proofpoint.

SOLUTION BRIEF

Proofpoint + RSA NetWitness

Email security events in your SIEM.



Key Benefits

- Bring email gateway events into the SIEM you already run
- Run your SIEM's reports and alerts on Proofpoint events
- Set up and control the export yourself

Email Events With Your Security Data

Security teams use SIEMs to monitor, correlate, and alert across their tools. An email gateway with events the SIEM can't read becomes a blind spot, and analysts end up checking a separate console to investigate email events. Proofpoint Email Protection (formerly Proofpoint Protection Server, PPS) can forward its mail-flow and filter logs by syslog to your own SIEM, and a Proofpoint event source on your NetWitness SIEM (RSA's former SIEM line) parses them, so email events sit alongside your other security data for reports and alerts.

Send Email Logs to Your NetWitness SIEM

Admin-Controlled Export	Proofpoint Event Source
Proofpoint Email Protection An administrator turns on MTA Syslog and Filter Syslog and sets the log level, remote host, and protocol (UDP or TCP). Email Protection forwards its mail-flow and filter logs to your own SIEM, on-premises or on Proofpoint on Demand, and nothing is sent to RSA or NetWitness.	**NetWitness SIEM** A Proofpoint parser on the NetWitness Log Decoders turns Email Protection logs into events the SIEM can use. Teams run the SIEM's reports and alerts on them, alongside their other sources, with no new console.

Extend Your SIEM to Email

NetWitness is one of several SIEM platforms Proofpoint Email Protection works with, and you configure and control the export. The export covers mail-flow and filter logs, not TAP threat events, and Proofpoint on Demand customers need the remote syslog license. To see how this could fit your environment, including your PPS version and NetWitness deployment, talk to your Proofpoint representative.

Learn more: proofpoint.com/us/partners/vmware-carbon-black

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com
Connect with Proofpoint: LinkedIn

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries.
All other trademarks contained herein are the property of their respective owners.

proofpoint.