



**FORTINET**

# FortiGuard AI-powered Security Services



# Threat Landscape That is More Complex Than Ever

## LONG-LIVED EXPLOITS



98% of firms saw exploits created over five years ago

## NEW VULNERABILITIES



17% YoY growth in new vulnerabilities

## TARGETED ATTACKS ON THE RISE



More time on specific vectors vs spam

## APT THREAT ACTORS



30% of APT groups were detected as active in 1H 2023

## INDUSTRIAL RANSOMWARE



44% of ransomware and wipers targeted OT

## CLOUD RISKS



69% of companies use two or more clouds

## SUPPLY CHAIN ATTACKS



12% of data breaches originated with a software supply chain attack

## INSIDER RISK



+32% year-on-year increase in insider risk incidents



# Challenges Facing Security Teams



## Attackers have More Resources

- Threat actors constantly looking for ways into your network
- Initial access sold to ransomware gangs



## Digital Transformation is expanding the Attack Surface

- Ever-growing IOT digital footprint
- Dynamic cloud assets
- Mergers & acquisitions



## Security teams are stretched

- Cybersecurity skills shortage
- Firehose of information
- New attack vectors
- New TTPs



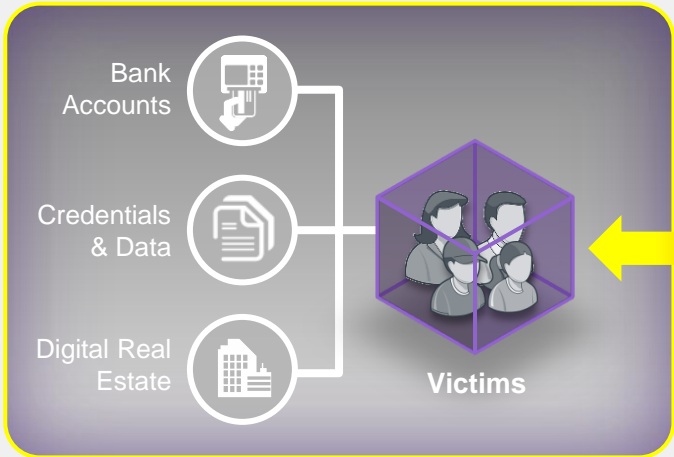
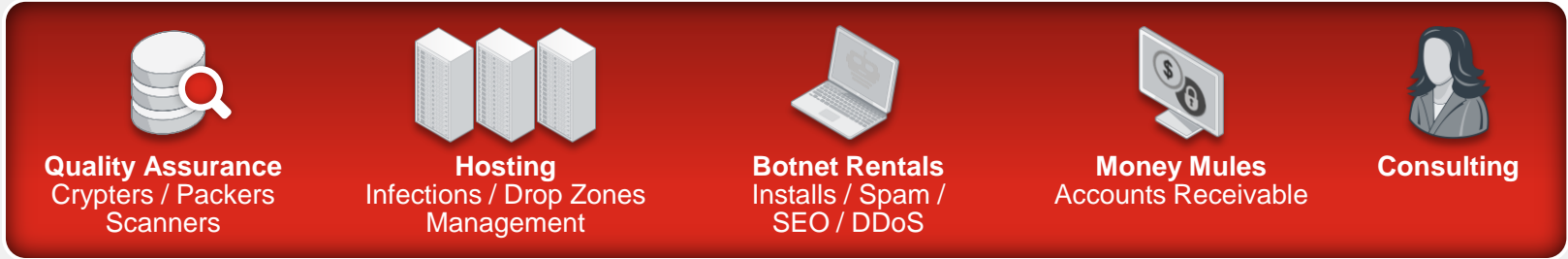
## Damages to Brand Perception Impact Company Value

- Market valuation
- Revenue and customer faith/loyalty
- Customer safety
- Business credibility

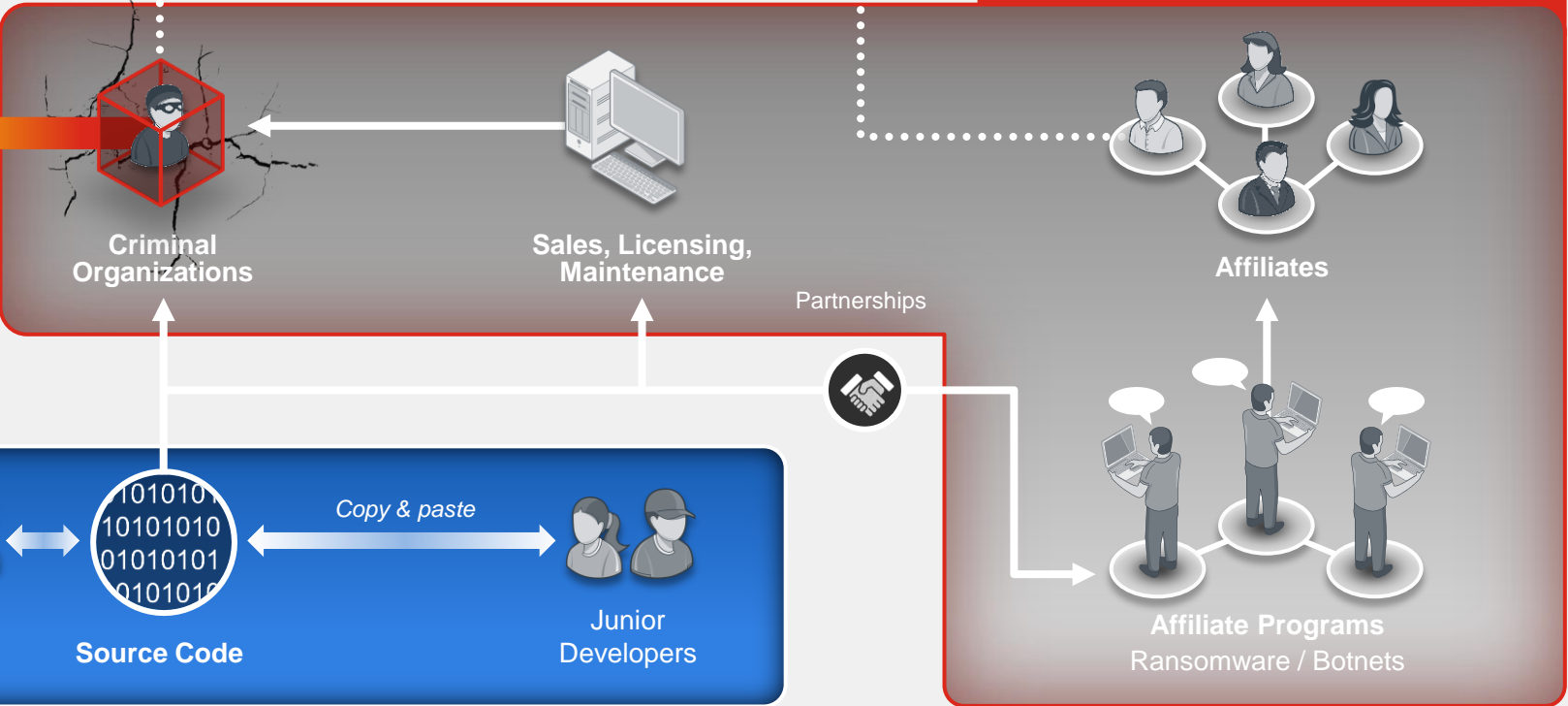
Urgent need to gain visibility of the entire attack surface and prioritize remediation

# Cybercriminal Ecosystem

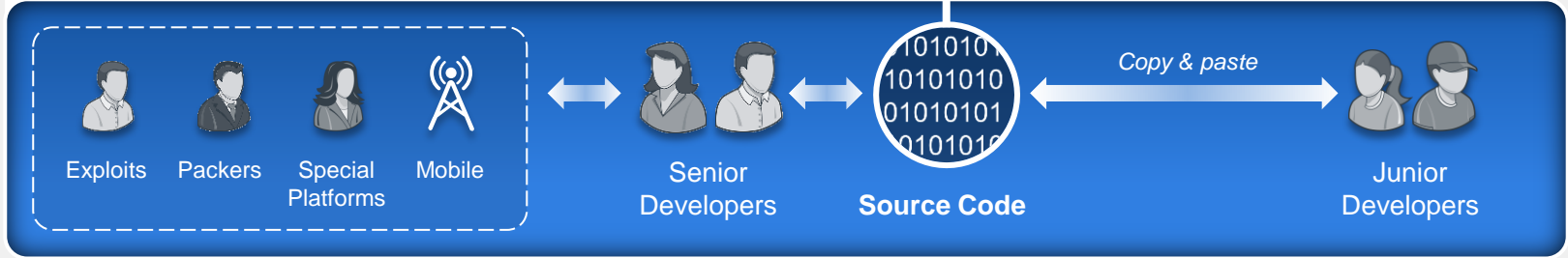
## CRIME SERVICES ENABLERS



## COMPOUNDED CYBERCRIME



## CRIMEWARE PRODUCERS





# FortiGuard Labs

2002

Founded

1K+

Researchers, Threat Hunters,  
Engineers, Analysts and  
Data Scientists

1K+

0-days discovered &  
Reported

Global  
Alliances



MITRE

AI-Powered  
Threat  
Intelligence for  
an Evolving  
Digital World

Monitors the Threat  
Landscape / Formulates  
Threat Intelligence

Conducts Zero-Day and  
Other Threat Research

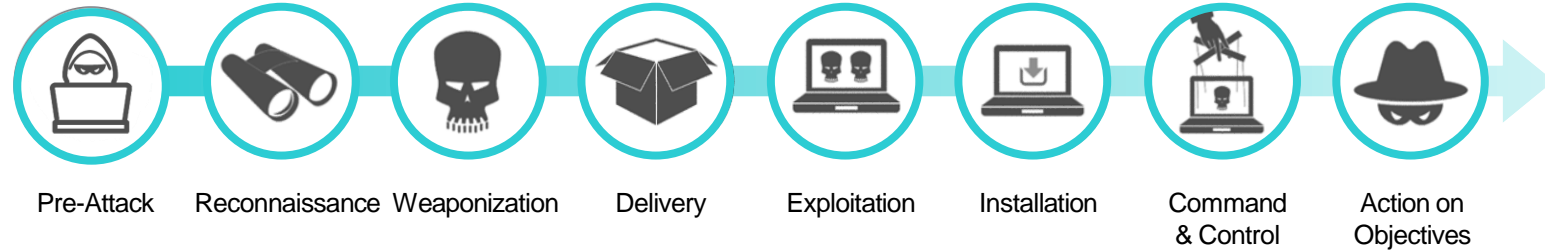
Develops and Enhances  
FortiGuard AI-powered  
Security Services

Publishes Outbreak  
Alerts, Threat Briefs,  
Threat Predictions, and  
Other Reports

# Understanding Your Posture

## Digital Risk Prevention

Mitigating risks to your external attack surface



### Attack Surface Management

Monitor and remediate external and internal attack surfaces



### Brand Protection

Detect Brand Impersonation, web site typo-squatting, rogue applications



### Adversary Centric Intelligence

Curated FortiGuard Threat Intelligence



# Enabling Coordinated Network Detection and Response

FortiGuard Labs News / Research Services Threat Intelligence Resources About FEATINET

## Outbreak Alert

### PAN-OS GlobalProtect Command Injection Vulnerability

Released: Apr 12, 2024 Updated: Apr 22, 2024 [Download PDF »](#) [SHARE](#)

**PAN-OS GlobalProtect Attack** Critical Severity Routers Platform Palo Alto Vendor Attack Type

Overview Analysis **Solutions** Threat Intelligence References Subscribe

### FortiGuard Cybersecurity Framework

Mitigate security threats and vulnerabilities by leveraging the range of FortiGuard Services.

PROTECT	DETECT	RESPOND	RECOVER	IDENTIFY
<ul style="list-style-type: none"><li>AV</li><li>AV (Pre-filter)</li><li>IPS</li></ul>	<ul style="list-style-type: none"><li>Outbreak Detection</li><li>Threat Hunting</li><li>Playbook</li></ul>	<ul style="list-style-type: none"><li>Assisted Response Services</li><li>Automated Response</li></ul>	<ul style="list-style-type: none"><li>NOC/SOC Training</li><li>End-User Training</li></ul>	<ul style="list-style-type: none"><li>Attack Surface Hardening</li><li>Inventory Management</li><li>Business Reputation</li></ul>

**IPS** Detects and blocks exploitation attempts targeting the PAN-OS Global Protect vulnerability (CVE-2024-3400) X

- FortiGate DB 27.768
- FortiSASE DB 27.768
- FortiNDR DB 27.768
- FortiADC DB 27.768
- FortiProxy DB 27.768

**AV** Detects and blocks known malware related to the PAN-OS GlobalProtect Attack (CVE-2024-3400) X

- FortiGate DB 92.03313
- FortiWeb DB 92.03313
- FortiClient DB 92.03313
- FortiSASE DB 92.03313
- FortiMail DB 92.03313
- FortiCASB DB 92.03313
- FortiCWP DB 92.03313
- FortiADC DB 92.03313

**AV (Pre-filter)** Detects and blocks known malware related to the PAN-OS GlobalProtect Attack (CVE-2024-3400) X

- FortiProxy DB 92.03313
- FortiEDR DB 92.03313
- FortiSandbox DB 92.03313
- FortiNDR DB 92.03313

## Scan and Sign-up

Two green downward arrows pointing to a QR code.

The background features a grid of light grey squares and semi-circles. A red horizontal bar is positioned at the top left. Another red horizontal bar is located in the upper right quadrant, partially overlapping a grey square. A third red horizontal bar is at the bottom left. In the bottom right, there is a grey square with a vertical bar on its right side and a grid of small grey dots to its left.

**F**  **RTINET**