Radware ERT Services

Experience. Intelligence. Expertise.

Three ingredients to boost your application and network security

Today organizations care about securing sensitive network assets and ensuring the availability of applications and services. Keeping confidential data secure and being able to protect it from sophisticated attacks have become a burden for organizations' IT departments. There are two reasons for this. First, they cannot maintain and develop the expertise in-house. Second, they do not move as fast as threats do and fail to address newly introduced attack vectors.

Since service availability is a key factor for businesses today, there is little room for trial and error in the event of a cyberattack. Even during peacetime, organizations must reduce the attack surface as much as possible and prevent threat actors from getting anywhere near their valued assets. Maintaining application service-level agreements (SLAs), keeping data confidential and assuring performance and flow are all critical requirements that are complex to achieve in today's threat landscape. Organizations that struggle to maintain updated knowledge of this threat landscape require access to security expertise and real-time intelligence to protect their network assets, applications and data. Even with the best protection devices and a knowledgeable staff, denial-of-service (DoS) attacks, application exploits and malware outbreaks are a major challenge to your business and can create unwanted situations. As threats evolve and become more complex, security needs to be managed by experts.

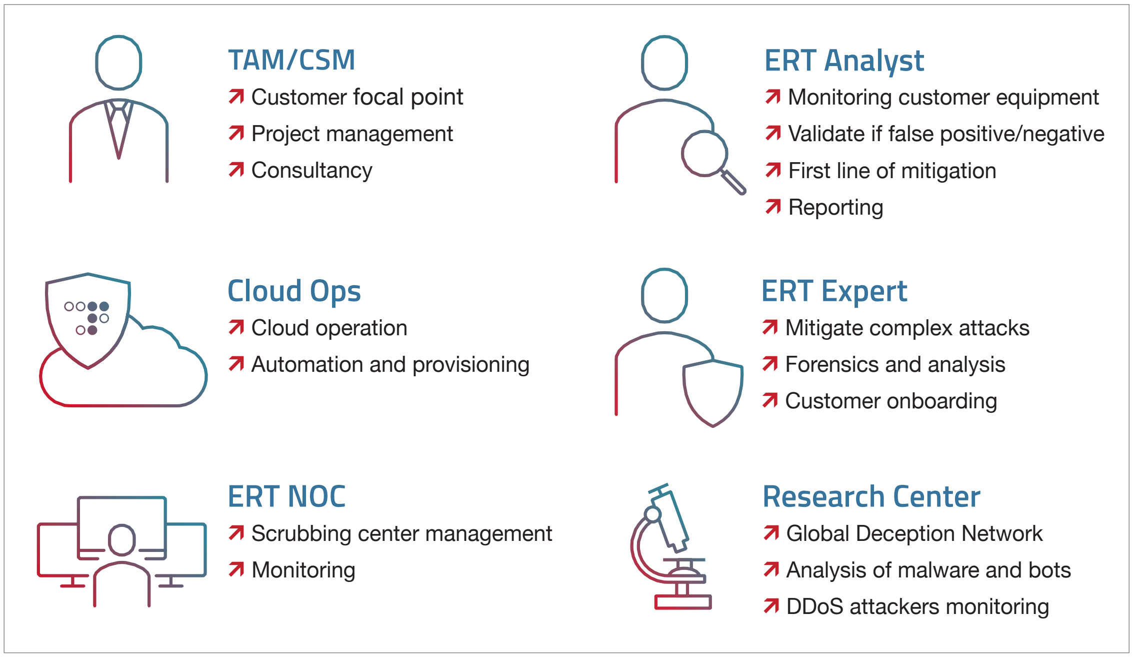
Meet Radware's Emergency Response Team

Radware's Emergency Response Team (ERT) is a group of security experts available 24x7 for proactive security support services for customers facing an array of application- and network-layer attacks. The ERT features experienced security engineers for immediate response and escalation, as well as reputable threat researchers who have brought to market discoveries like the BrickerBot and JenX internet of things (IoT) botnets, CodeFork malware and more. They leverage a global threat-detection network to provide a real-time threat intelligence feed to organizations around the globe.

The team engages in security events such as DoS attacks, malware outbreaks and application exploits. Radware's ERT security analysts and engineers combat common and emerging attacks on a daily basis, providing customers with industry-leading expertise, best practices and a deep knowledge of threats, attack tools, intelligence and mitigation technologies.

Figure 1

ERT roles and responsibilities



TAM/CSM
- Customer focal point
- Project management
- Consultancy

ERT Analyst
- Monitoring customer equipment
- Validate if false positive/negative
- First line of mitigation
- Reporting

Cloud Ops
- Cloud operation
- Automation and provisioning

ERT Expert
- Mitigate complex attacks
- Forensics and analysis
- Customer onboarding

ERT NOC
- Scrubbing center management
- Monitoring

Research Center
- Global Deception Network
- Analysis of malware and bots
- DDoS attackers monitoring

Effective Security with Radware's ERT

Expertise and intelligence are a must-have against evolving threats. Radware's ERT provides an extended scope of value-added services, bringing to market the fastest under-attack service, a fully managed application- and network-security service and threat intelligence subscriptions.

Security Protection Services

ERT Under-Attack Service
ERT Managed Service

Threat Intelligence Subscriptions

ERT Security Update Service
ERT Active Attackers Feed

ERT Managed Security Service

Radware's ERT offers a fully managed application- and network-security service. The service is provided 24x7 by security experts and covers a broad range of attack types from different forms of DoS to a variety of application attacks against your servers or data centers. It includes immediate response, onboarding, consulting, remote management and reporting.

Technical Account Manager

Quarterly optimization and software upgrade

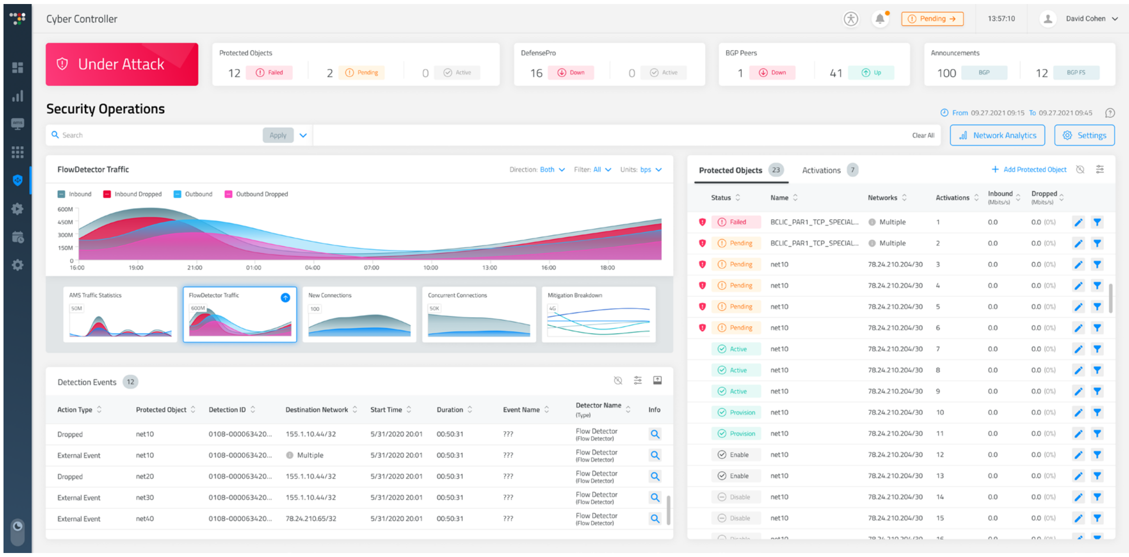
Monthly security reports

24x7 monitoring

24x7 designated support engineers

Figure 2

Screenshot of online dashboard



Detection Events 12

Action Type	Protected Object	Detection ID	Destination Network	Start Time	Duration	Event Name	Detector Name (Type)	Info
Dropped	net10	0108-000063420...	155.1.10.44/32	5/31/2020 20:01	00:50:31	???	Flow Detector (Flow Detector)	
External Event	net10	0108-000063420...	Multiple	5/31/2020 20:01	00:50:31	???	Flow Detector (Flow Detector)	
Dropped	net20	0108-000063420...	155.1.10.44/32	5/31/2020 20:01	00:50:31	???	Flow Detector (Flow Detector)	
External Event	net30	0108-000063420...	155.1.10.44/32	5/31/2020 20:01	00:50:31	???	Flow Detector (Flow Detector)	
External Event	net40	0108-000063420...	78.24.210.65/32	5/31/2020 20:01	00:50:31	???	Flow Detector (Flow Detector)	

Protected Objects 23 Activations 7

Status	Name	Networks	Activations	Inbound (Mbits/s)	Dropped (Mbits/s)
Failed	BCLIC_PAR1_TCP_SPECIAL...	Multiple	1	0.0	0.0 (0%)
Pending	BCLIC_PAR1_TCP_SPECIAL...	Multiple	2	0.0	0.0 (0%)
Pending	net10	78.24.210.204/30	3	0.0	0.0 (0%)
Pending	net10	78.24.210.204/30	4	0.0	0.0 (0%)
Pending	net10	78.24.210.204/30	5	0.0	0.0 (0%)
Pending	net10	78.24.210.204/30	6	0.0	0.0 (0%)
Active	net10	78.24.210.204/30	7	0.0	0.0 (0%)
Active	net10	78.24.210.204/30	8	0.0	0.0 (0%)
Active	net10	78.24.210.204/30	9	0.0	0.0 (0%)
Provision	net10	78.24.210.204/30	10	0.0	0.0 (0%)
Provision	net10	78.24.210.204/30	11	0.0	0.0 (0%)
Enable	net10	78.24.210.204/30	12	0.0	0.0 (0%)
Enable	net10	78.24.210.204/30	13	0.0	0.0 (0%)
Disable	net10	78.24.210.204/30	14	0.0	0.0 (0%)
Disable	net10	78.24.210.204/30	15	0.0	0.0 (0%)
Disable	net10	78.24.210.204/30	16	0.0	0.0 (0%)

Security Experts Will Take Care of It — ERT Under-Attack Service

The ERT under-attack service provides 24x7 access to a security expert within 10 minutes — the industry's fastest SLA. The ERT engineer will take the lead, fight off attacks and provide postmortem analysis of security events. The ERT under-attack service lets organizations know there is someone to rely on, guaranteeing support throughout the attack life cycle from the moment it begins. The battle-proven ERT experts are available 24x7 and assist large enterprises worldwide with complex multivector attacks against their networks, data centers and application services.

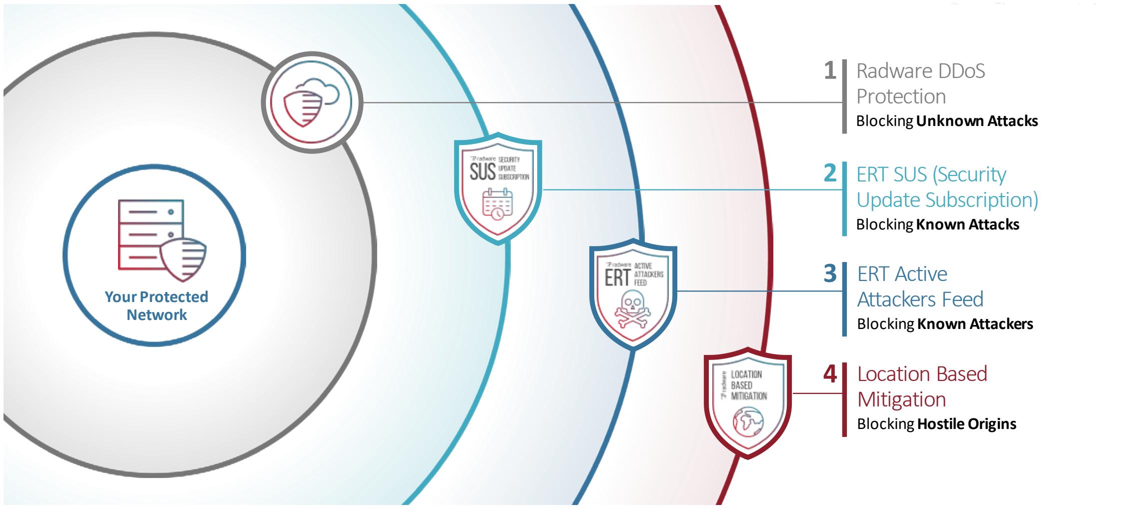
Keep Your Protections Current — ERT Security Update Service

Radware's ERT Security Update Subscription (SUS) is a security advisory and managed monitoring/detection system dedicated to protecting network elements, hosts and applications against the latest security vulnerabilities and threats. The service delivers rapid and continuous updates to current subscribers:

- **Periodic Updates** | Updates provide protection from the most recent known attack tools and vulnerabilities, such as DoS flooding tools; slow DoS attacks and tools; DoS single-packet vulnerabilities; and critical application vulnerabilities, such as the OWASP top 10 (including injections, password cracking, remote scripting, web scraping and more).
- **Emergency Updates** | When an immediate response is necessary, ERT will issue an emergency signature file update.
- **Custom Signatures** | Customers can contact Radware's ERT to report environment-specific or newly discovered threats and request signatures to mitigate them.

Figure 3

Multilayered defense


Your Protected Network
SUS SECURITY UPDATE SUBSCRIPTION
ERT ACTIVE ATTACKERS FEED
LOCATION BASED MITIGATION
1 Radware DDoS Protection
Blocking **Unknown Attacks**
2 ERT SUS (Security Update Subscription)
Blocking **Known Attacks**
3 ERT Active Attackers Feed
Blocking **Known Attackers**
4 Location Based Mitigation
Blocking **Hostile Origins**

Real-Time Preemptive Protection — ERT Active Attackers Feed

Radware's ERT Active Attackers Feed is a threat intelligence feed specifically designed to protect against emerging DDoS threats, including those involving IoT botnets and new DNS attack vectors. This new subscription service enhances Radware's Attack Mitigation Solution (AMS) by identifying and blocking IP addresses involved in major attacks in real time to offer preemptive protection from known attackers. It is another layer of defense on top of Radware's customer premise equipment (CPE) and SUS, which protect against unknown and known attacks. ERT Active Attackers Feed draws intelligence data from three main sources: Radware's Cloud Security Services, Radware's Global Deception Network (a global array of honeypots) and the company's experienced ERT, which deploys proprietary algorithms and manual research techniques to identify threats. These sources are correlated to generate a validated list of IPs involved in active DDoS attacks. That list is downloaded to AMS to block attacks before they target the network. The system then continuously monitors suspect IP addresses, taking them off blacklists when attacks have subsided to decrease the risk of false positives.

Preemptive Protection
against known DDoS attackers

Preemptively blocks attackers before they enter your network

Active Attackers
blocked in real time

Blocks IPs actively involved in DNS and IoT botnet DDoS attacks in 24 hours

Data Correlation
across multiple Radware sources

Correlates Cloud DDoS intelligence, Global Deception Network and real-life attack data

Location-based Mitigation

Radware's location-based mitigation solution is a service that enables network traffic filtering by countries and regions based on the geolocation mapping of IP subnets. Radware's solution also supports per-policy block and allow lists, making it a perfect solution for carriers and service providers that wish to protect multitenant networks. A dedicated dashboard shows the top attacking origins and helps select the protection mode — always active or on demand. This subscription helps organizations comply with global and industry regulation requirements (such as the Office of Foreign Assets Control and others).

Most Comprehensive Security Service Offering

- **Fastest Attack Mitigation**
  Fastest to detect, fastest to respond, fastest to resolve. Radware's ERT maintains a 10-minute SLA to provide organizations under attack with immediate access to security experts.
- **Fully Managed Service**
  Installation, tunings, management, consulting and immediate attack mitigation for application and network security by experienced professionals.
- **Preemptive Threat Intelligence**
  Actionable real-time data for immediate protection against active suspicious IPs. Access to Radware's Threat Research Center's alerts, advisories and attack reports.
- **Security Update Service**
  Continuous protection from the most recent known attack tools and vulnerabilities — ongoing signature files, rapid response to high-impact security events and development and distribution of custom filters.
- **Location-Based Mitigation**
  Network and data center protection from country-based DDoS attacks through immediate traffic filtering based on geolocation mapping of IP subnets, ensuring data flow alignment based on an organization's requirements.
- **Technical Account Management (Optional)**
  A fully dedicated and proactive cyber consultant. This person is the customer focal point for configuration, integration, upgrades and attack mitigation.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.