NETWORK HEROES

THE PHANTOM MALWARE

ManageEngine | AN FSO COMIC SERIES | Story by Sharon A. Ratna

Welcome to Antar, a city where even the streetlights have API endpoints.


All was calm until a glitch pulsed through the heart of the city's IT grid...

Zylker Corp.
Midnight shift.

ZYLKER NETWORK COMMAND HUB

SOC + NOC HYBRID

72%

Hi, I'm Eva Harson, Chief IT and Cyber Response Admin at Zylker Corp.

Something's wrong...

WHIR WHIR

The system detects an anomaly in the network traffic.

ANOMALY DETECTED

Source: Unknown /...

Threat Level: CRITICAL

Eva boots Zia, Zylker Corp's AI-powered network monitor.

Harson, our adaptive thresholds'baseline deviation exceeds tolerance.

Zia quickly scans the entire network with full-stack observability

There's an east-west traffic spike in Legacy Subnet 12. Unauthorized lateral traversal. Probability of malware: 0.91.

It's time to suit up!

Zia, prep Deep Packet Inspection mode. It's time to enter the network fabric.

Zia opens the portal...

ZYLKER NETWORK COMMAND HUB

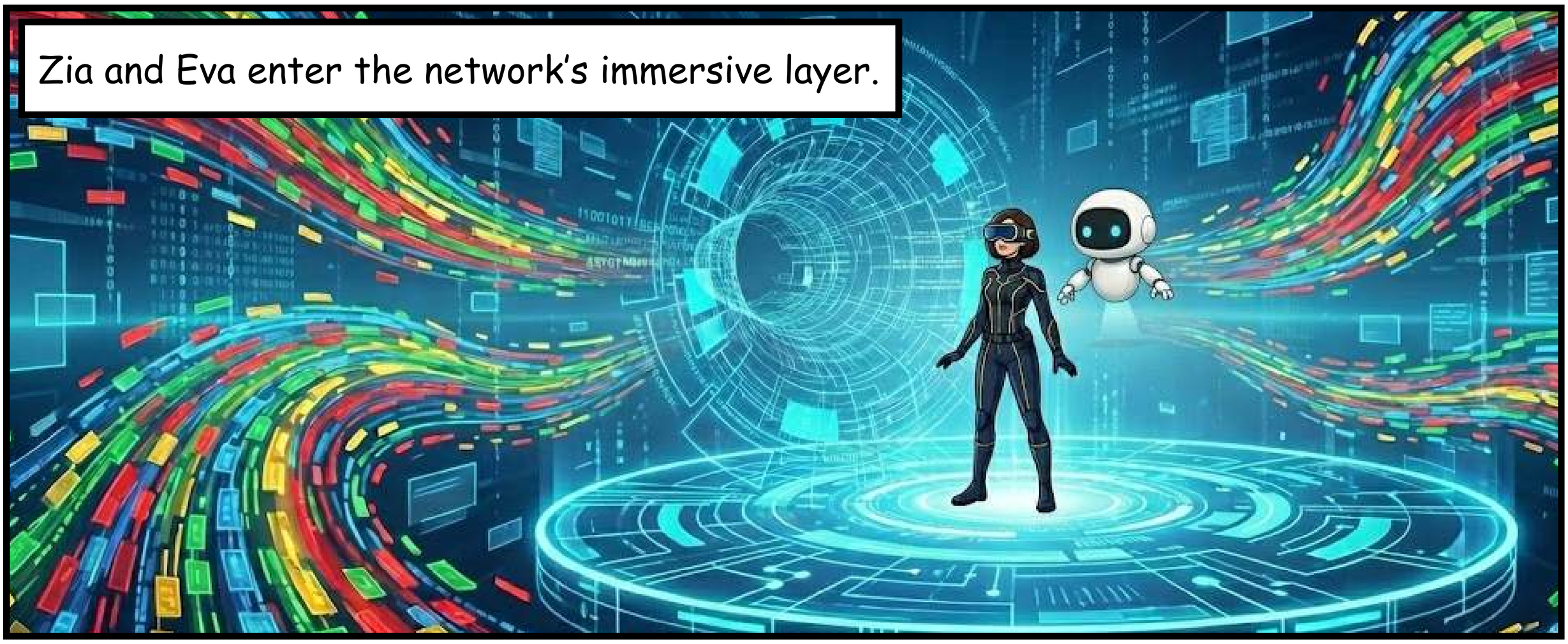
SOC NOC

ZAP!

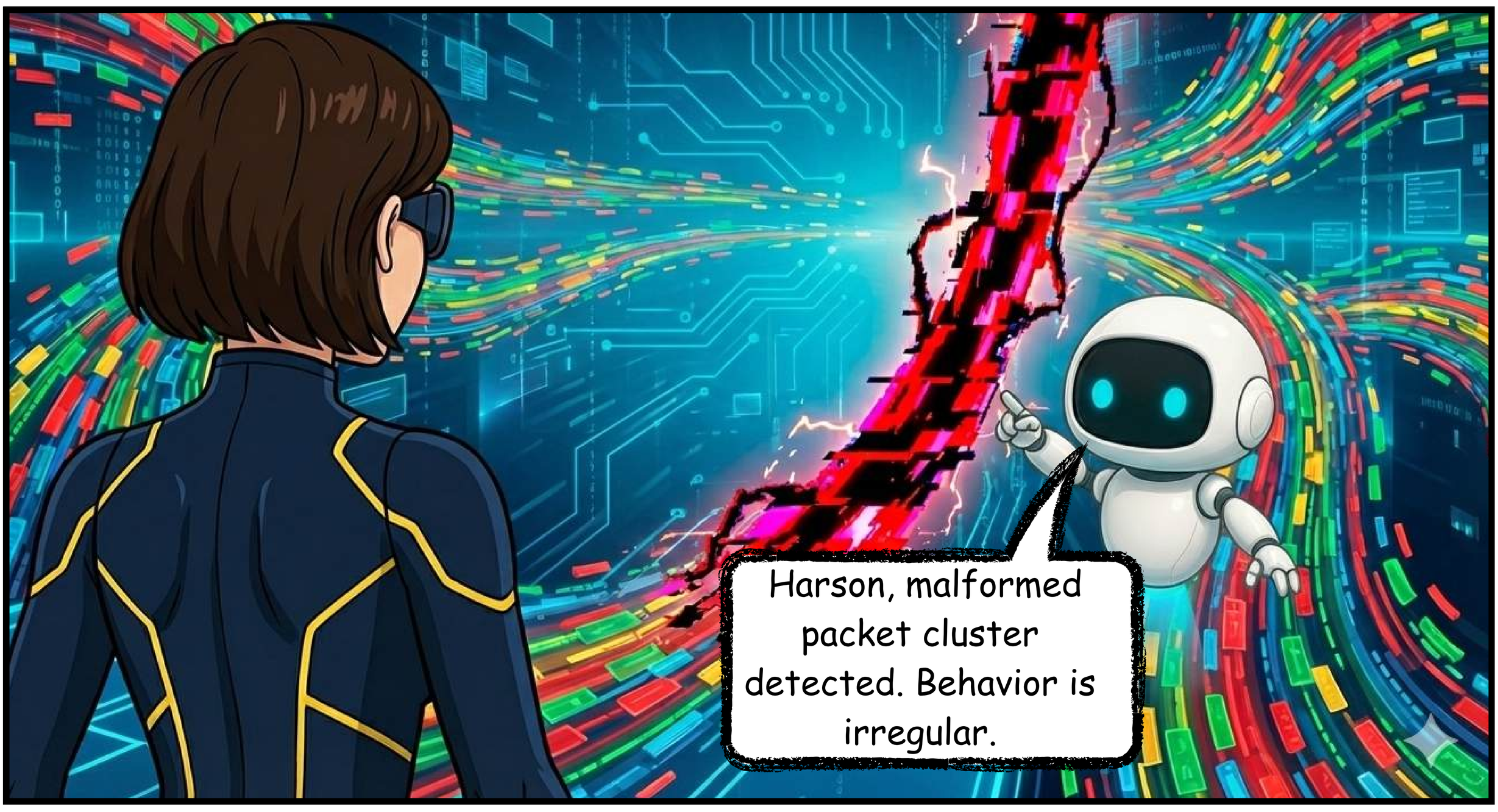
Harson, let's go!

ZAP!

VREEM!


Zia and Eva enter the network's immersive layer.


SCANNING...
BZZZT!


Harson, malformed packet cluster detected. Behavior is irregular.

Shade, a digital cryptid, emerges from the malformed packets.

Harson, polymorphic signature confirmed. Threat: aggressive.

We need to catch this before it's too late. Zia, INSPECT!

It's pivoting. Credential theft suspected. Initiating trace.

Shade zooms into an encrypted tunnel.

Zia, launch the Deep Packet Inspection engine —we can't let it escape!

Analyzing... Warning!!! This signature doesn't exist in any known database.

ERR_NOISE

ERR_NOISE

This looks like a zero-day.

Ah yes... that story never gets old!

HARSON!!! LOOK!!!!

BZZZ

Zia! Maybe warn me BEFORE homicidal packets spawn behind me?

Haha!!! A basic traffic block? Seriously?

Initiating packet behavior analysis. Harson! It forked its process!

It's going to take more than that to bring down my IT!

One commit reverted!

Have fun playing whack-a-packet!

It's heading for the Core Vault!

It's routing through the legacy subnet. Tag and track, Zia!

They follow Shade into the legacy subnet— forgotten but still active.

Entities communicating with outdated protocols...

Yep... this place. I warned them about decommiss ioning.

Shade extracted stale LDAP credentials. The system's previous password rotation alerts: **IGNORED!**

Movement pattern accelerating. East-west traversal is at high risk.

It's using a stolen identity to pivot.

BEHAVIOR HEATMAP
THREAT LEVEL : EXTREME
CRITICAL ANOMALY
UNSTABLE DATA FLOW

Launching behavior analysis. Zia, predict next hop.

BEHAVIOR HEATMAP
MOVEMENT PREDICTION MAP

Predicting next hop: 78% chance toward the core.

MOVEMENT PREDICTION MAP

Then let's cut it off!

They sprint toward a glowing corridor of high-speed traffic.

Dashboard

Shade is not far from the core.

Suggestion: Honeypots

Eva builds a data honeypot to lure Shade.

Let's trap it in this microsegment!

Sounds like a plan!

Shade assesses the dataset...

Shade enters into the honeypot with stolen credentials.

The microsegment closes in, restricting Shade's lateral movement.

Arghhh... It's a darn trap!

But that's no match for me!

Shade's advanced attack tactic shatters the microsegment containment.

SERIOUSLY!!!

Microsegment compromised.
Threat level: Critical.

Power up, Zia.
Let's end this!

Path analysis initiated for the core

Eva and Zia chase Shade into the network core.

Shade enters the network core through a compromised tunnel.

Eva and Zia are not far behind!

Harson, Shade has entered through the backdoor caused by a developer credential leak.

ZAP!

CRACKLE!

Ah!

CRACKLE!

KZZZT!

GLITCH!

ERROR!

BZZZT!

Threat battle mode: Initiated.

BZZZT!

PACKET REWRITE
TRAFFIC REROUTE
AUTO-CONTAINMENT
Initiating packet rewrite.
Enabling traffic rerouting.
AUTO CONTAINMENT!

Zia launches security workflows and forces Shade into a collapsing data tunnel.

Ahhhhh noo!
I will be back!

POOF

The network lives another day!

And people think IT is boring.

Back at Zylker Corp, Zia and Eva return to their peaceful shift...

What say you, Zia, should we tell them our secret?

Yes, Eva!!! Let's help our fellow IT admins.

"EVA?" That's new!

MEET OPMANAGER PLUS: THE DETECTION ENGINE BEHIND EVA AND ZIA'S SUCCESS

1.Detect threats the moment they slip into your flow fabric

OpManager Plus' advanced security modules such as ASAM and Firewall log analyzer analyze security data (NetFlow, sFlow, IPFIX, etc.) to flag abnormal traffic patterns, spikes, scans, DDoS attacks, and other anomalies in real time.

2. Hunt stealthy attackers across north-south and even east-west traffic

By monitoring records from routers, switches, firewalls, and interfaces, OpManager Plus provides deep visibility into internal traffic, helping detect lateral movement, credential misuse, and sudden communication changes often missed by traditional tools.

3. Predict intent with behavior-based, MITRE-ATT&CK®-aligned classification

The ASAM maps suspicious behaviors, such as scanning, probing, and data exfiltration, to known attacker tactics, giving teams clear context and enabling faster decision-making using a familiar ATT&CK-style framework.

4. Reveal evasive activity with DPI and advanced behavior analysis

Our NetFlow module supports deep packet inspection to break down traffic by application, protocol, and service signatures. This adds deeper visibility when analyzing suspicious flows.

5. Strengthen security response with remote configuration deployments and seamless integrations

Our Configuration Manager lets you track and deploy network configuration changes from a single console. Built-in integrations enable OpManager Plus to seamlessly integrate with existing security workflows by forwarding alerts to security solutions and IT desk tools.

OUR NETWORK HEROES HANDLE MORE THAN JUST SECURITY THREATS.

From gaining visibility into your complete network stack to finding vulnerabilities at the firmware level, make sure your network is up and running with ManageEngine's suite of full-stack observability products. Check network availability, application performance, traffic, configurations, DDI metrics, and even firewall logs with a unified solution. Get started today!

Check-out our AI-powered solutions at www.manageengine.com/fso

THE NETWORK HAS FALLEN...

At Zylker Corp's NOC + SOC command hub, Chief IT admin Eva and her AI-powered observability sidekick Zia spot a critical anomaly. A digital cryptid, infamously known as 'Shade', is traversing laterally deep into their forgotten legacy subnet. Eva and Zia must stop its malformed packets and zero-day threats before it breaches the core network.

manageengine.com/fso