Check Point SOFTWARE TECHNOLOGIES LTD

Endpoint Protection Business Whitepaper

WELCOME TO THE FUTURE OF CYBER SECURITY
CLOUD • MOBILE • THREAT PREVENTION

ENDPOINTS AT THE EDGE: THE STAKES KEEP RISING

EXECUTIVE SUMMARY

Today's modern IT infrastructure has enabled us to work freely outside our offices and network perimeter. We routinely use our endpoint devices to access corporate email, SaaS apps, and download documents. Remote and mobile computing has boosted our productivity, but how safe is it when research says 70 percent of successful breaches start on the endpoint?[1]

In this paper we ask, "Are you prepared to prevent sophisticated endpoint cyberattacks?" If your answer is 'No" or you're unsure, then use our five best practices to elevate your endpoint threat prevention so it protects your organization against destructive known and unknown cyberattacks.

> "66 percent of respondents say their organization will experience a data breach or cybersecurity exploit that will seriously diminish shareholder value." [2]

NETWORK-CONNECTED ENDPOINTS ARE PRIME TARGETS

Laptops, tablets, mobile phones, or other wireless endpoints (i.e., IoT) connected to the corporate network will grow to 30 billion devices by 2023.[3] Cyberattackers have done the math and know even a miniscule number of under-protected endpoints and ill-advised user decisions represents a Greenfield opportunity. This is why exploited endpoints are commandeered as a frequent attack path for a myriad of advanced security threats.

Phishing attacks using social engineering deceive users with tainted emails and websites, leaking valuable data. The phrase, *"To err is human, to really foul things up requires a computer,"* unfortunately applies to users and endpoint devices. One report found 4 percent of people will click on a phishing campaign.[4] This may seem like a small number until you realize a single wrong click exposes an organization to fraud or the theft of user credentials, customer or patient information, proprietary corporate data, and more.

Ransomware is cyber tyranny on steroids. Locked up systems and its contents can paralyze organizations, resulting in huge financial and reputational losses and lucrative paydays for criminals. The stakes keep rising as cyber extortionists found they can target high net-worth individuals, earning the thieves an average of $360,000 a year.[5] And if attacks by outside threat actors weren't enough to lose sleep over, according to the Ponemon Institute, insider threats costs a global organization more than $8 million per year.[6]

With endpoints in the crosshairs of today's highly targeted and evasive malware threats, all organizations need to re-think their endpoint protection strategy. While signature-based antivirus plays a role in protecting known threats, it's simply not enough in today's threat landscape where the bad actors invent one new attack method after another, spreading malware at higher rates than ever before.

FIVE BEST PRACTICES FOR BUILDING ADVANCED ENDPOINT THREAT PREVENTION

[1] "Cybercrime: The Credential Connection," IDC
[2] "2018 Study on Megatrends in Cybersecurity," Ponemon Institute, February 2018
[3] "The Future of Endpoint Protection, 2019 to 2024," by Chris Sherman, Forrester Research, Inc., January 24, 2019
[4] "2018 Data Breach Investigations Report," Verizonenterprise.com, 2018
[5] "Cyber Extortionists Can Earn $360,000 a Year," by Kelly Sheridan, Dark Reading, February 21, 2019
[6] "2018 Cost of Insider Threats: Global," Ponemon Institute, April 2018

The graphic below identifies five principles you should apply when building strong endpoint security.

1
Reduce attack surface
2
Prevent before it runs
3
Runtime protection
4
Contain and remediate
5
Understand and respond

Figure 1. Five best practices to elevate endpoint security

1. Reduce the attack surface

A common approach in information security is to reduce the attack surface. For endpoints, you need to take full control of peripherals, applications, network traffic, and your data. You need to encrypt data in motion, at rest, and when it's in use. It's also important to make sure you enforce your corporate policies to achieve endpoint security compliance.

Check Point's SandBlast Agent offers the following capabilities to help reduce your attack surface:

- Security controls such as Port Protection, Endpoint Firewall, and Application Control.
- Encryption including IPSec and SSL VPNs, Full Disk Encryption, Media Encryption, and Document Security
- Policy enforcement with Endpoint Compliance

2. Prevent before it runs

The next practice is to first block known attacks by using endpoint anti-malware and reputation, and then prevent unknown attacks. Pre-execution static and dynamic analysis are recommended to provide on- and off-machine inspections. To thwart various exploits, use anti-exploit technology to prevent drive-by attacks and protect your applications. Finally, you can inhibit user mistakes by implementing zero-phishing technology that blocks phishing sites, prevents credential re-use, and detects compromised passwords.

SandBlast Agent offers the following prevention capabilities:

- Block unknown attacks with Endpoint Anti-Malware and Reputation
- Prevent unknown attacks with Pre-Execution Static and Dynamic Analysis
- Thwart exploits with Anti-Exploit
- Inhibit user mistakes with Zero-Phishing
- Prevent zero-days with Threat Emulation and Threat Extraction

> "Check Point SandBlast Zero-Day Protection was on a level by itself. Check Point was one of the only companies that could do Threat Emulation and Threat Extraction
> —and they were the best."
>
> – *Russell Walker,*
> *Chief Technical Officer,*
> *Mississippi Secretary of State*

3. Runtime protection

Anti-ransomware technology allows you to detect signs of ransomware and uncover running mutations of known and unknown malware families by using behavioral analysis and generic rules. This can help you expose file-less attacks that use scripts and cannot be detected by signatures.

SandBlast Agent includes the following runtime protection capabilities:

- Detect ransomware activities with Anti-Ransomware
- Uncover running mutations of known malware with Behavioral Guard: Malware Families
- Discover unknown malware behaviors with Behavioral Guard: Generic Rules
- Expose file-less attacks with Behavioral Guard: File-less Malware

> "The anti-ransomware blade is an amazing piece of technology. Not only does it protect you from ransomware but it doesn't rely on signatures to do it. That means that even if you lose your internet connection you are still protected from unknown variants."
>
> – *Russell Walker,*
> *Chief Technical Officer,*
> *Mississippi Secretary of State*

4. Contain and remediate

Contain attacks and control damages by detecting and blocking command and control traffic and prevent the lateral movement of malware by isolating infected machines. You can then remediate and sterilize your environment by restoring encrypted files, quarantining files, kill processes, and sterilizing the full attack chain.

SandBlast Agent offers capabilities to contain attacks and control damage to an organization:

- Detect and block C&C traffic with Anti-Bot
- Prevent lateral movements by isolating infected machines with Endpoint Firewall

SandBlast Agent remediates and sterilizes environments using these capabilities:

- Restore encrypted files with Anti-Ransomware
- Quarantine files, kill processes, sterilize full attack chain with Forensics-based attack remediation

5. Understand and respond

The final principle is to know you must quickly triage events, understand the full nature of the attack, and immunize other surfaces by sharing Indicator of Compromise (IoC) and Indicator of Attack (IoA) information.

SandBlast Agent helps your organization understand threats and make right responses using:

- Accurate attack status (Active, Dormant, Clean, Blocked) provides quick and efficient triage and event handling
- Understand full attack details with Automated Forensics Reports
- Auto-immunization of other attack surfaces (Network, Cloud, Mobile) with ThreatCloud-based intelligence sharing
- Active threat hunting with Push Operations lets you proactively and retroactively search for observed IOCs, generate forensics reports, and remediate attacks

SANDBLAST AGENT: COMPLETE ENDPOINT SECURITY TO MINIMIZE RISK

SandBlast Agent is Check Point's threat prevention and response solution, providing protection to endpoints and web browsers. It leverages our industry-leading network protections, delivering complete, real-time threat prevention and remediation across all malware threat vectors. With SandBlast Agent, your users work safely no matter where they are, and without compromising their productivity.

> "Since we deployed SandBlast Agent, we have not had a single advanced malware or ransomware incident."
>
> *– Joe Honnold,*
> *IT Manager of Network Services,*
> *Starkey Hearing Technologies*

SandBlast Agent has been built according to three design principles:

1. Innovative threat prevention technologies

- Works across all cyber kill-chain phases: reconnaissance, weaponization, delivery, exploitation, installation, command & control, and action
- Utilizes static, dynamic and behavioral detection and prevention technologies, some using advanced artificial intelligence and machine learning technologies
- Provides high security efficacy and prevention accuracy with highest catch rates and lowest false positives

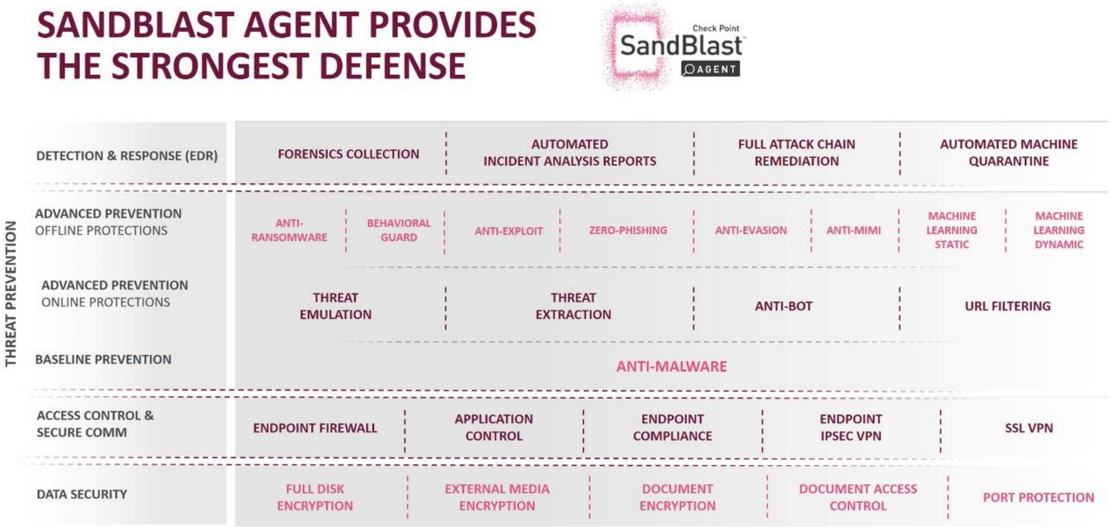
2. Insightful visibility, detection, and response capabilities

- Assures continuous collection of comprehensive and complete row forensics data
- Uses advanced automatic forensics data analysis algorithms to create detailed, yet easy to consume insightful event forensics reports, triggered by endpoint, network or third-party detections
- Employs full attack remediation capabilities including encrypted file restoration, full attack chain sterilization, and machine isolation

3. Complete endpoint security solution

- Elevates threat prevention with a robust solution, consolidating multiple endpoint security functions, agents, and consoles to a single agent managed through a single console
- Offers flexible and scalable management (cloud service or on-premise) and wide platform support
- Integrated into the Check Point Infinity to get maximum prevention across all attack surfaces, shared intelligence, and a single point of management

SandBlast Agent is a complete endpoint security solution that allows you to consolidate your legacy point products into a single product as evidenced in the chart below:



SANDBLAST AGENT PROVIDES THE STRONGEST DEFENSE

DETECTION & RESPONSE (EDR)	FORENSICS COLLECTION	AUTOMATED INCIDENT ANALYSIS REPORTS	FULL ATTACK CHAIN REMEDIATION	AUTOMATED MACHINE QUARANTINE				
THREAT PREVENTION: ADVANCED PREVENTION OFFLINE PROTECTIONS	ANTI-RANSOMWARE	BEHAVIORAL GUARD	ANTI-EXPLOIT	ZERO-PHISHING	ANTI-EVASION	ANTI-MIMI	MACHINE LEARNING STATIC	MACHINE LEARNING DYNAMIC
THREAT PREVENTION: ADVANCED PREVENTION ONLINE PROTECTIONS	THREAT EMULATION	THREAT EXTRACTION	ANTI-BOT	URL FILTERING				
THREAT PREVENTION: BASELINE PREVENTION	ANTI-MALWARE							
ACCESS CONTROL & SECURE COMM	ENDPOINT FIREWALL	APPLICATION CONTROL	ENDPOINT COMPLIANCE	ENDPOINT IPSEC VPN	SSL VPN			
DATA SECURITY	FULL DISK ENCRYPTION	EXTERNAL MEDIA ENCRYPTION	DOCUMENT ENCRYPTION	DOCUMENT ACCESS CONTROL	PORT PROTECTION			

Figure 2. SandBlast Agent Complete Security

SandBlast Agent advanced prevention capabilities have earned high ratings from the NSS Labs Advanced Endpoint Protection (AEP) test, Forrester ESS Wave Q2 2018 report, and “Top Product” by AV-TEST.

FLEXIBLE ENDPOINT SECURITY MANAGEMENT

Manage your endpoint security on premise or delivered as a cloud service, fully deployed, maintained, updated, and optimized by Check Point. The cloud service offers high availability, elasticity to incorporate your growth, and location independence to manage from anywhere and anytime.

CHECK POINT INFINITY: INTEGRAL TO THE HOLISTIC SECURITY ARCHITECTURE

SandBlast Agent is a core component of Check Point’s Infinity Architecture protecting against advanced 5th generation, large-scale, multi-vector mega attacks across endpoint, network, mobile, and cloud.

CHECK POINT THREATCLOUD COLLABORATIVE INTELLIGENCE

Up-to-date global threat intelligence using a worldwide network of threat sensors that proactively mitigate threats based on global threat information.

CONCLUSION

Technology has improved user productivity outside the network with remote and mobile computing via portable endpoint devices. But it has also elevated the risks. Malware and unknown, zero-day threats are penetrating endpoints to harvest sensitive data from the network. Check Point recommends that you review your security strategy by comparing your current endpoint protection with our five best practices for advanced endpoint threat prevention.

> “We are really pleased with the unified approach to security provided by Check Point Infinity. All of our security platforms communicate and share data with each other, which means that rather than just relying on detection, we know that we are actively preventing problems from occurring. This gives us confidence that our corporate and customer data is secure and that we are GDPR compliant.”
>
> *– Laurent Grutman, CIO, Laurenty*

For further information on SandBlast Agent, contact your local Check Point representative or visit us at https://www.checkpoint.com/products/advanced-endpoint-threat-prevention/