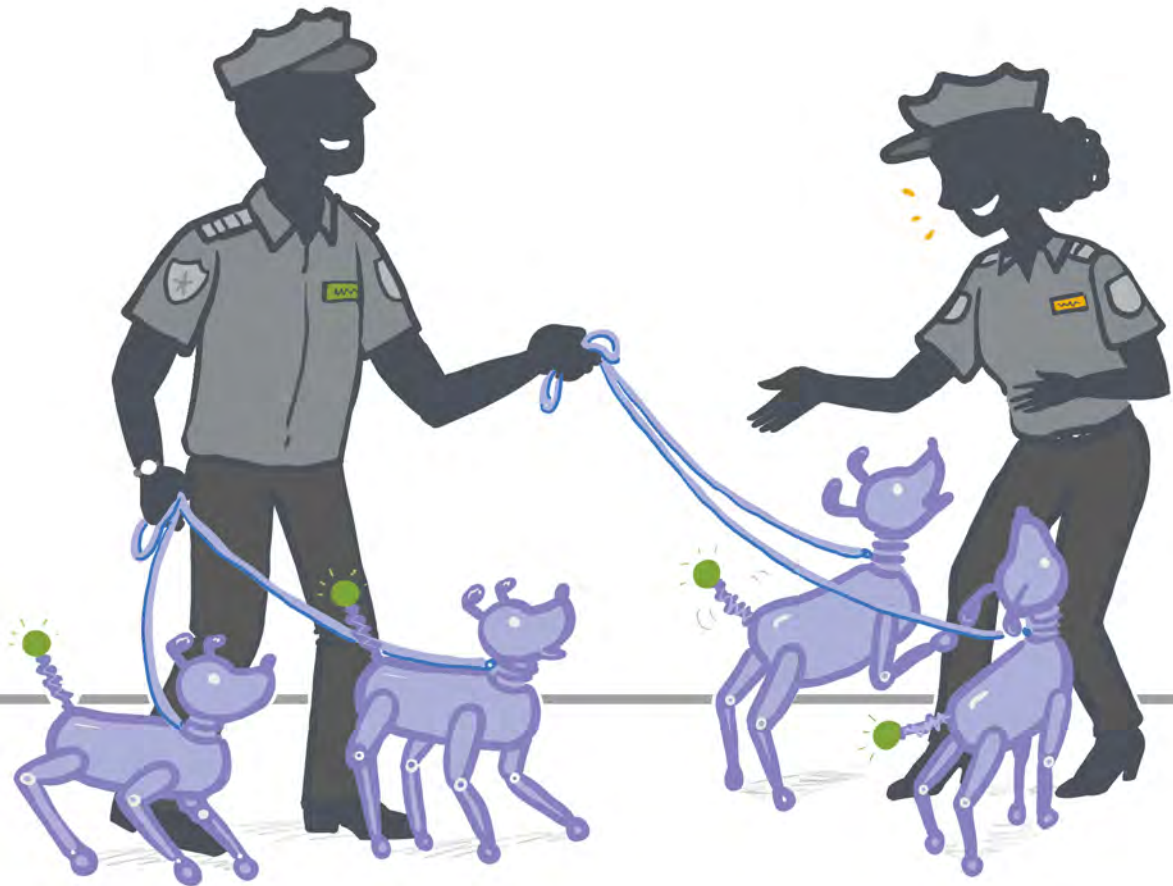
And problems can be fixed wherever you find them...



...effectively safeguarding users, applications, and infrastructure by extending security to all points of connection across the network.



Are you connected?



SIMPLIFIED: CONNECTED SECURITY

<https://www.juniper.net/us/en/solutions/security/>



© 2019 by Juniper Networks, Inc. All rights reserved.

Juniper Networks and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo and the Junos logo, are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Text by Michael Bushong and Trevor Pott. Concept by Tarek Radwan. Illustrated by Debora Aoki.

Published by Juniper Networks Books August 2019 3 4 5 6 7 8 9 10