Lookout

TOP TAKEAWAYS

Endpoint to Cloud Security:

5 Best Practices for Achieving Zero Trust in a Changing Threat Landscape

Overview

For state and local governments, the pandemic shifted the goalposts on cybersecurity.

"With the move to telework, as well as the proliferation of cloud applications, everything has changed," said Stephen Banda, Security Solutions Manager at Lookout, an integrated endpoint to cloud security organization that enables Zero Trust for commercial and government customers. "The legacy security perimeter is obsolete."

Looking across a range of state and local verticals, a number of recent vulnerabilities have become apparent:

Healthcare: With doctors and nurses increasingly dependent on mobile devices and cloud-based applications, which allow people to work from anywhere, there's been an upsurge in attackers using social engineering to exfiltrate personal data and even to manipulate medical devices.

Transportation: Recent cyberattacks, for example on the New York City subway, show how transportation may be vulnerable to exploits, many of which are initiated through mobile connectivity.

Public safety: The use of mobile devices and cloud apps have escalated ransomware attacks against police departments, as well as enabled bad actors to exfiltrate data on criminal gangs and even public safety personnel.

Utilities: The Colonial Pipeline attack underscored the vulnerabilities inherent in the utility infrastructure. As mobile becomes increasingly a part of the operational landscape, utilities' industrial control systems and other key assets may be susceptible to attack.

Education: K-12 schools are seeing a huge rise in ransomware attacks as malicious actors exploit vulnerabilities in distance learning systems, according to an alert by the FBI. In fact, according to MS-ISAC, August and September of 2020, 57% of all MS-ISAC reported ransomware incidents involved K-12 schools--nearly doubling the percent reported from the first half of 2020.

To effectively address emerging security risks in these changing times, state and local governments need a new approach to cybersecurity. In particular, they need to implement a series of best practices to ensure their organization and data is secure from endpoint to the cloud. The answer, many are finding, lies in a Zero Trust security framework.

Zero Trust moves away from automatically granting users, devices or networks access to applications or data, which can introduce risks. Instead, organizations need to grant access dynamically and in real time based on the risk level of the user and device.

In fact, the method has proven so successful that the federal government is already moving aggressively towards Zero Trust frameworks. Thanks to a May 2021 executive order from the Biden Administration, agencies are required to have a plan to adopt a Zero Trust framework within 90 days.

"The Zero Trust framework is really the guiding light," Banda said. "You need to ask yourself what you can put in place today to ensure your organization will have a Zero Trust security posture that extends from mobile all the way to the cloud."

5 best practices

As state and local governments look to move forward with Zero Trust frameworks, it's important to note that it will require more than just purchasing disparate security solutions. Zero Trust requires agencies to adopt both trusted technologies and implement best practices, which call for organizations to implement modernized endpoint protection to defend all devices against phishing, application threats, network attacks and other modern cyberattacks.

What does this look like in practice? These five key areas help define the modernized approach to developing a Zero Trust architecture:

1. Mobile Endpoint Security
2. Zero Trust Network Access, or ZTNA
3. Cloud Access Security Broker, or CASB
4. Threat Intelligence
5. Secure Access Service Edge, or SASE

1. Mobile Endpoint Security

Mobile Endpoint Security (MES) protects mobile devices, beyond the perimeter, from known and unknown threats in compliance with Federal Risk and Authorization Management Program and privacy standards. It defends against phishing and ransomware, as well as against nefarious applications and network-based threats. It also continuously monitors the device to ensure its risk level is low when connecting to sensitive data.

"Lookout uses [machine intelligence] to analyze telemetry data from 200 million devices and 140 million apps," Banda said, noting that the data helps to ensure devices behave as they should. Meanwhile, organizations can tap Lookout MES to rapidly detect and address anomalous device behavior or events.

"Lookout uses [machine intelligence] to analyze telemetry data from 200 million devices and 140 million apps,"

Stephen Banda
Security Solutions Manager
Lookout

2. Zero Trust Network Access, or ZTNA

Based on the principles of the Zero Trust security framework, ZTNA is a means of dynamically granting access to private enterprise applications that are on-premise or in a private cloud. ZTNA modernizes these applications with secure access capabilities, ensuring that teleworkers have seamless access from any device without sacrificing security. Organizations have used VPN to deliver remote access to these applications but are shifting to ZTNA due to the many benefits it provides including easy IT administration, improved user experience and security.

Traditionally, government managed access to sensitive data through a virtual private network, but modern attack methods can compromise this safeguard, Banda said. ZTNA offers a further level of defense.

"With Zero Trust, we know very specifically the behavior of that user, the rights of that user and they only get access to this one application and not the rest of the environment," he said "Lookout gives you that in a ready-made solution that is easily deployed."

3. Cloud Access Security Broker, or CASB

Similar to how ZTNA secures access for on-premise and private applications, CASB provides secure access control for software-as-a-service (SaaS) applications in the cloud. It removes risk from countless cloud apps, providing visibility into users, cloud and data, to detect and respond to threats and dynamically control access.

"CASB ensures the user has the right to access specific applications," Banda said. "It also has a Data Loss Prevention component, which ensures that data is not leaking out of the cloud applications." With CASB, administrators have greater control of who has access to what data.

"You can set granular control policies and can manage those from a single console, with full visibility into how applications in your cloud are being used: who is using them, where and with what devices," Banda said. "All that comes to a single point-of-view console."

of mobile threats have been detected by Lookout's Threat Intelligence Services Team over the past 5 years

4. Threat Intelligence

Lookout works to enhance public and private collaboration through a global sensor network of millions of mobile devices, along with insights from mobile security research. All this helps support endpoint detection and response — and it already has. Lookout's Threat Intelligence Services team has detected more than 90% of all mobile threats over the past five years, according to the company, including Pegasus spyware, malicious actor Dark Caracal, who ran significant espionage and phishing campaigns, and several significant Android surveillanceware tools.

"Threat Intelligence is all about being able to take a lot of data and using it to empower not just security response but also things like forensic investigations," Banda said. "If you think you may have been breached, Threat Intelligence tells you whether that threat is persisting in your environment, and what systems may have been impacted."

5. Secure Access Service Edge, or SASE

To ensure organizations are secure from endpoint to cloud, SASE encompasses a range of defenses including ZTNA and CASB. SASE enables organizations to secure data while providing a seamless and efficient user experience regardless of where they work or what device they use. It provides granular and dynamic access that matches user risk posture with the ability to encrypt data on the go to prevent unauthorized access.

"The benefit to SASE is that it delivers these protections via a platform approach," Banda said. "Rather than have multiple solutions in play, SASE offers IT a frictionless means to deploy a wide range of capabilities in a coordinated way."

Next steps for a more secure future

For state and local entities seeking to adopt Zero Trust and bolster their endpoint defenses, it makes sense to start with a look inward.

"Your first step is to do an inventory of what you have," Banda said. "Most organizations will have a mobile device management solution in place, but that's strictly for management. To understand the security posture, you need to ask: What do your users need to access? Do you want to enable your users to use their own personal devices as part of your strategy for being productive? What are the critical applications they need to access?"

Government agencies will need to factor in the regulatory landscape, taking into consideration the privacy and security rules that may impact their data uses.

Organizations also will want to consider their efforts to support the Zero Trust framework, to look at how those efforts align with their overall security efforts and initiatives. With this information in hand, it's possible to assess the commercial offerings and determine which solutions are the best fit. The Lookout Cloud Security Platform offerings deliver integrated endpoint-to-cloud security, helping organizations secure data and empower productivity in a privacy-focused world.

Learn more

about how Lookout can keep your agency secure.