RSA

THE 7 BUILDING BLOCKS OF BETTER THREAT VISIBILITY

BUSINESS-DRIVEN SECURITY™

To have a fighting chance against the next cyber threat to your organization, there's one simple principle to keep in mind.

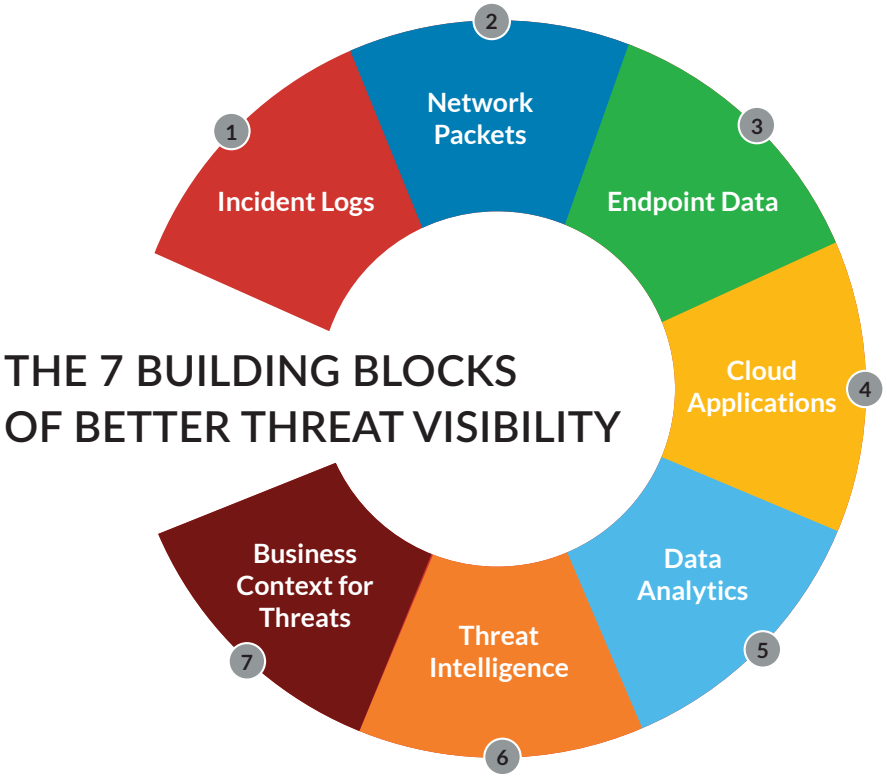
If you can't see it, you can't stop it.
And these days, there's plenty to see. Mobile, cloud and the internet of things are constantly expanding the attack surface, giving more openings to attackers.

The problem is you can't always see an attack coming. (And they're coming, all right—every 39 seconds, according to one study[1]). Sure, data from logs can provide your security team with clues when a known threat is looming. But what about when a zero-day attack you've never seen before is about to hit? After all, that's one of the biggest concerns security professionals have today.

To see what threats you're up against, you need visibility into all the data available from logs, packets, endpoints and threat intelligence, as well as a complete contextual view across all those sources.

[1] "Hackers Attack Every 39 Seconds," Security Magazine, February 10, 2017

THE 7 BUILDING BLOCKS OF BETTER THREAT VISIBILITY



You can put together a complete picture of threats with these building blocks. (Learn more about them on p. 7-8)

When you're able to take stock of everything that's coming at you, you can quickly assess the potential impact, so you can prioritize protecting what matters most to the business.

The stakes are high, with losses to cybercrime expected to climb to $6 trillion by 2021.[2]

Being on the winning side begins with more visibility.

$6 trillion
anticipated losses to cybercrime by 2021

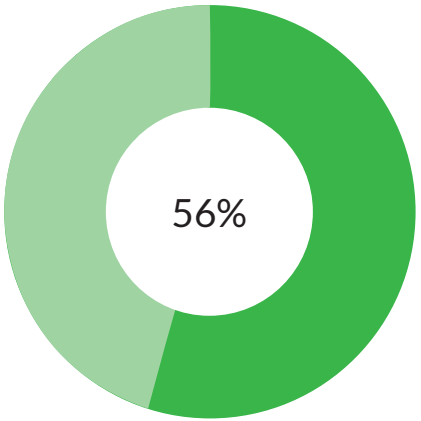
#1 concern of IT execs
keeping up with new threats

"To see what threats you're up against, you need visibility into all the data available from logs, packets, endpoints and threat intelligence, as well as a complete contextual view across all those sources."

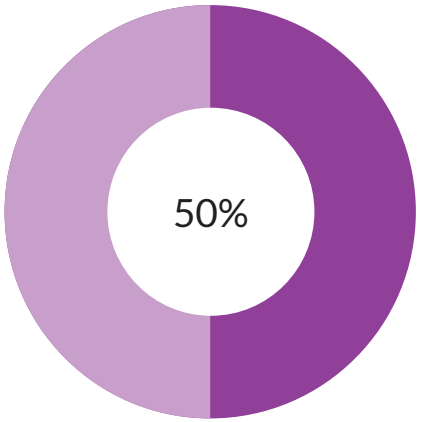
[2] 2016 Cybercrime Report, Cybersecurity Ventures, 2016

3 TOP THREAT DETECTION CHALLENGES

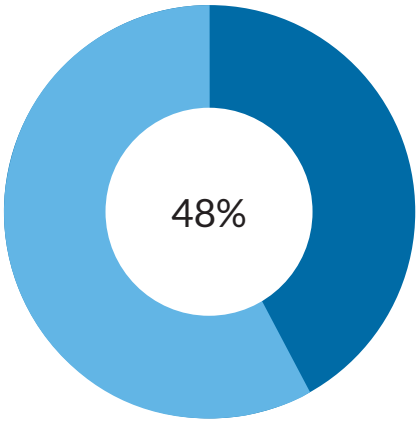
More visibility could give today's IT executives an advantage over their top three threat detection challenges. When we asked about what challenges they face, they said:



Keeping up with new threats, including zero-day threats



Understanding the full scope of the attack



The ability to detect an attack while it's in progress

Source: "Information Security Strategies in the Age of Zero-Day Threats," Gatepoint Research PulseReport commissioned by RSA, April 2017

START WITH LOGS (JUST DON'T STOP THERE)

Logs are a critical component in any cybersecurity infrastructure. They can tell you when a preventative control in your security infrastructure—an anti-virus application, for example—has detected signs of a problem and triggered an alert.

That's 100% useful.

Assuming the problem is caused by malware, and not by someone logging in using stolen credentials.

And that it isn't a whole new kind of malware that the control won't recognize.

And that it's not a zero-day attack that's coming in through a software weakness that hasn't been patched yet.

Logs can't give you visibility into any of those things.

So you start adding other sources of data—network traffic monitoring, packet capture, endpoint security, cloud security—to alert you to more kinds of threats.

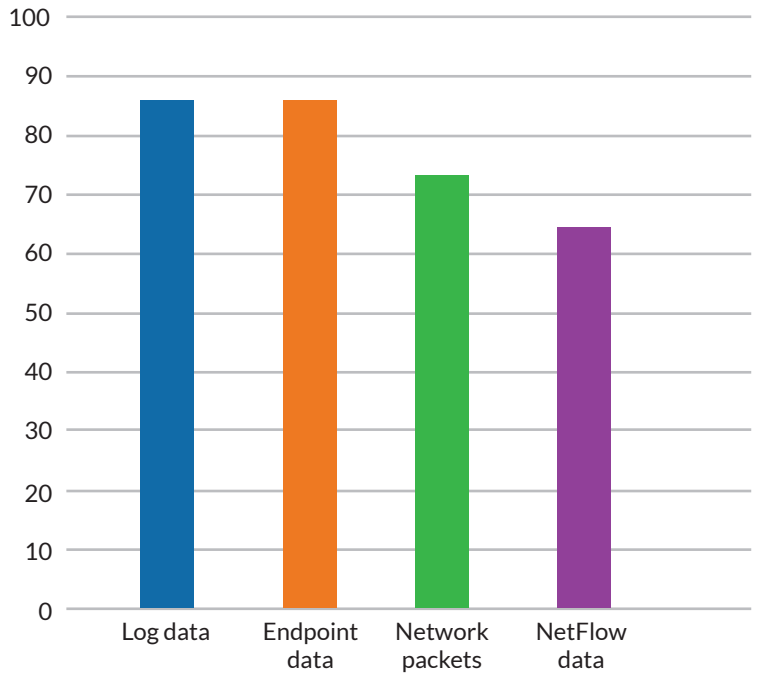
And before you know it, your team has more data coming at them than they can possibly keep up with, especially when there's no way to correlate information across all these sources and no business context for the data to help set priorities.

That's exactly what happens to a lot of organizations, according to a study RSA commissioned. The vast majority of IT executives surveyed reported having security tools to collect, monitor or analyze logs, endpoint data and network packets. But only 38% reported being able to correlate the data well.

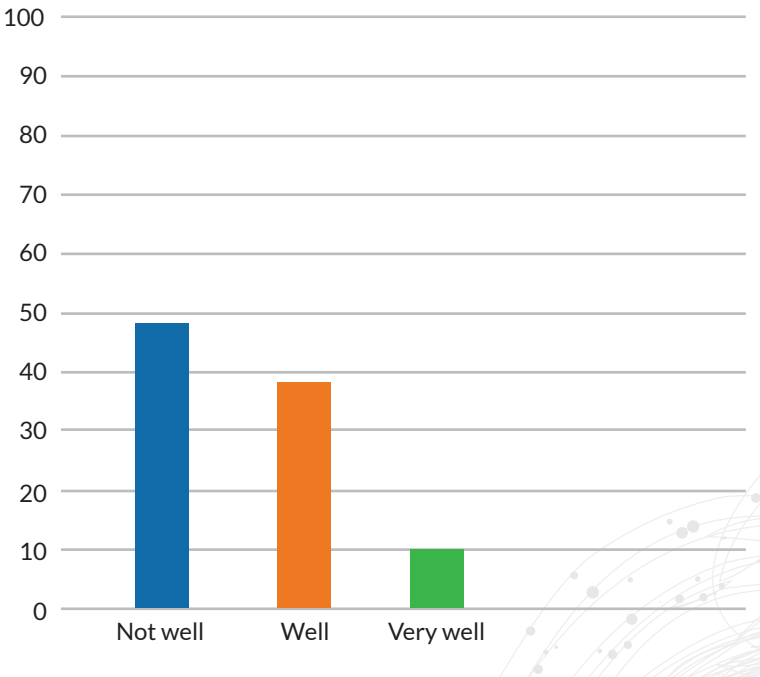
Time to step back and rethink your strategy.

SURVEY SAYS

Do you have security tools that collect, monitor or analyze the following?



How well can you correlate data coming from different sources?

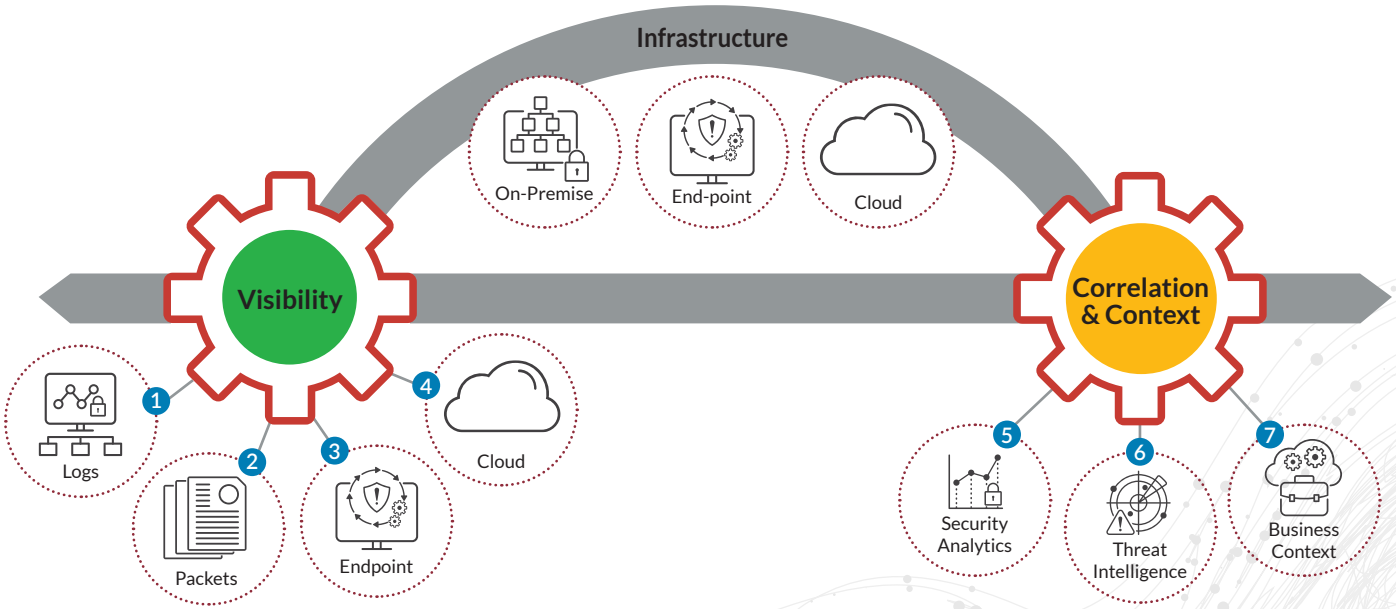


Source: "Information Security Strategies in the Age of Zero-Day Threats," Gatepoint Research PulseReport commissioned by RSA, April 2017

SEE WHAT YOU'RE MISSING

Visibility into logs, packets and endpoints is important, so that your team can identify threats wherever they appear. But you also need that visibility throughout the entire IT infrastructure—from endpoints to the cloud—so your view extends into all the places your organization does business.

Visibility across these sources of data, informed by security analytics, threat intelligence and business context, is even more important to a full understanding of what's happening in the threat environment. With the level of visibility these seven building blocks give you, you can be confident the team always has a full view of what's coming, unimpeded by any failure to connect and correlate the data.



The 7 Building Blocks of Better Threat Visibility

BRINGING THE VIEW INTO FOCUS

Data analytics

Data analytics provides information to detect threats and to prioritize responses. Once threats are visible, analytics can bring a laser focus to decisions about how to strike back.

Data analytics includes behavioral analytics to detect when user behavior signifies a potential threat, data science modeling to identify threats and machine learning to create baselines for what's normal (and what's not) in network and endpoint activities.

Threat intelligence

Time to fight smart: Threat intelligence from analysts and experts, as well as intelligence crowdsourced from the community of users, adds a layer of context with which to identify threats and plan how to respond.

Threat intelligence can be applied across logs, packets and endpoints to look at threat data in context and prioritize responses accordingly.

Business drivers

When your organization is inundated by threat data, it can be hard for the security team to know which threat they need to fight off first. But if they know the business context in which threat data is appearing, they can act quickly and decisively against whatever poses the greatest risk to the business.

Business context is the information that lets your team know, for example, whether a server at imminent risk for attack holds all the organization's source code—or just its daily lunch menu.

GOOD CATCH: PHISHING ATTACKS

Better visibility into threat data means a better chance of catching a phishing attack before it can inflict major damage. According to RSA's 2017 Global Fraud and Cybercrime Forecast:

- There were more phishing attacks in 2Q 2016 than in all of 2015
- A new phishing attack is launched every 30 Seconds
- Phishing costs global organizations $9.1 billion annually

MORE VISIBILITY WITH RSA NETWITNESS® SUITE

Target the real threats to your organization, with RSA NetWitness Suite providing complete, integrated visibility into the threat environment. Rely on it to:

- Collect large amounts of data across capture points—logs, packets, endpoints, NetFlow
- Extend visibility into compute platforms beyond the physical infrastructure, including the cloud
- Provide context for what you see, based on analytics, threat intelligence and business drivers

RSA NetWitness Suite is an RSA Business-Driven Security™ solution, integrating with RSA NetWitness SecOps Manager to match alerts to specific business assets and define how critical each asset is to business operations.

Visibility is just the start. Learn more about how RSA NetWitness Suite speeds your response to threats and increases the impact with your existing team.

RSA NetWitness® Suite

RSA NetWitness® Suite is a threat detection and response platform that enables organizations to be three times as impactful in identifying and responding to the full scope of a compromise by leveraging logs, packets, endpoints, business context and threat intelligence. For more information, go to rsa.com/netwitness.

- 3X more visibility
- 3X faster response
- 3X security team impact